IPHV2I30002X

International Journal Of Advanced Research and Innovation -Vol.II, Issue .3

ISSN Online: 2319 – 9253

Print: 2319 – 9245

INTERACTIVE IMAGE RETRIEVAL USING BIASED MAXIMUM MARGIN & SEMI SUPERVISED ANALYSIS

[1]Dilip Venkata Kumar.V, [2]Rajesh Nichenametla

1. **Associate Professor, St.John's College Of Engineering &Technology,Yemmiganur, A.P**
2. **Assistant Professor, Sri Kottam Tulasi Reddy Memorial College Of Engineering,Mahabubnagar.**

ABSTRACT:

Information retrieval is minimum need to every system, lot of considerable changes improvements were occurred in this area and so many potential practical applications, content- based image retrieval (CBIR) has attracted substantial attention during the past few years. A variety of relevance feedback (RF) schemes have been developed as a powerful tool to bridge the semantic gap between low-level visual features and high-level semantic concepts, and thus to improve the performance of CBIR systems.

Among various RF approaches, support-vector-machine (SVM)-based RF is one of the most popular techniques in CBIR. Despite the success, directly using SVM as an RF scheme has two main drawbacks. First, it treats the positive and negative feedbacks equally, which is not appropriate since the two groups of training feedbacks have distinct properties. To utilize the information of unlabeled samples in the database, we introduced a Laplacian regularizer to the BMMA, which will lead to Semi BMMA for the SVM RF. Second, most of the SVM-based RF techniques do not take into account the unlabeled samples, although they are very helpful in constructing good classifier.

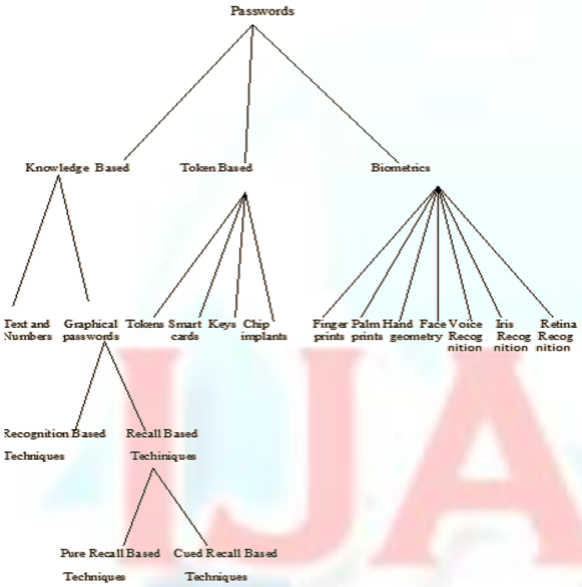
Key terms: Relevance Feedback, CBIR,SVM,BMMA

INTRODUCTION

Graphical passwords were first described by Blonder. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme.

EXISTING SYSTEM:

Existing approaches to Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. Despite the vulnerabilities, it’s the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks.



Disadvantage:

1. The strong system-assigned passwords are difficult for users to remember.

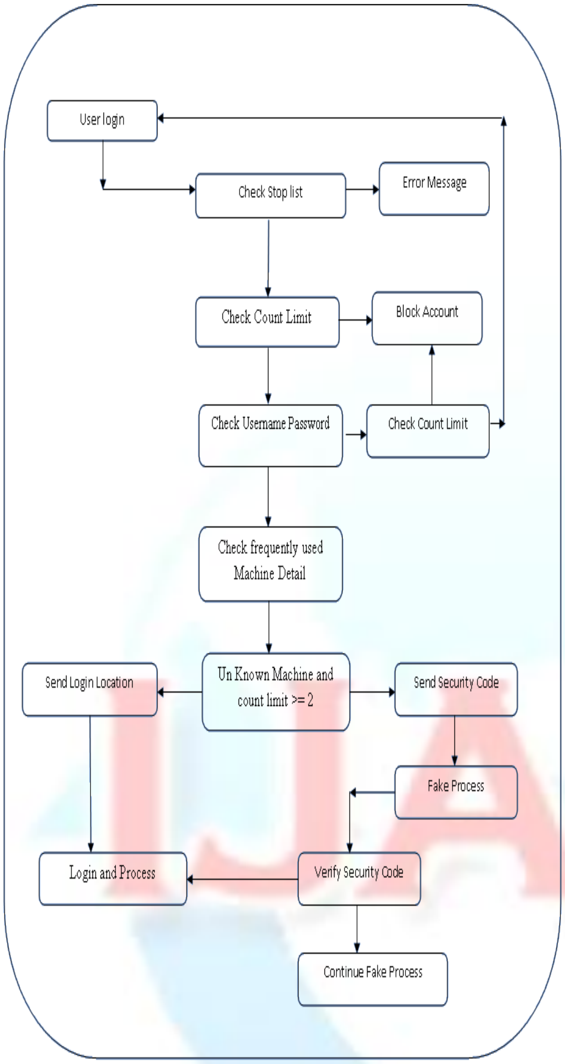
PROPOSED SYSTEM:

We propose is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. The proposed system work merges persuasive cued click points and password guessing resistant protocol. A major advantage of Persuasive cued

click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade‟s .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users.

Advantage:

1. Human brain is good in remembering picture than textual character.



MODULES

1. Pass Points Module.
2. Cued Click Points Module.
3. Persuasive Cued Click-Points Module.

Pass Points Module:

Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

Cued Click Points Module:

Cued Click Points (CCP) was developed as an alternative click based graphical password scheme where users select one point per image for five images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

Persuasive Cued Click- Points Module:

To address the issue of hotspots, Persuasive Cued Click Points (PCCP) was proposed. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

CONCLUSION:

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node bot nets.

REFERENCES

[1] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS , LNCS 4734, pp.359-374,Springer- Verlag Berlin Heidelberg 2007.

[2] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.

[3] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, „An association-based graphical password design resistant to shoulder surfing attack", International Conference on Multimedia and Expo (ICME), IEEE.2005

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of9th USENIX Security Symposium*, 2000.

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwes Instruction and Computing Symposium*, 2004.

[6] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin forUndergraduate Research*, vol. 4,2002.

[7] Sonia Chiasson, Alain Forget , Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIXSecurity Symposium*, 1999.

[9] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedingsof International conference on security andmanagement*. Las Vegas, NV, 2003.

[10] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communicationsof the ACM*, vol. 42, pp. 41-46, 1999.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIXSecurity Symposium*, 1999