INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

THE IMPLEMENTATION ON THE PROCESS OF AUTHENTICATION IN DIFFERENT AUTHENTICATORS BY USING IMAGE SELECTION TECHNIQUE

IMAGES INTO ALPHA-NUMERIC-SYMBOLIC CONVERSION WHILE AUTHENTICATION

ZEESHAN. I. KHAN[1], DR VIJAY. S. GULHANE[2]

1. Student of Master of Engineering in (CSE), PRMIT&R college of Engineering and Technology, Amravati, India.
2. Assistant professor Department of (CSE), PRMIT&R College of Engineering and Technology, Amravati, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: The technology users have to face an authentication process everywhere, then it might be an option of Internet banking, ATM, a social networking profile or simply an email account. The authentication is compulsory for maintaining the level of privacy as well as security. The purpose of the title is to describe a mechanism for authenticating a user at any authenticator by using a visual login technique called as Image Password which will be converted into alpha-numeric-symbolic textual password for database storage to increase processing speed at the time of authentication. The given technique allows the user to navigate in the panel containing large number of images and interacts or selects a set of images which can be registered inside a memory. The sequence of selection or interaction by the user towards the set of images inside the panel constructs the user's image password. The recognition based image selection authentication technique can be proved as a convenient as well as easy to remember for the user in the process of authentication.

Keywords: Authentication, Image, Alphanumeric, Pattern Matching

Corresponding Author: MR. ZEESHAN. I. KHAN

Access Online On:

www.ijpret.com

How to Cite This Article:

Zeeshan I. Khan, IJPRET, 2015; Volume 3 (9): 1489-1498

PAPER-QR CODE

INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. Authentication is the process of actually confirming that identity whereas the **Authenticators** is a system or a program usually running somewhere on the computer network, that takes care of authentication.

An **image** is an artifact that depicts or records visual perception, for example a two-dimensional **picture** that has a similar appearance to some subject – usually a physical object or a person, thus providing a depiction of it.

Using a 2-D image as a login technique on the different authenticators can be proved more superior to a traditional textual based authentication technique. Adequate user authentication is a persistent problem with the different authenticators, which tend to be highly personal and at the fringes of an organization's influence and also motivating users to enable simple PIN or password mechanisms and periodically update their authentication information is a constant struggle. It describes a general-purpose mechanism for authenticating a user on any device using an image based login technique called as *Image password*. The underlying rationale is that the image recall is an easy and natural way for users to authenticate, removing a serious barrier to compliance with organizational policy. Features of image password include style dependent image selection, password reuse, which overcome a number of problems with knowledge-based authentication for authenticators. Though authenticators are mentioned, it can be a computer system or a handheld device or ATM which simply supports a 2-D image.

- Analysis of Problem

What is a password?? It tells us about a string of characters that allows access to a computer, interface, or system.

These strings of Characters are creating a problem now a days of forgetting it when we have many accounts and all are having different passwords.

For any authentication mechanism to gain user acceptance, it must be convenient to use and match the capabilities of the device. Difficulties due to cumbersome attachments, slow performance, or error-prone user interfaces are typically not tolerated. The aim then is to devise authentication mechanisms for such authenticators that are well suited to the typical interfaces and capabilities supported by such devices.

From an authentication perspective, several issues loom over the use of such device, including the following items:

- The basic problem of textual password is the lapse of memory in that case where you have many accounts and all containing different passwords.
- Various rules we must have to follow while setting up the password like alphanumeric or symbolic character must be included in it.
- The password which you had set will be expired periodically giving an overhead to set and remember a new complex password.
- Use of PIN instead of password, decreases its level of security.
- Use of biometrics is also a costlier technique and also gives pitfalls in the case of pirated fingerprints.
- Proposed Work and Objectives

The aim of the work is to give such type of login technique for the users which is more convenient, easy to remember, fast response mechanism by using different 2-D images as a primary data. The image based login technique authentication mechanism has two distinct parts: the initial password enrollment and subsequent password verification. During enrollment, a user selects a theme identifying the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used to derive the associated password. At the time of authentication process, the user selects few images which he had decided for a password. After a successful authentication, the user may change the password, selecting a new sequence and/or theme. Picture Password offers benefits over PINs and textual passwords, especially for the visually inclined user. However, instead of having to memorize and enter a string of random-like alphanumeric characters, a sequence of thumbnail images must be selected and retained. Experimental results suggest that human visual memory is well suited to such visual and cognitive tasks [David Melcher| Year 2001] and [Alvin Goldstein and June Chance, Visual Cognition| Year 1971]. Moreover, an image sequence that has some meaning to the individual user (e.g. a sequence of activities done by user after entering into his office or a bedroom) can be used.

- *The Objectives of the proposed system are:*

1) To create such authentication scheme which contains the images as a primary data which will be used to authenticate the user.

2) A panel of images will be constructed and presented in front of the user to select the set of images of his choice which will be registered as a password.

3) Alphanumeric letters will be generated along with the images which will be stored at the back end for verification to save the processing time.

Note: All or few given objectives will be tried to accomplish the project.

- *Methodology*

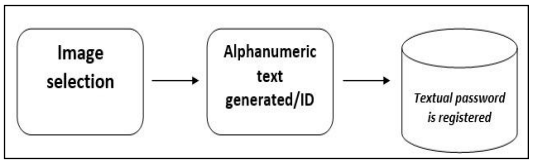
The process of authentication will contain some few steps:

Phase 1: Initial Password Enrollment

a) Selection of few images from the given set of images.

b) While selecting an image, simultaneously an alphanumeric textual based password/ID is automatically generated depending on that image.

c) Registering the sequence and the alphanumeric password which is stored behind that image selection process.



Phase 2: Password Verification/Authentication

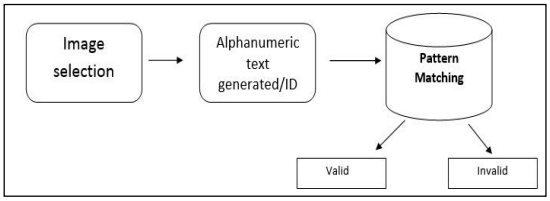
a) A Panel containing images is displayed on the screen from which user has to encounter/click the same set images and the sequence which have already enrolled in the phase 1.

b) While selecting an image, simultaneously an alphanumeric textual based password is automatically generated again depending on that image.

c) Verification for a valid password will be done on the comparison of alphanumeric text which is generated along with the image selection.

d) The comparison of alphanumeric text will be done by any efficient pattern matching algorithm/process.

e) If the alphanumeric password is matched then the user is authenticated else proved invalid.



IV IMPLEMENTATION

The given idea is implemented as a desktop application by using asp.net and C# module to check the nature and time complexity of the application containing such a large set of images.

The application is made with the help of some important files like,

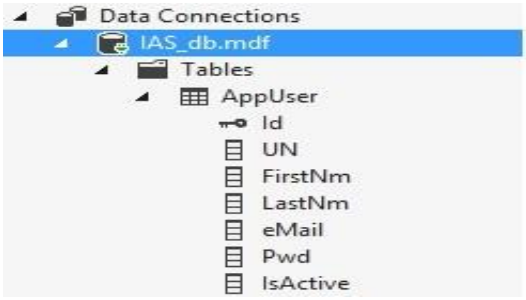
1) Initial_Form.cs:- At Front end , It manage the process of new registration as well as login process and proceed to the image panel for password selection and At Back end , It stores the user information as well as selected images in terms of alpha-numeric-symbolic textual password in data base.

2) Image_Panels.cs:- After the completion of first phase, this phase arrives in which, At Front end, An image selection and simultaneous conversion into alpha-numeric-symbolic accomplished and, At Back end, storing/verifying the user's selected images in/from the database.

3) Finish_Authentiation_Phase.cs:- At Front end, a finish button will ask to finish authentication and at back end, it performs pattern matching process to check whether the entered password is valid or invalid.

4) Database_connectiviy.cs:- This file acts as a middleware which provides the connectivity between the application and database, to store the password which is nothing but the conversion of images into alpha-numeric-symbolic textual password.

5) Database structure:- It stores the textual information only while all the images are stored in normal file storage and only the image id is stored in the database.



V Flow of Application

A. Home Page having Register / Login Options

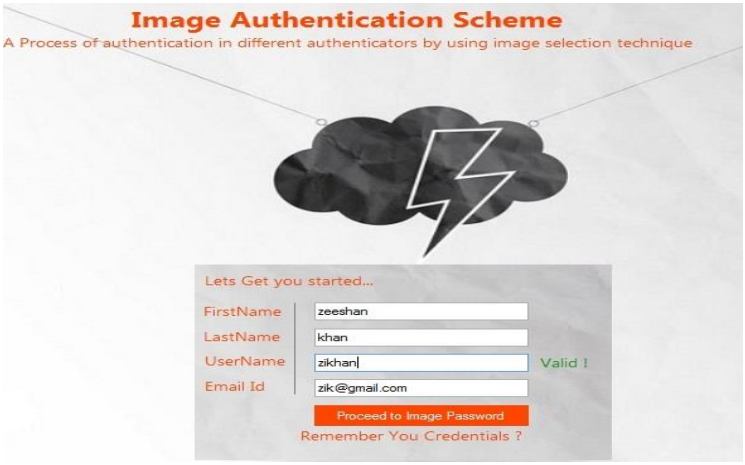
Registration Process collects,

- ✓ First Name
- ✓ Last Name
- ✓ User Name
- ✓ Email ID

Login Process collects,

- ✓ Email ID

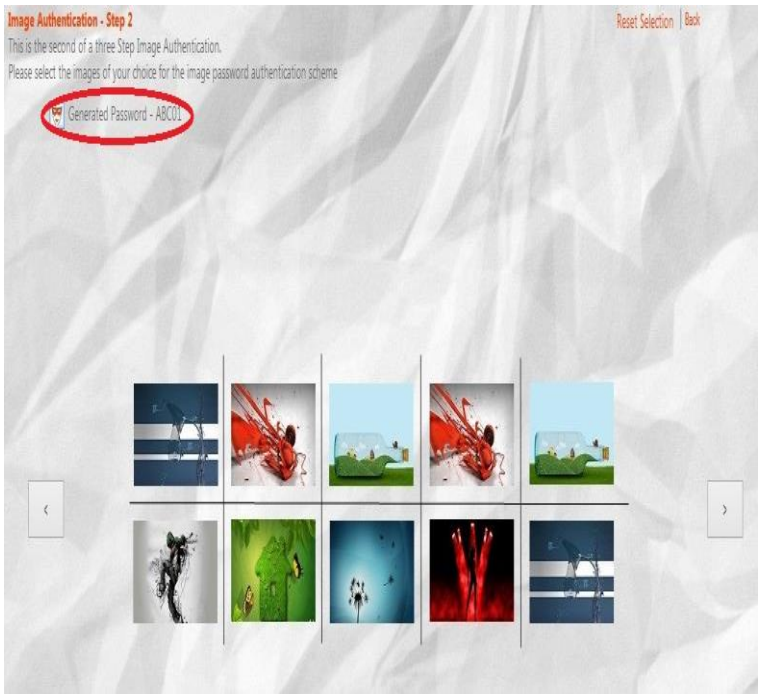
B. Registration Process



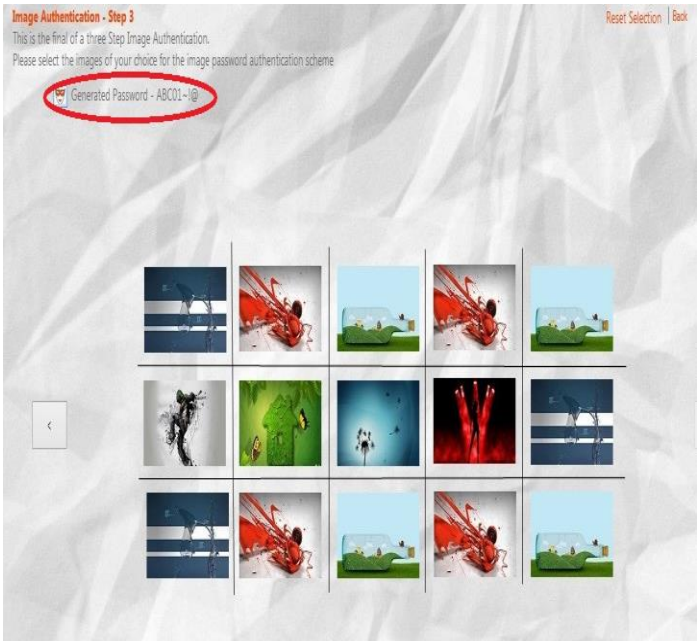
✓ After complete and successful registration, it proceeds towards image password

C. 1st Panel containing 26 Images for 26 Alphabets

D. 2nd Panel containing 10 Images for 10 Numbers



E. 3rd Panel containing 15 Images for 15 Symbols



✓ The symbols (images) can be extended as per requirement to apply maximum complexity)

F. Validation Panel

✓ It shows the status of the entered password form the above three panels.

V Result analysis

i. It helps the user to remember the set of images easily rather than alpha numeric symbolic passwords.

ii. Time consumption for authentication is lower since the simple pattern matching algorithm is used behind the whole process.

iii. The authentication time is quick when user already the whole process of authentication.

V References

1. [Alvin Goldstein and June Chance, Visual Cognition| Year 1971] for Complex Configurations, Perception and Psychophysics, 9, 1971, pp. 237-241.

2. [Deborah Nelson, Kim-Phuong L. Vu | Year 2010]: "Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords" in Computers in human behavior [26 (2010) 705–715].

3. [David Melcher| Year 2001] for the persistence of visual memory for scenes, Nature, 412(6845), p. 401(July 2001).

4. [Mr. A. A. Shinde , Ms. S.R. Chokhandre, Mrs. R.C. Roychaudhary, Mrs. S. S. Telrandhe, Mrs. C. N. Rokde|Year 2014] for "A Survey: Login with Image Based Password Authentication" in International Journal of Advanced Research in Computer Science and Software Engineering in 2014 [ISSN: 2277 128X].

5. [Rachna Dhamija and Adrian Perrig | August 2000] Deja Vu: A User Study Using Images for Authentication, Proceedings of the 9th Usenix Security Symposium [Dha00].

6. [Ronak B.Singh|Year 2013] for "Three-Dimensional Password System Implementation Technique" in the International Journal Of Pure And Applied Research In Engineering And Technology [ISSN: 2319-507X].

7. [Ting-Yi Changa, Cheng-Jung Tsaib, Jyun-Hao Lina|Year 2012]:"A graphical-based password keystroke dynamic authentication system for touchscreen handheld mobile devices" in the journal of System and Software [85 (2012) 1157– 1165].

8. [Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers, Ryan Swanstrom | Year 2003] "Picture Password: A Visual Login Technique for Mobile Devices" in National Institute of Standards and Technology [NISTIR 7030].