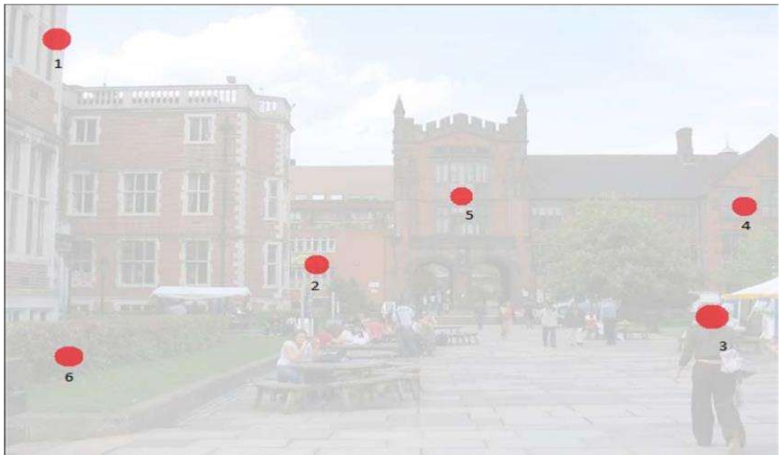
Graphical Password for Authentication

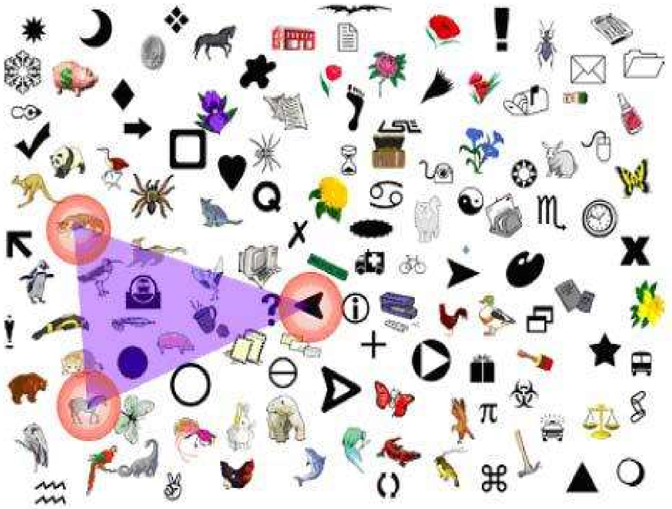
P.Mounika, K.Divya Kalyani, S.Venkata Lakshmi
Assistant Professor, Dadi Institute of Engineering and Technology
reddymounika010593@gmail.com, divyakalyanik@diet.edu.in
venkatalakshmisalapu@gmail.com

Abstract

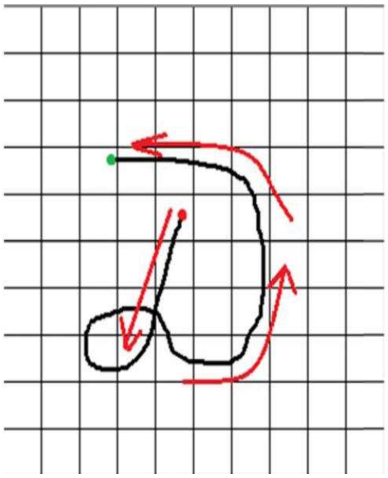
The usage of alphanumeric usernames and passwords is the most popular computer authentication technique.It has been established that this approach has serious disadvantages.Users frequently choose passwords that are simple to guess, for instance. On the other side, a password that is difficult to guess is frequently also difficult to remember. Some researchers have created authentication techniques that employ images as passwords to solve this issue.Humans are better at remembering visuals than text passwords, which have memorable passwords that are simple for hackers to guess but harder for users to remember.The potential impact of a single account being compromised is increased by using the same password on multiple accounts.Costly and inconvenient biometric authentication methods exist.Privacy concerns arise since biometric data is an integral element of an individual's identification.A graphical password is an authentication method that asks the user to choose from a set of images that are given to them in a graphical user interface (GUI) in a particular order). The graphical-password strategy is sometimes referred to as graphicaluser authentication (GUA) for this reason. It can be applied to mobile devices, ATMs, and web log-in applications. Two groups,By recognising and identifying the photographs he chose throughout the registration process, a user authenticates themselves using recognition-based techniques after being shown a series of images. Techniques Based on Recall,a user is requested to duplicate anything that he previously created or chose while registering. Password is a collection of places on large photos. Here, the user must choose a background image from the provided library and provide control points for the image.The points will be utilised in order to authenticate.The user must do a right click on each point in the correct order during authentication.

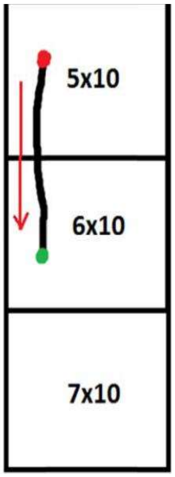


An array of pass-objects (pre-selected by the user) are displayed by the system using recognition-based techniques, the Sobrado and Birget scheme. The user clicks inside the convex hull bounded bypass-objects.Space for password: N!/K(N-K)!There are N total picture objects. Pre-registered object count (K).

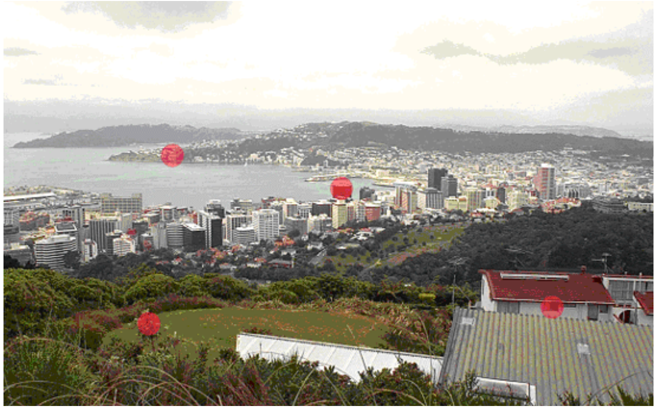


DAS-Draw A Secret: Recall Based Techniques Each field in the matrix with dimensions n*n has its own position due to the input plane's breakdown on fields. By creating a password, the user can access many areas.User must pass through the same field and replicate their drawing from the creation phase as closely as possible during authentication.



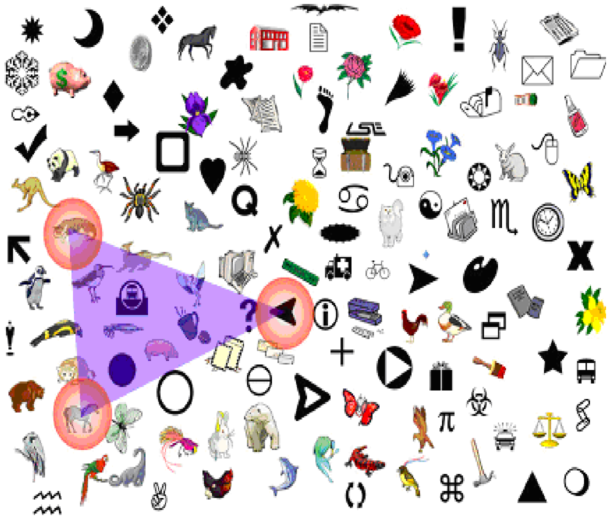


Comparison of Graphical & Alphanumeric Passwords Alpha-numeric password recommendations that are frequently used include: There should be at least 8 characters in the password. The user's last name or birth date, for example, should not be used as the password. The user should ideally mix capital and lowercase letters, as well as numerals. illustrative passwords,The actions the user does on a picture make up the password.Such passwords are more secure and simpler to remember.The user selected these areas when he or she constructed the password using a simple graphical password scheme. The four locales are chosen at random, although the user will select locations that are simple for him or her to recall. The user can upload personal images to create graphical passwords. Additionally, for increased security, more than four areas is arbitrary, but the user will select locations that are simple for him or her to recall. The user can upload personal images to create graphical passwords. Additionally, more than four click points could be selected for increased security.

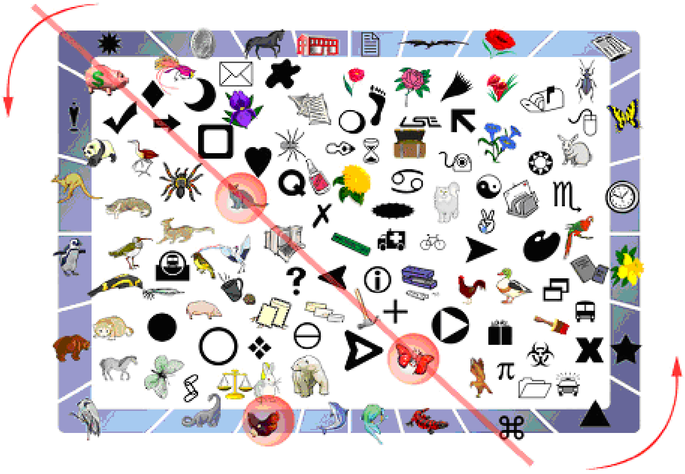


Advantages of graphic passwords include methods for creating more approachable passwords.The system's security at this place is really high.Here, we make use of a progression of selectable graphics on different screen pages.Dictionary attacks cannot succeed.Drawbacks include a lengthy password registration and login process, as well as shoulder surfing.

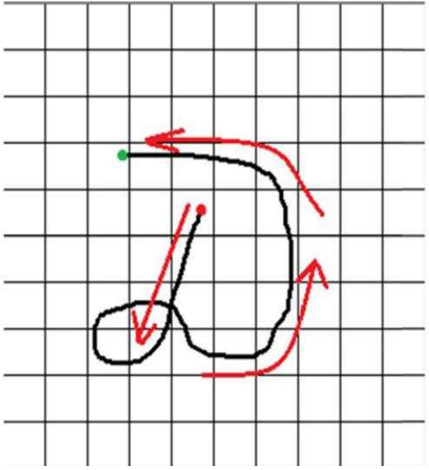
Fix for the shoulder surfing issue 1 Triangle Plan

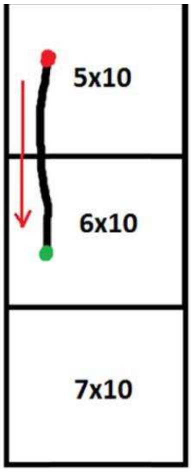


(2) Movable Frame Scheme



Biometric authentications and text-based alphanumeric passwords are both alternatives to graphic passwords.It satisfies the two opposing objectives of being both simple to recall and challenging to guess.The shoulder surfing issue is resolved, making the password system more safe & simple. More security can be attained by using additional unique geometric designs, such as triangles and movable frames.The classic attack techniques, such as brute force search, dictionary attack, or spyware, are typically more difficult to crack than graphical passwords.





Alpha-Numeric vs. Graphical Password ComparisonAlpha-numeric password recommendations that are frequently used include: There should be at least 8 characters in the password. The user's last name or birth date, for example, should not be used as the password. The user should ideally mix capital and lowercase letters, as well as numerals. The password for a graphic password is made up of some user-performed operations on a picture.Such passwords are more secure and simpler to remember.

Requried References