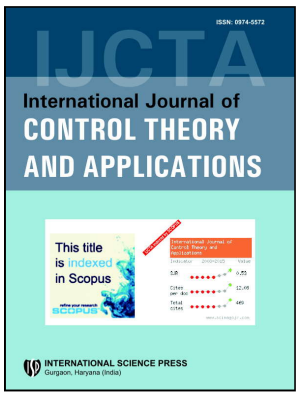

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 15 • 2017

Using Keystroke Dynamics to Generate Cancellable Fingerprints

Saurabh Singh[1] and Madhavi Sinha[2]

[1] Department of Computer Science and Engineering Amity University, Noida, UP, India,
Email: saurabh.iiet@gmail.com
[2] Department of Computer Science and Engineering Birla Institute of Technology,Jaipur, Rajasthan, India,
Email: madhavisinha@bitmesra.ac.in

Abstract: Fingerprints are probably the most commonly used biometric trait today. Due to large number of fingerprint applications, biometric data of an individual is available at various places and these applications become good source of sensitive data for intruders. Also, once the biometric data is exposed, it is exposed forever. No one can change one's biometric data like passwords, pins etc. Cancelable biometric provides solution to this problem by storing the distorted version of the original biometric using some transformation functions. This solution is excellent but still not provides security against the theft of biometric data from user's end. For example, someone's fingerprints may be recovered from user's belongings like table, chair etc. In this paper, we propose to transform the original fingerprint using user's behavior with keyboard characteristics. Experimental results of our approach yielded impressive equal error rate of 1.26%.

Keywords: Cancellable Biometric, Fingerprints, Keystroke Dynamics, Multi-model biometrics.

1. INTRODUCTION

Biometrics systems utilize human's physical and behavioral characteristics to recognize the individual. There are many advantages of such systems. However, there are some challenges associated with these systems [1].

1. A biometric trait of a person has to be used by a person lifelong. If it is exposed, user cannot change it like passwords or pins.
2. A biometric trait like fingerprint is used in numerous applications, which makes the original biometric data access easy to intruders.
3. Biometric trait is not a secret like passwords, pins etc. that are known only to the user. Biometrics like face, fingerprints, voice etc. can be easily recorded.

Cancellable biometrics proposes a solution to above problems by transforming original biometrics before storing them in user's profile. Since, in this scheme user do not use original biometric, if it is exposed, a new

transformed version of the original biometric may be used. This provides the solution to the 1st problem described above. Cancellable biometric also enable the user to have different transformed version of the same biometric for different applications solution to 2nd problem). Although cancelable biometric ensure security of biometric data from system end, It is not helpful, if biometric data is stolen directly from user's belongings (Fingerprints can be recovered from table, chair touched by the user).

In the proposed work, we present a new transformation scheme to transform the biometric data of user's fingerprint using his/her keystroke dynamics characteristics. We are intentionally not calling this scheme a multimodal biometric scheme, because we are not combining the biometric data of fingerprint and keystroke dynamics, rather, we are distorting the fingerprint using keystroke characteristics, Moreover, end user can change this distortion by changing the transformation code. This work provides solution to all the challenges described above, if anyone records user's biometric, even then he/she cannot get access to the system, because, in this scheme, the transformation function is devised by behavioral biometric which cannot be recorded easily. Rest of the paper is organized as follows- Section 2 reviews the work done so for in this area.

2. RELATED WORK

Cancelable biometric was first defined by Ratha et al. [1] in 2001 (also called revocable biometrics). After that, cancelable biometric has become a popular area of research. Many alternate solutions have emerged from both the biometric and cryptographic community. In password salting [2] [3], a robust biometric key is defined from the additional information provided by the user. This biometric key is then used salt the original biometric signal. Another technique called *biometric* key generation [4] [5][11] uses biometric signal itself to generate the key to be used to salt the biometric signal. In non-invertible transformation technique, the biometric signal is transformed using a one way function to achieve irreversibility. Ratha et al. [6] transformed a fingerprint template by dividing the fingerprint image into cell and these cells were shifted using one way mapping. Fig. 1 shows the shifting process. The one way function maps the cell numbered 8 and 16 are mapped into same cell, this ensures the irreversibility of the process. They also proposed a polar shifting method in which, cell's orientation is altered. Fig. 2 shows the polar orientation process. Jinyu Zuo et al. [7] proposed a cancelable technique called GRAY COMBO for iris pattern, in this technique they shifted and combined rows in unwrapped iris image. S. Chikkerur et al. [8] proposed a registration free cancelable method for fingerprint template in which, they used localized self-aligned texture features of finger prints.

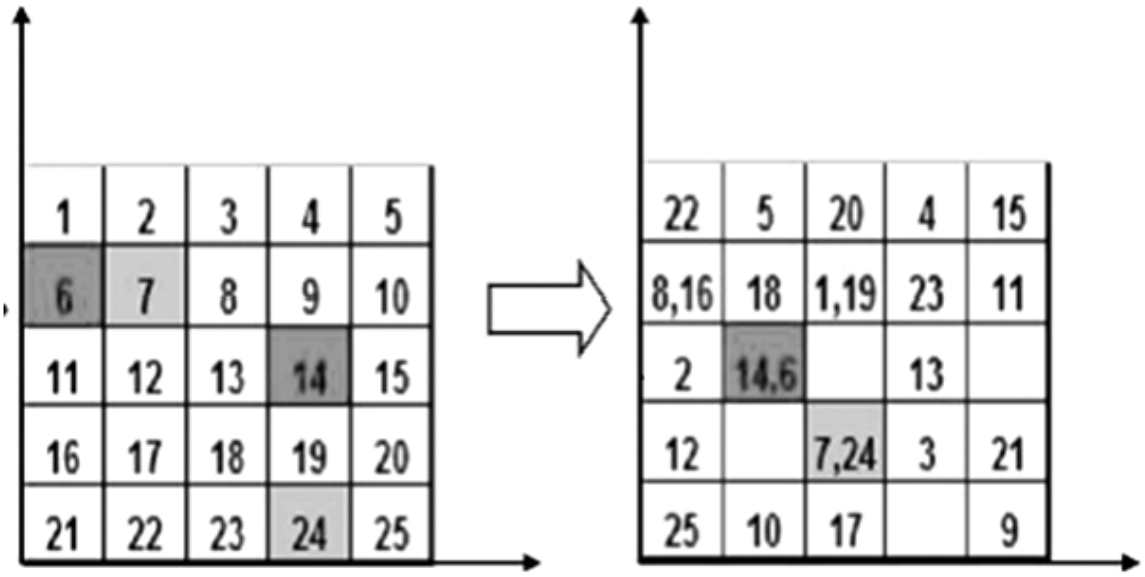

Figure 1: The Cartesian Transform [6]

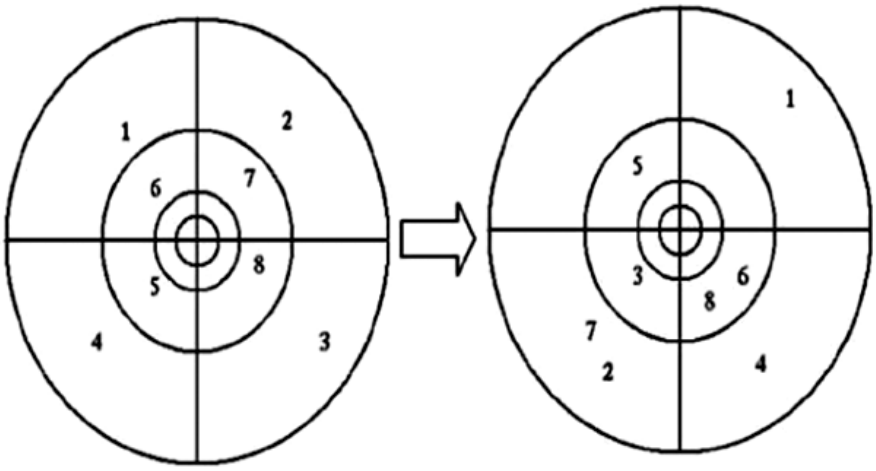

Figure 2: The polar Transform [6]

3. PROPOSED WORK

In our work, we propose to construct cancelable fingerprint template by a key derived from user's keystroke dynamics characteristics. This approach takes following advantage over previously developed approaches – previous approaches concentrated only on preventing fingerprint template from system end but if anyone acquires user's fingerprint from anywhere else like belongings of the user (table, chair etc.), it can still be misused. In the proposed approach, we combine fingerprint (Physiological) and keystroke dynamics (Behavioral) to construct the template. It is very difficult to acquire someone's behavioral characteristics.

Moreover no one can acquire the fingerprint template from system as it is transformed by a key generated by keystroke dynamics of the user. The enrolment and authentication process of the proposed system is illustrated in Fig. 3.

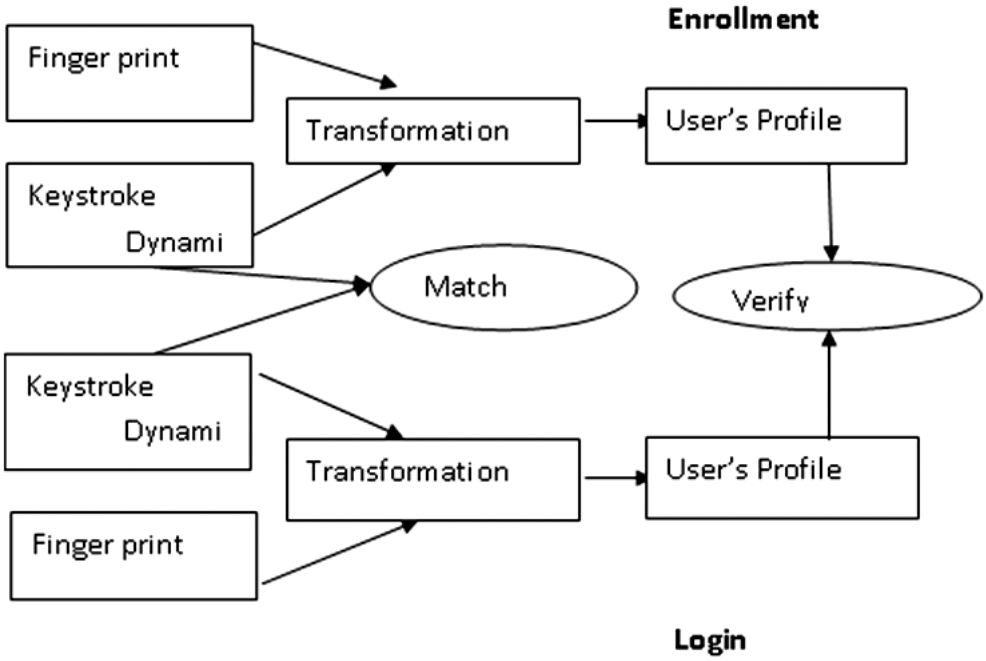

Figure 3: Enrollment and Authentication Modules of the Proposed System

Principle steps of the complete process are explained in following sections-

3.1. Acquiring keystroke behavior

Keystroke dynamics analyses rhythm of the keystroke pattern entered by the user. Commonly keystroke dwell time and flight time is used to represent keystroke behavior. Dwell time is the duration between a key press and release and flight time is the time interval between two characters. In the proposed work, we have selected flight time for analysis. Singh and Arya [9] found that the standard deviation of flight time is evaluated to be greater than that of dwell time. Data collected from 10 users is illustrated in table 1, this justifies the selection of flight time.

From the collected flight time for a particular password, a vector is prepared, which will be used to generate cancelable fingerprints. By changing this password, multiple transformed fingerprints can be generated. For instance, a vector prepared from a password of 5 characters is shown below- (12, 14, 11, 18)

3.2. Constructing of Transformed fingerprint Template

After forming flight time feature vector as discussed in previous section, the vector is used as transformation key for the original fingerprint image. For instance, consider a portion of fingerprint matrix which is being transformed by a transformation key:

$$[12\ 14\ 11\ 18]\begin{bmatrix}1 & 1 & 0 & 1\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 0\\ 1 & 1 & 0 & 1\end{bmatrix}=\begin{bmatrix}12 & 14 & 0 & 18\\ 0 & 14 & 11 & 0\\ 0 & 0 & 11 & 0\\ 12 & 14 & 0 & 18\end{bmatrix}$$

In above example, we have considered a binary fingerprint template, which is used to generate a transformed template using a transformation key. In the transformation process, elements of the key are multiplied with corresponding elements of the matrix and then the same operation is performed with the next row. It is obvious that, by changing the password, we can change the transformation vector and hence, the generated template. If the same password is entered by any other user, the transformation vector will be far away from the legitimate user's transformation vector and the intruder will be rejected.

Table 1
Dwell Time and Flight Time (in ms) of The Password "intel" entered by 10 users [8]

Threshold	10	15	20	25	30	35	40
FAR	0.593	0.83	0.92	1.23	1.56	1.98	2.1
FRR	2.9	2.3	1.98	1.41	1.02	0.97	0.42

Table 2
FAR and FRR Values Obtained for Different Threshold Values

User	*D(i)*	*FT*	*D(n)*	*FT*	*D(t)*	*FT*	*D(e)*	*FT*	*D(i)*
1	4	12	4	14	3	11	4	18	5
2	3	11	4	16	5	-1	6	19	4
3	4	-2	9	-2	2	15	3	9	7
4	6	7	4	10	4	23	2	12	3
5	3	10	4	19	3	9	6	51	7

(*contd...Table 2*)

User	*D(i)*	*FT*	*D(n)*	*FT*	*D(t)*	*FT*	*D(e)*	*FT*	*D(i)*
6	4	16	6	13	4	30	4	-2	6
7	6	21	4	9	5	10	6	27	7
8	7	8	8	11	6	25	5	24	10
9	9	23	3	7	5	28	4	-1	6
10	7	20	3	12	4	35	5	9	7
STD DEV	2.00	7.60	2.07	5.70	1.19	11.3	1.35	15.4	1.93

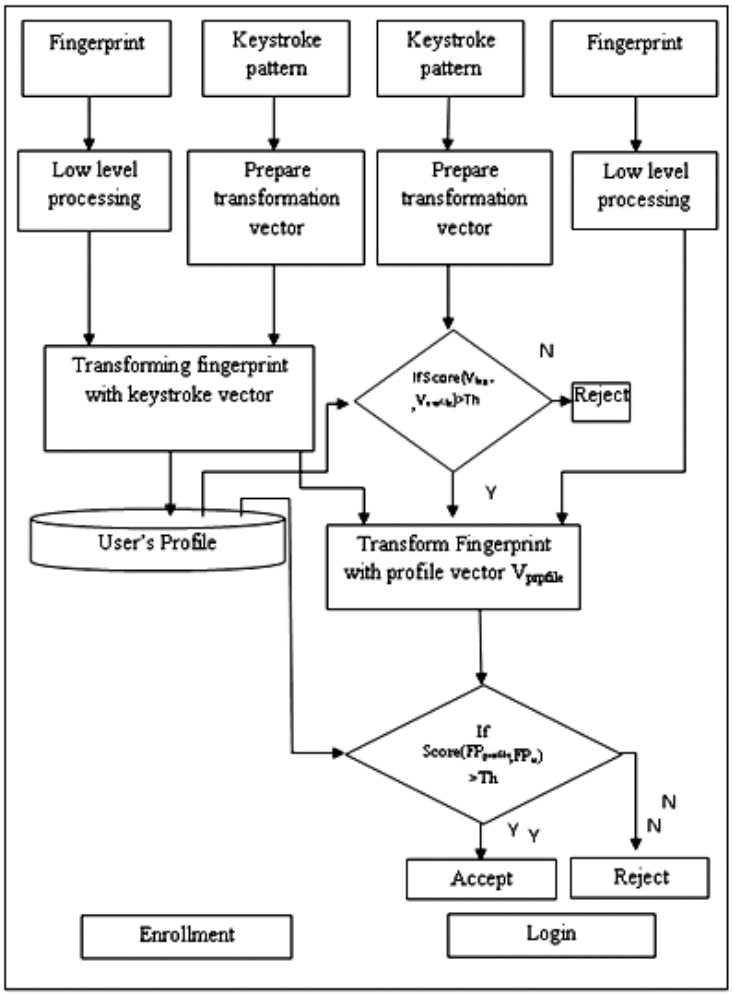

Figure 4: The Proposed System

4. EXPERIMENTAL SETUP

For experimental study, a program is developed to capture flight time and to prepare timing vector. In the experiment, 50 participants having adequate typing experience were asked to enroll. Each user tried 5 times as legitimate user and one time as intruder for all other participants. For different threshold values, the FAR (False Acceptance Rate and FRR (False Rejection Rate) is calculated, which are illustrated in Table 2. Graph of figure 5 illustrates that the Equal error rate of 1.26 is obtained at threshold value of 26.

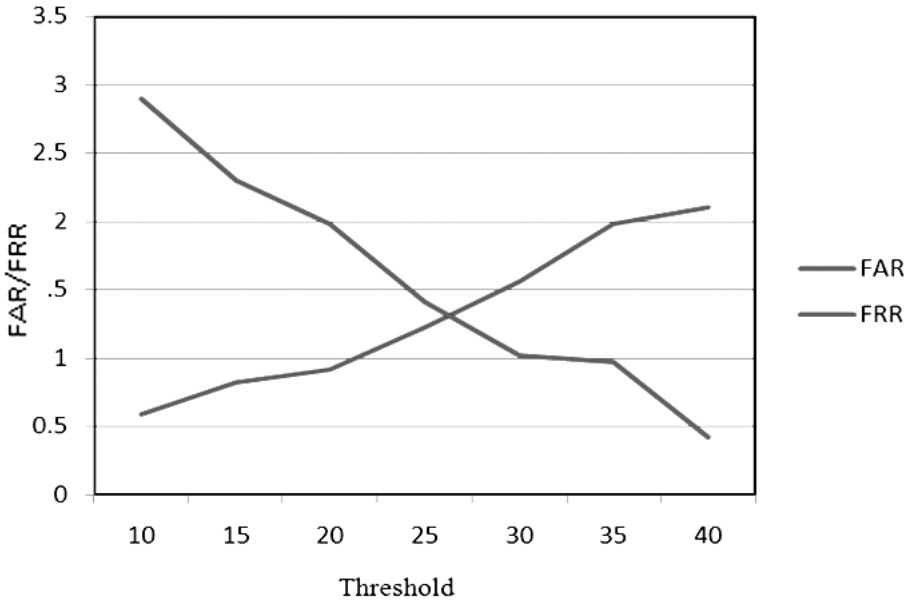

Figure 5: Graph for FAR and FRR against Threshold value.

5. CONCLUSION

In this paper, we proposed a new approach of biometric cancelability. In which, we have generated cancelable fingerprints using user's keystroke dynamics. Being a behavioral characteristic, keystroke dynamics cannot be easily recorded. The security of the system cannot be easily compromised either from system end or from user end. With this implementation, equal error rate achieved is 1.26%. The proposal can be extended to other biometric systems like iris scan. Further study is required to examine the possibilities of combining two physiological or two behavioral biometric systems.

REFERENCES

[1] N.K. Ratha, J.H. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication System," IBM Systems Journal, vol. 40(3), pp. 614-634, 2001.

[2] Y. Sutcu, H.T. Sencar, and N. Nemon, "A Secure Biometric Authentication Scheme Based on Robust Hashing," Proc. SeventhWorkshop Multimedia and Security, pp. 111-116, 2005.

[3] T. Connie, A.B.J. Teoh, M.K.O. Goh, and D.C.L. Ngo, "PalmHashing:A Novel Approach for Cancelable Biometrics," Information Processing Letters, vol. 93(1), pp. 1-5, Jan. 2005.

[4] F. Monrose, M.K. Reiter, and S. Wetzel, "Password Hardening Based on Key Stroke Dynamics," Proc. ACM Conf. Computer and Comm. Security, pp. 73-82, 1999.

[5] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable Key-Based Fingerprint Templates", Proc. 10th Australian Conf. Information Security and Privacy, pp. 242-252, 2005.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Generating Cancelable Fingerprint Templates", IEEE transactions on pattern analysis and machine intelligence, vol. 29(4), 2007.

[7] Jinyu Zuo, Nalini K. Ratha and Jonathan H. Connell, "Cancelable Iris Biometric," Proc. 19th International Conference on Pattern Recognition, pp. 8-11, 2008.

[8] S.chikkerur,N.K. Ratha,J.H. Connell,R.M. Bolle, "Generating registration-free cancelable fingerprint templates", Proc. 2nd IEEE International conference on biometrics: Theory,applications and Systems.Arlington, 2008.

[9] S. Singh and K. V. Arya, "Key Classification: A New Approach in Free Text Keystroke Authentication System", Proc. 3rd pacific Asia conferance on Circuit, Communication and System, pp237-242, 2011.

[10] R. Mehul, "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proc. the 2003 IEEE TENCON, pp. 935-938, 2003.

[11] H. Saevanee, N. Clarke and S, Furnell, "Continuous user authentication using multi-model biometrics", Computers and Security, pp.34-246, 2015.