FULLTIME BIOMETRIC MOUSE DESIGN FOR CONTINUOUS AUTHENTICATION

P. T. Ndung'u[1], R. W. Mwangi[2] and S. M. Kang'ethe[3]
[1,2]Institute of Computer Science and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi
[3]Inorero University, Nairobi
E-mail: waweru_mwangi@icsit.jku

Abstract
As we embrace the information and communication technology in our everyday activities and day-to-day transactions, security concerns have increasingly come to light, especially in some of the critical areas of our society today such as education, health and commerce, where such security concerns are even higher. The need for complete and clear authentication and authorisation is of paramount importance. This paper explores and presents the optimal use of full-time biometric mouse (FBM) for continuous authentication, which would not only enable authentication during log in and start of an application, but will enable continuous authentication throughout a transaction. We formulate a full-time biometric mouse (FBM) design that would ensure thumb positioning and its ergonomics while ensuring comfort and maximum contact with the scanner to enable continuous authentication of the user in a speedy, easy and non-strenuous way. The mouse employs a simple algorithm that ensures quick operation to cut on possible delays and yet maintain the accuracy of the system

Key words: Biometrics, continuous authentication, identification, verification, authentication, minutiae

1.0 Introduction

The computer mouse is gaining popularity as a tool of contact between the human being and computer system. Biometric mice have been used in user emotional and labour productivity analysis (Kaklauuskas et *al.,* 2008), detecting computer misuse and intrusion using mouse movements, (Eusebi et *al.*, 2008), and behavioral biometrics (Ahmed and Traore 2005). This is a clear indication of the fact that the computer mouse has been identified as the one device with the highest amount of contact with the human user and thus reliable in detecting and measuring usage and the physiological and psychological state of the user during usage. This therefore makes the mouse a superior tool for security checks monitoring and analysis, to offer credible and reliable personal identification and authentication from the onset (log in), as well as continually.

In an increasingly digital world, reliable personal identification and authentication has become an important human computer interaction activity. Existing security measures rely on knowledge-based approaches like passwords or token-based approaches such as swipe cards and passports, to control access to physical and virtual spaces. Though ubiquitous, such methods are not very secure since they can be shared, forged, replicated, bypassed, stolen or forced out of the owner and used with or without the owner's knowledge and consent. Passwords and PIN numbers may also be stolen electronically. Even worse is the fact that when used after unlawful and unauthorised acquisition, the systems that apply them do not detect since they cannot differentiate between authorised and unauthorised user.

Biometrics offers a means of reliable personal authentication that can address these problems. This is because biometrics proves not only the identity of the owner but also the presence of the owner in the concerned activities. It is more effective since it cannot be stolen unless one is kidnapped and forced to personally access the system and go through security checks under duress. Biometrics is defined as the science of verifying the identity of an individual through physiological measurements or behavioural traits. Jain et *al.* (1999) defines biometric authentication as a process of determining whether someone is in fact the one the person is declared to be, based on physiological and behavioural characteristics of the individual. Biometric identifiers are associated permanently with the user, and thus used for both identification and verification.

Fingerprints were accepted formally as valid personal identifier in the early twentieth century and have since then become a de-facto authentication technique in law-enforcement agencies world over. Fingerprints have several advantages over other biometrics, since it is highly distinct, permanent, easy to collect, accurate and widely accepted world over. Automatic fingerprint identification systems (AFIS) provide the tools and techniques required for quick and clear personal identification. The fingerprint image is acquired using a live capture device consisting of an optical, capacitive, ultrasound or thermal sensor (Maio et.al*,* 2003), which means even fake fingers can be detected.

In this paper we propose an optimal full-time biometric mouse (FBM) for continuous authentication. This is mainly because one handles and uses a mouse throughout the operation with a computer and thus the mouse, unlike any other computer device offers a constant point of contact where the fingerprint can be scanned upon execution of commands issued using a mouse, thus ensuring that those commands are issued by the authorised person and it is thus safe to execute them. Specifically, we look at its design, ergonomics and logical structure of its operation in continuous authentication

2.0 Existing Scanners (Systems)

Most of the existing systems are based on one-time identification and authentication, where once one is identified and authenticated, the system assumes that all subsequent operations are done by the said person until such a point that the said user logs out. This is very dangerous especially in hostile and security-sensitive environments, where exposure for a few minutes could lead to far-reaching transactions and with the initial authorised user being implicated. This is prominent in multi-user environment environments where computers are shared by different people and are not personalised to individuals such as supermarkets, banks and other customer service and transaction processing terminals where one handover the terminal after a few hours of work. Also, in a busy environment where terminals are next to each other, a few seconds of break from the system may allow the next neighbour enough time to interfere in ways that the innocent original user is implicated of wrong doing. This is because the audit trail registers allocate the transactions to the logged on person regardless of the fact that a different person carried out the transaction.

The existing biometric mouse-scanning devices fall short of the envisaged capability and thus do not meet the stated need. They are designed to enable biometric login control and security management. However, they are incapable of fulltime and continuous authentication during system operations. This is because they are either made as separate devices (mouse and scanner), thus once the user log on sets the scanner aside and proceed working with the mouse and doesn't refer back to it any more for further authentication as seen in the Microsoft Corporation's biometric mouse, see Figure 1. Other versions that combine the functions of two devices for the purpose of portability fall short of achieving the purpose since the location of fingerprint acquisition on the scanner is misplaced. The Siemen's version of biometric mouse is one such example where the camera is located at the top of the scanner, which means that one authenticates once and forgets about the scanner since the palm of the hand covers it during the normal usage of the mouse. See Figure 2.

While there have been improvements made on security by the introduction of the biometrics, it is acknowledged that in hostile and security-sensitive environments, continuous authentication, or re-authentication is desirable so that a system can be monitored for the duration of the session to reduce the vulnerability (Sim *et al.,* 2007). The system must be able to discriminate and protect the users by blocking any commands issued by any unauthorised persons. To achieve this, there has to be an input device that is

able to capture, detect, analyse and report appropriately and in timely manner. A new ingenious design needs to be developed, placing the scanner at the right position to gain maximum and full time contact and availability for the intended purpose.

Figure 1: The Wireless IntelliMouse Explorer with Fingerprint Reader.
Photo courtesy: Microsoft Corporation

Figure 2: A computer mouse with a built-in fingerprint scanner
Photo courtesy: Siemens

3.0 Proposed Biometric Mouse Scanner

In this research, we propose the design and development of a full-time biometric mouse that creates a unified combination of the functions of an optical mouse and fingerprint scanner in one device. The scanner shall be placed directly at the point corresponding to where the thumb rests on the mouse as shown in Figure 3. In this way, the thumb shall rest on the scanner all the time and its cameras should be made in such a way that they are triggered by the mouse buttons any time the user clicks on it to execute specific key commands.

The scanner should have the capability for aliveness detection, capable of detecting and determining aliveness of the user. The scanner uses a thermal camera as an input device where the infrared (IR) image of the dorsal surface of the finger is acquired at the same time as the biometric sample by a scanner (Ribaric and Fratric 2005). The combination of aliveness detection and biometric capture (of thumbprint) and the capability of verifying and authenticating them in the same system increase the fraud detection and makes the biometric authentication system more robust.

The biometric mouse shall be event-based in its activation, where in the event that the user executes the specified commands, the scanner is activated, where it captures the thumbprint of the user, detects the aliveness and authenticates the user. These may include events such as print, open (existing or new file), save or save as, close, move to a new page. This means that if an authorised person logs in and the system is taken over by a different user, it should react as appropriate, depending on the status of the new user. The system can logout or suspend its operations, shut down or change the log in details to suit the new (authorised operator) and make appropriate report on intrusion, capturing the fingerprint of the said intruder and storing in a database as clear evidence for investigation and prosecution purposes. The system should be customisable to allow users set up the events they would deem important enough to warrant activation of the scanner. This way, the system could be relieved of some basic instances depending on the security situation and the environment of the users. The reactions of the system to an intrusion while an authorized user is logged on to the system are as shown in Table 1.

Table 1: System reaction to intrusion

Intruder type	**System check**	**System reaction**	**Effects on privileges**	**Reports**
Administrator	Identify fingerprint in database	-Request logged on user to authorise continuation of existing work. -Close the existing work. -Authorise and log in as administrator	Allow the Administrato r's privileges	Any transactions be marked for this user
Authorised user (same privileges)	Identify fingerprint in database	-Request logged on user to authorize continuation of existing work. -Close the existing work. -Authorise and log in as the new user	Allow same privileges	Any transactions be marked for the new user
Authorised user (lower privileges)	Identify fingerprint in database	-Request logged on user to authorise continuation of existing work. -Close the existing work. -Authorize and log in as the new user	Lower privileges as appropriate	Any transactions be marked for this user
Unauthorised user	-Check fingerprint in existing database	-Close the existing work. -System log out and stop any operation. -Capture the fingerprint and store in intruders database	Stop any usage (no rights/ privileges at all)	-Report on the intrusion as an alert to the administrator and security-Store the fingerprint sample for possible printing and identification for investigation and prosecution

3.1 The Design Structure

3.1.1 Physical Design

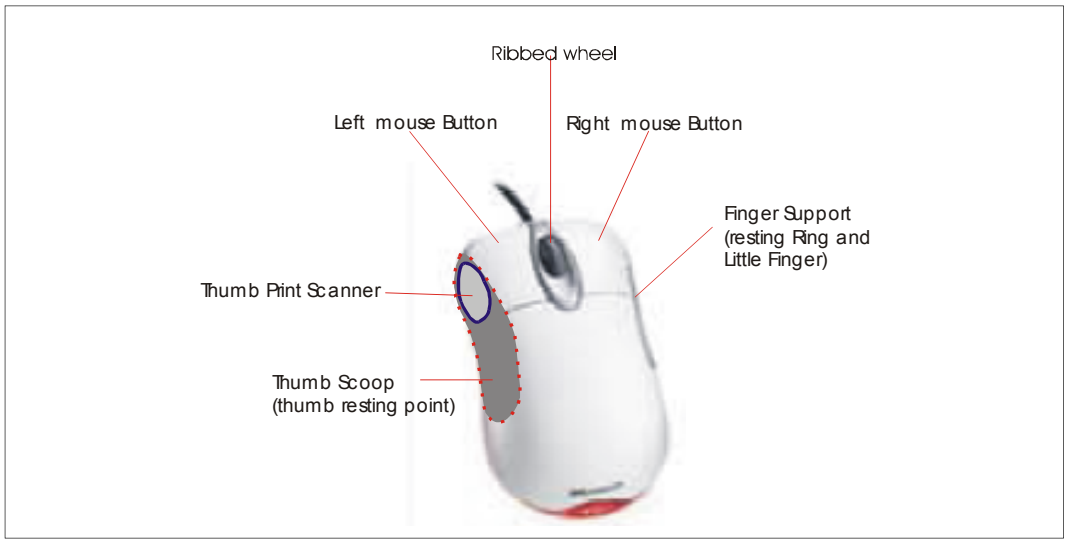

Figure 3: Proposed biometric mouse indicating the proposed position for the thumb print scanner (for a right hand user)

3.1.2 Logical Design

The biometric mouse is expected to work on the optical technology for both the scanner as well as the mouse**.** The scanner works with optical sensors where a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal. They can provide resolutions up to 500 DPI, and are mostly based on FTIR (frustrated total internal reflection) technique to acquire the image. In this scheme, a source illuminates the fingerprint through one side of the prism as shown in Figure 4. Due to internal reflection phenomenon, most of the light is reflected back to the other side where it is recorded by a CCD camera. However, in regions where the fingerprint surface comes in contact with the prism, the light is diffused in all directions and therefore does not reach the sensor resulting in dark regions (Pankanti *et al.* 2002).

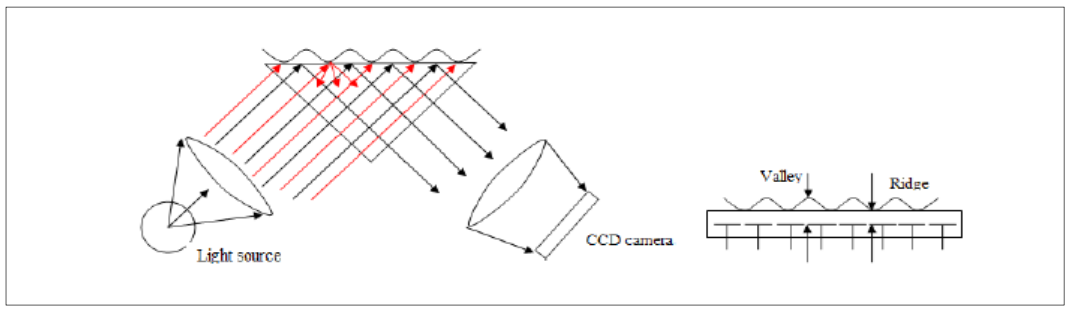

Figure 4: (a) General schematic for an FTIR based optical sensor
(b) Schematic of a capacitive sensor

Our proposed biometric authentication system is minutiae-based, which must have three major components namely the scanner, processing software, and the interface. The scanner provides mechanisms and the means to capture a digital image of a living person's biometric fingerprint. This include aliveness detection component built into the same device. The software does the processing and storage as well as matching of the captured sample and the template in the database. On the other hand, there must be a clear interface with the software that makes use of (consume) the results by confirming the person's identity and act on the results. The resultant biometric authentication security system is illustrated in Figure 5.

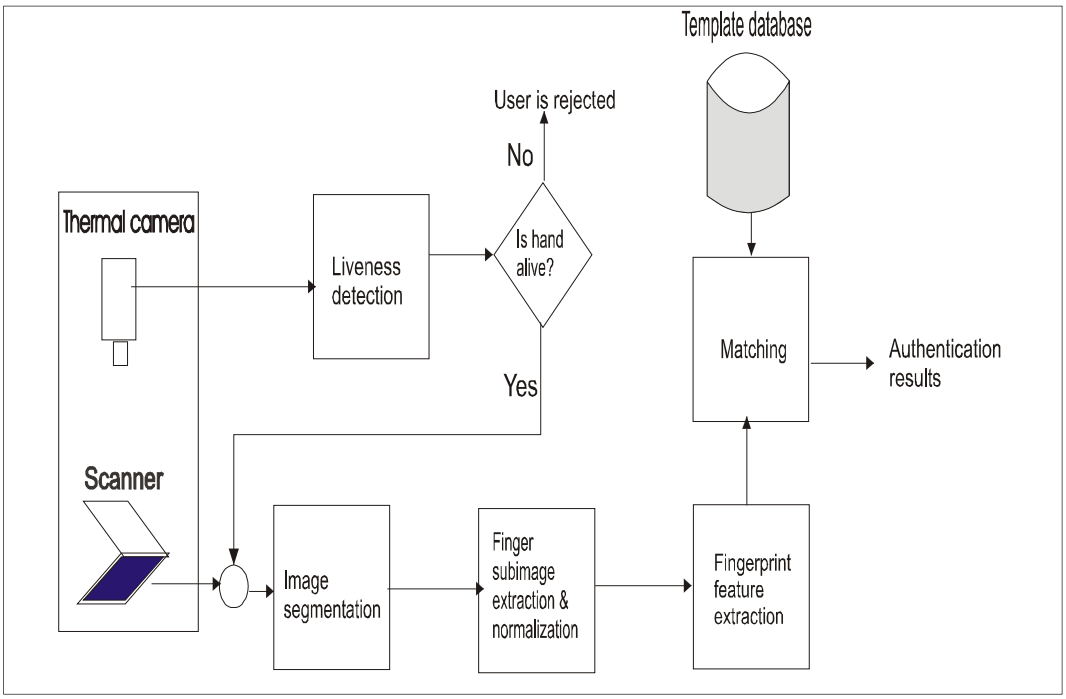

Figure 5: Biometric authentication system

For authentication to take place, a number of activities have to be undertaken by the system. These include fingerprint processing, which involves fingerprint scanning, minutiae extraction; de-noising, normalisation, binarisation and low pass filtering processes. This is followed by biometric enrollment and matching. In the enrollment stage, the individual's biometric samples are acquired, registered and stored for the first time as the true unaltered identity of the said person for future reference. In biometric matching, identification and authentication is performed.

Figure 6: Positioning of thumb and the small finger in gripping mouse

4.0 Recommendations

4.1 Algorithms

For the proposed biometric mouse, we recommend the use of the most appropriate algorithms that would achieve maximum security without compromising on the speed of processing since this is a routine task that shall be repeated several times and we do not wish to slow down the system. The algorithms should therefore be able to achieve the following technical capabilities:

(i) Detection of fake fingers - through aliveness detection.
(ii) Immediate and quick Fingerprint capturing.
(iii) Fingerprint image processing (fingerprint analysis and minutiae detection).
(iv) Elimination of noise (enhance quality for both dry and wet fingerprints).
(v) Fingerprint matching (1:1, 1:n).
(vi) Presentation of search/match report to administrator and audit trail system.
(vii) Storage of such report as appropriate in a database.

We strongly recommend the Delaunay triangulation algorithm, which is one of the most effective minutiae-based algorithm in accuracy and time management. This is a triangulation of the minutiae such that for each triangle of the triangulation, the circumcircle of that triangle is empty of any other minutiae. The algorithm allows for choosing of minutiae groups (i.e., triangles) during indexing, preserves index selectivity, reduces memory requirements without sacrificing recognition accuracy, and improves recognition time. Assuming N minutiae per fingerprint on average, the proposed approach considers only O(N) minutiae triangles during indexing or recognition as compared to $O(N^3)$, the number of triangles usually considered by other approaches. Besides their small number, the minutiae triangles we used for indexing have good discrimination power since, among all possible minutiae triangles, they are the only ones satisfying the properties of the Delaunay triangulation. One of the major strength of the Delaunay triangulation is that it can be computed efficiently in O(NlogN) time. The proposed approach has been tested on a database of 300 fingerprints (10 fingerprints from 30 persons), demonstrating good performance (Bebis *et al.,* 1999)

4.2 Handedness

For the best results and accuracy, the scanner should be created as a right hand or left hand specific, allowing the users to acquire the mouse that would best suit them. Creating some of the mice with the scanner at the right hand side and others on the left hand side would achieve this. This allows maximum contact without taking chances.

A possible alternative to the handedness question could be achieved by a study of mouse ergonomics with a focus on the way the hand grips a mouse. According to the American patent for Ergonomic Computer Mouse (U.S. Pat. No. 5,726,683 1998) 'a mouse is gripped with the ring and little finger on one side of the mouse opposing the thumb on the opposite face. The index and middle finger are curved over the top and front face of the mouse where the one or more buttons are located' (Hedge, 1999). During this research, we experimented with ten right hand and ten left hand users and established that the position held by the thumb of the left hand user is approximately the same position held by the small finger of the left handed person. By drawing a straight line linking the tips of both the thumb and the small fingers across the mouse as shown in Figure 6, the experiment showed that the position is the same and thus the scanner placed on one side could be used to capture the print of either the thumb or the small finger, and be used with equal success. This however requires further research mainly on ergonomics.

4.3 Further Research

In this research, we have discussed the development of a fulltime biometric mouse that would ensure continuous authentication of the users, based on fingerprint identification and specifically based on the minutiae extraction and matching. The biometric scanner is located strategically to achieve maximum contact with the thumb while ensuring minimum strain possible. The success of this proposed system is based on the assumption that the user is physically and physiologically capable of holding and working with a mouse, and has a functional thumb capable of authenticating, and that his/her fingerprints are existent and not damaged as in the cases of severe burns. In this case, however, we recommend further research that would help bring on board such persons whose thumbprints may have been damaged, the disabled and those with missing thumbs all together in order to enjoin them in the continuous biometric authentication. We also recommend further and thorough research on mouse ergonomics with the aim of establishing the proportionality of the thumb-small finger placement and possibility of their sharing a common scanner with right-left hand interchange. Another area for further research is on improvement of algorithms used in order to lessen the systems load, increase the speed and maintain accuracy to the acceptable threshold.

5.0 Conclusion

Fulltime authentication is of critical need in the world today and as electronic transactions increase and the Internet continues to revolutionise the way we conduct our day-to-day operations in increasing areas of our lives. Crime rate has also increased, with sharp and well-trained criminals taking advantage of the vulnerable infrastructures not only to frustrate users but also con them of their property. The fulltime biometric mouse becomes

an effective tool for ensuring confidence that one can with a high degree of certainty rest assured that the transaction performed through the Internet or any network was with the intended person and not an imposter. Such considerations need be explored further to include other devices such as keyboards as well as special keys on an ATM terminal.

References

Ahmed A., Traore I. (2005). Detecting Computer Intrusions Using Behavioral Biometrics, Department of Electrical and Computer Engineering, University of Victoria, Canada.

Bebis G., Deaconu T and Georgiopoulos M. (1999). Information Intelligence and Systems, 1999. Proceedings. 1999 International Conference on Volume, Issue , 1999 pp 452- 459 Digital Object Identifier 10.1109/ICIIS.1999.810315

Eusebi C., Gilga C., John D. and Maisonave A. (2008). A Data Mining Study of Mouse Movement, Stylometry, and Keystroke Biometric Data, Proc. CSIS Research Day, Pace Univ., May 2008.

Hedge A., (1999), Ergonomic Guidelines for Arranging a Computer Workstation-10 Tips for Users; Ergonomics Research Laboratory, Cornell University--Department of Design & Environmental Analysis

Jain A.K., Hong L. and Bolle R.M. (1997): Online Fingerprint Verification, IEEE Trans. On PAMI, **19** (4), pp 302-313.

Jain A. K., Prabhakar S., and Hong L. (1999). A multichannel approach to fingerprint classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, **21(**4) pp 348-359, 1999.

Kaklauskas A., Zavadskas E. K., Seniut M., Krutinis M., G. Dzemyda, S. Ivanikovas, Stankevič V., Šimkevičius Č., Jaruševičius A. (2008). Web-Based Biometric Mouse Decision Support System For User's Emotional and Labour Productivity Analysis. Institute of Internet and Intelligent Technologies, Vilnius Gediminas Technical University, Vilnius, Lithuania

Koreman J., Morris A. C., Wu D., Jassim S. A., (2006): Multi-modal Biometrics Authentication on the Securephone PDA, in Proc. Second Workshop on Multimodal User Authentication, Toulouse, France, May 2006.

Liu J., Yu F. R, Chung-Horng L and Tang Helen (2007). Optimal Biometric-Based Continuous Authentication in Mobile Ad hoc Networks; Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada; Defense R&D Canada - Ottawa, ON, Canada; IEEE Conference on WIMOB 2007.

Maio D., Maltoni D., Jain A. K., and Prabhakar S. (2003). Handbook of Fingerprint Recognition. Springer Verlag.

Pankanti S., Prabhakar S., and Jain A. K. (2002) On the individuality of fingerprints. Transactions on PAMI, **24(**8), pp 1010–1025.

Ribaric Slobodan and Fratric Ivan (2005), An Online Biometric Authentication System Based On Eigenfingers And Finger-Geometry, Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia

Sim T., Zhang S., Janakriaman R. and Kumar S. (2007) "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Patten Analysis and Machine Intelligence, **29**(4), pp. 687-700, Apr. 2007.

Pseudo-code Algorithm for Full time Biometric Mouse
Continued usage case

/ This section will be executed on the events to be monitored. The events may be major events like Save, Open, Close, Search, move to new page, new transaction, print etc and an initial user is already logged to the system*/*

On event

Activate Camera/Scanner

Set Attempt = 1

If Attempt <= 3

Verify aliveness of the finger/thumb

If alive

Capture and extract User print sample

Compare Sample print with the Active user's template in the database

//To verify the user is the same

If sample is the same

Allow user to continue

Execute command

Else *//Sample not the same*

*/*The sample print is not the same as that of the active user, could be of a superior user, inferior user or user with same access privileges. */*

Check if sample exist in the database

If sample found

Request authorization of initial user

Set Attempt1 = 1

If Attempt1 <= 3

Verify liveness of the finger/thumb

```
                    If alive
                    Capture and extract User print sample
                    Verify authenticity of initial user
                        If User is authentic //Initial user
                            Accept commands and proceed
                        Else //If not authorized by initial use.
                            Save active users work and close
                            Log off active user
                            Log in new user and load a new form
                        End if
                    Else //Not alive
                        Reject sample print
                    End if
                Else //Attempt1 more than three times
                    Save the active users work and close
                    Restrict any other attempt and terminate the application.
                End if
            Else // Sample not found
                Save the active users work and close
                Register the user
                Store template temporarily
                Await activation by administrator
            End if
        End if
```

Else *//not Alive*

Reject sample print

End if

Else *//Attempt more than three times*

Save the active users work and close

Restrict any other attempt and terminate the application

End if

Continuous Usage flow chart