Fine Tuning Graphical Authentication System

Bhanwase Komal S.[1], Bhosale Anjali B.[2], Pophale Swapnali S.[3] Prof.P.S.Togrikar.[4]

[1,2,3] B.E,Dept of E&tc Engineering,s.b.patil college,Indapur,Maharashtra,India

[4]Prof.P.S.Togrikar, Dept of E&tc Engineering,s.b.patil college,Indapur,Maharashtra,India

---

Abstract – Traditional user authentication system have several problem like user friendly, not easy to memorize and security. Generally people use to create the security password for their own ease as it is difficult to remember strong password for long period. Therefore people normally used to choose the passwords which are easily memorable to them which finally creates the security issues.

In this paper, a full proof authentication system is proposed using "Fine Tuning Graphical Authentication System". This is implemented using hardware technology i.e. Arduino board for providing highest security & fast access.

Key Words: *Arduino board, Graphical Authentication System.*

1.INTRODUCTION

Use of the text password that is alphanumeric password is difficult to remember for the user. There are some weaknesses of text password. Many of the deficiencies of text password arises from the human memory numerous cognitive and psychological studies have revealed that people perform for better when remembering picture rather than words as saying goes, a picture is worth a thousand words. This is an inspirational research into the design of graphical password system in security.

1.1 Literature Survey:

1.NAPTune: Fine Tuning Graphical Authentication

Author: Rohit Ashok Khot, Kannan Srinathan, Rutuja Ashok Khot,

Graphical Password are consider to be a memorable and secure: alternative to text passwords. Users of different systems, authenticate themselves by identifying a subset of images from the set of displayed images. It is aimed to work as a cubed recognition based graphical authentication scheme that allows users to choose both text as well as images as their password with the same interaction and underlying design. Conclusion of the study are encouraging which indicates that our proposed design is potentially secure and usable method of authentication.

1.2 Methodology:

1) Implementation Diagram:

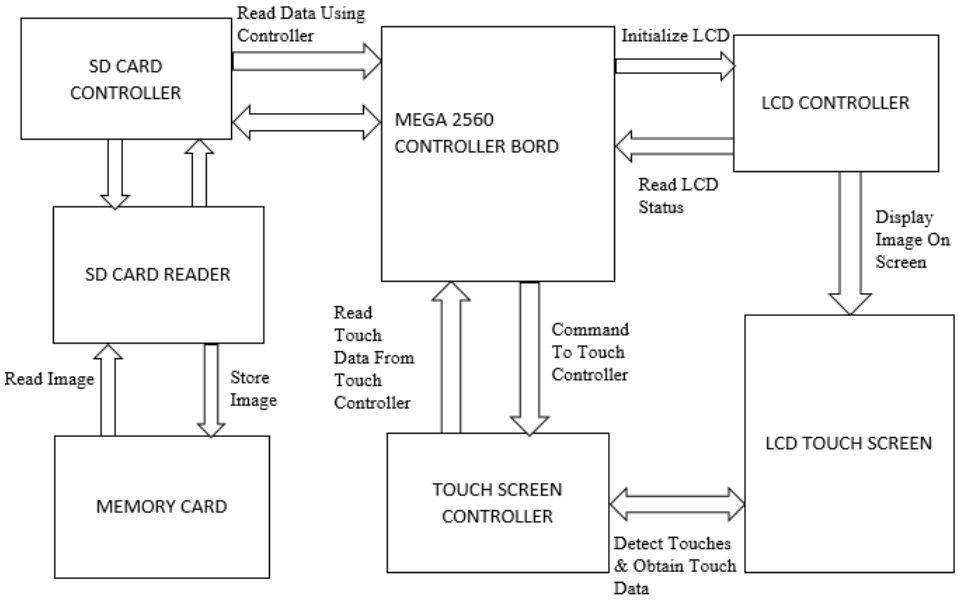

Fig. Block Diagram of project.

Description:

The touch screen controller used to detect touch from user and gives input to the ATMEGA 2560 Microcontroller .LCD Display controller is SSD1289 reads and write data on a display i.e., Image. That image is provided to LCD controller. The touch controller and display controller provide input to the microcontroller. The input is in the form of the signals that microcontroller understands.

ATMEGA 2560 Microcontroller will initialize LCD. LCD will read the status and send to controller. ATMEGA2560 Microcontroller sends command to touch controller and it will read touch data i.e. Image. SD card controller will provide data to microcontroller, similarly other two controller. The data provided from SD card is nothing but Image. Image is stored in BMP (BIT map IMAGE) Format.

2. Flow Chart:

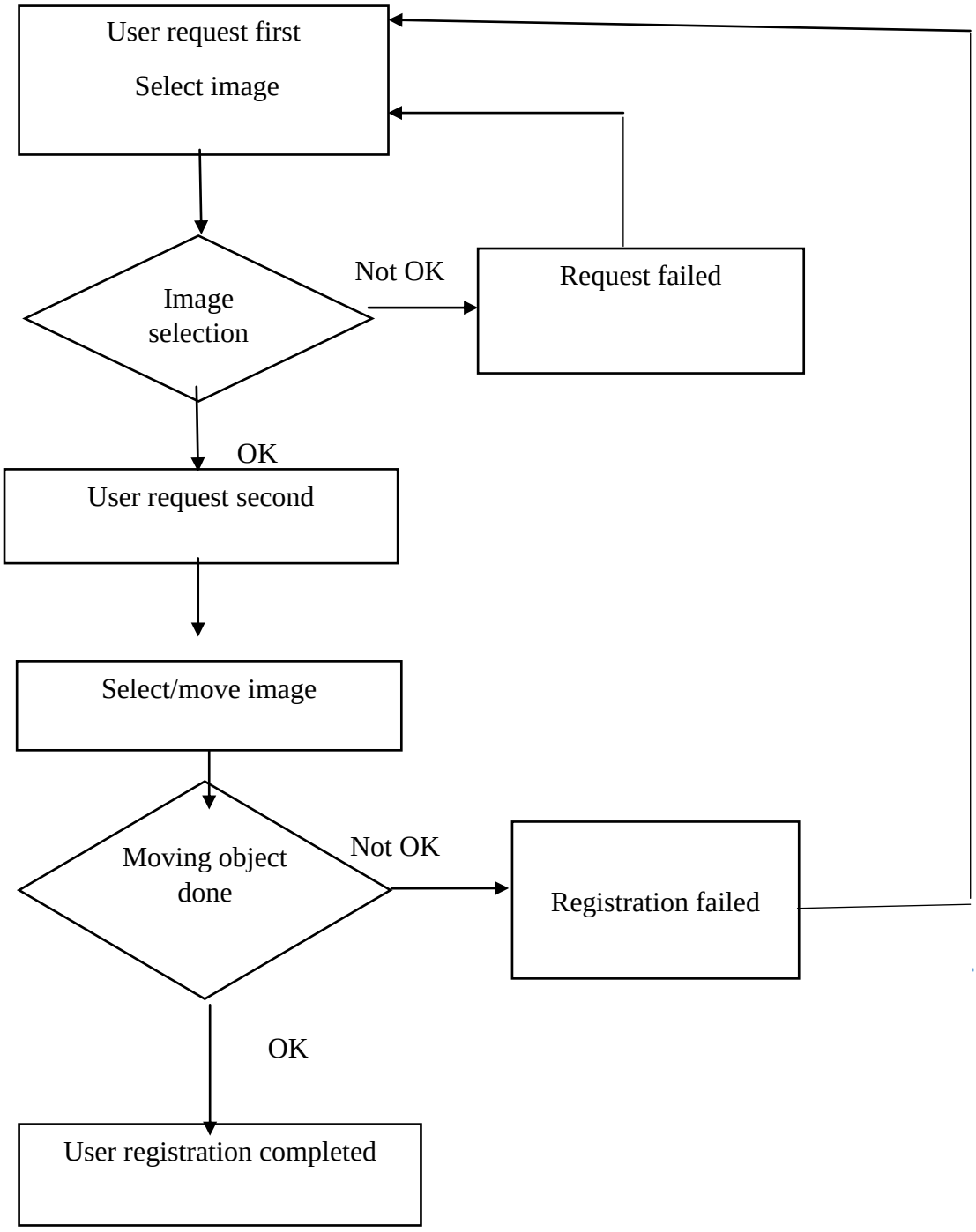

Fig.5.1 Password Registration module

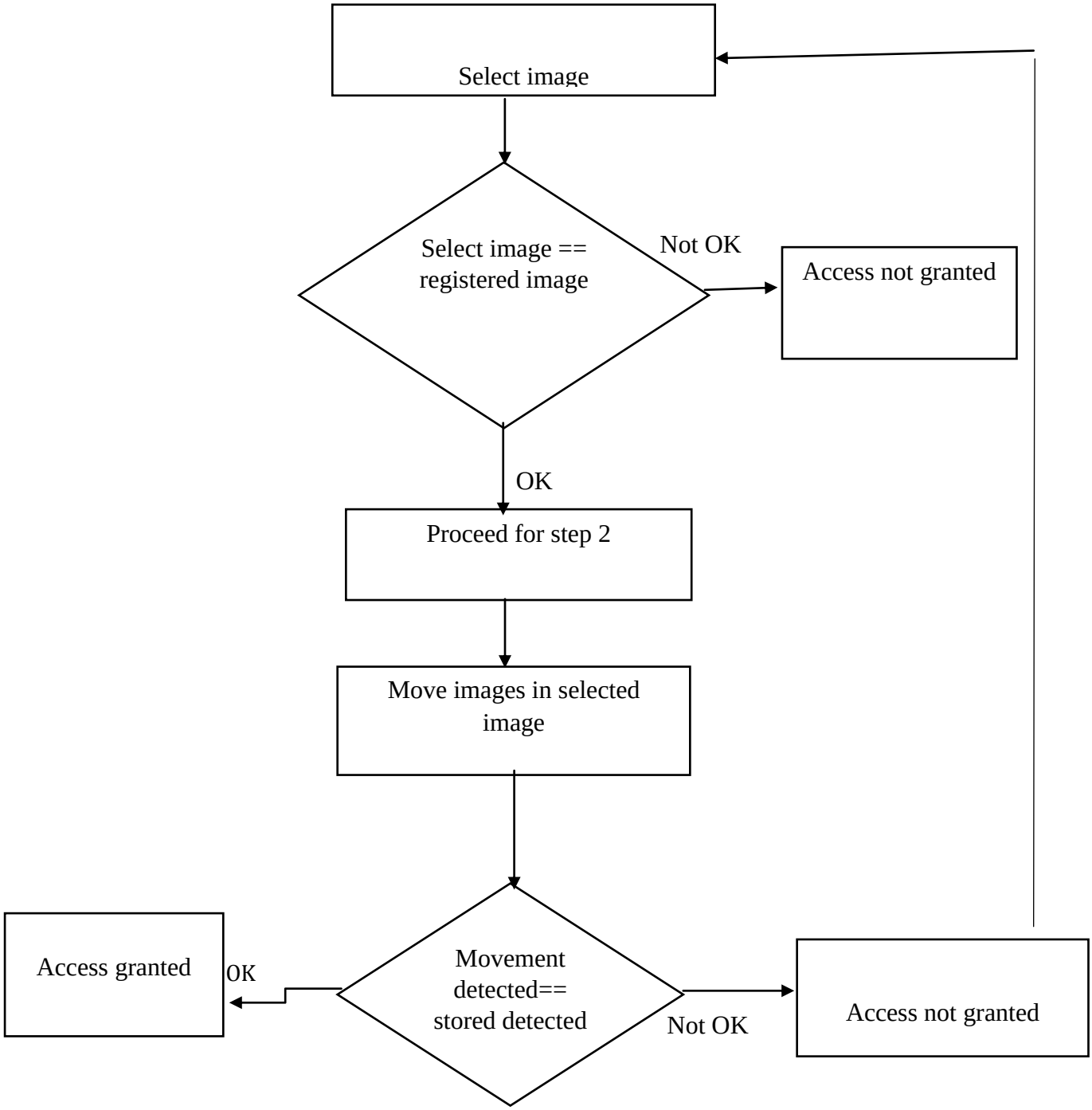

Fig.5.2. Password Authentication module .

Advantages:

1. Graphical passwords can be remembered easily since human brain is very efficient to remember the graphical password.

2. We are using many combinations of images so it is very difficult to hacker to guess.

3. Used to prevent unauthorized access.

Applications:

1. Web driven applications

2. Mobile lock system

3. Folder lock system

4. Banking sectors

5 .Governmental sector

6. Defense services

7. Chemical industries

Result:

User Registration Steps:

Step 1:Enter 4 Digit Numerical Password.

Step 2: Select any one image of these 4.

Step 3: Select any 4 different images out of 10 different images.

Step 4 : Move selected different images in main images **.**

Step 5: Registration Successfully.

User Authentication steps:

Step 1:Enter the register Numerical Password.

Step 2: Select register one image.

Step 3: Select 4 images in sequence which is registraterd.

Step 4 : Move these images as per registration **.**

Step 5: Login Successfully.

CONCLUSION

The graphical password is an alternative authentication system, which can be based on a selection of graphical images as the password to access to the system. It is useful to solve the problem of remembering the complex passwords in textual passwords.

The viability of this system in terms of accuracy (No of successful login), Efficiency (Time required to login), predictability (password strength) and user satisfaction.

Its strength lies in its simplicity and unique graphical way of working. We designed and tested a data server security prototype.

REFERENCES

[I] B .. Malek, M: Orozco, and A. EI Saddik, "Novel shoulder-surfing resistant haptic-based graphical password," in *Proc. EuroHaptics* 2006. '

[2] I.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang, "Shoulder-surfingproof graphical password authentication scheme," International journal] of information security, vol. 13, pp. 245-254,2014.

[3] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in Proceedings of the Seventh Symposium on Usable Privacy and Security, 2011, p. 6.

[4] NAPTune: Fine Tuning Graphical Authentication