INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CONTENT BASED DOCUMENT RETRIEVAL USING TEXT, COLOUR AND SHAPE IN ENHANCED ONLINE AUTHENTICATION USING VIRTUAL PASSWORD

[1]Ms. S. S. Desai, [2]Dattatraya.T

[1]Assistant, Professor, Computer science and Engineering, BLDEA'S College of Engineering.
[2]M.Tech 3rd SEM., Computer Science and Engineering, BLDEA'S College of Engineering.
Shreeja.cse@gmail.com, datta111@yahoo.co.in

Abstract: - A highly severe menace to any computing device is the impersonation of an authenticate user for Document Retrieval. The most frequent computer authentication scheme is to use alphanumerical usernames and passwords. But the textual passwords are prone to dictionary attacks, eves dropping, shoulder surfing and social engineering. As such, graphical passwords have been introduced as an alternative to the traditional authentication process. Though the graphical password schemes provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing. To address this problem, text can be used in combination with the colours and images to generate the session passwords, thereby making a stronger authentication means. In general, session passwords are those that can be used only once and for every new session, a new password is engendered. In this paper, we have proposed two authentication schemes for generating the session passwords which is identified as the primary level of authentication. Once the user has cleared the primary level, he is then allowed to deal with the secondary level of Authentication involving a graphical password scheme to retrieve Document Based on content, text, colour and shape. This method is most apposite to the PDAs besides other computing devices, as it is resistant to shoulder surfing. Document Retrieval system is a novel application for Searching and managing large scale document database. Document Based information Retrieval (DBIR) is a technique which uses visual contents of Document such as colour, shape and texture, etc. to search user required document from large scale document database according to user's requests in the form of a query document. Single feature represent only part of the document property so, to enhance the document retrieval effectively we are using multiple features such as colour, shape and texture to represent the whole document property. In this paper I have proposed an algorithm which incorporates all three features such as colour, shape and texture to give the advantages of various other algorithms to improve the accuracy and performance of retrieval of document. The accuracy of HSV colour space based colour histogram based matching gives better retrieval result. The speed of shape based retrieval can be enhanced by considering approximate shape rather than the exact shape. Grey Level Co-occurrence matrix (GLCM) is used to extract the texture features of the documents. The feature matching procedure is based on the Canberra distance.

Keywords*:* DBIR, Password, TBIR, CBIR

1. Introduction

The Authentication is the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is part of most online applications. Before a user can access its email account, it's online banking account or its favorite online shopping account, or Document. it has to identify and authenticate itself to the application and Database. The most common form of authentication is done through the use of passwords.

Internet usage and online applications are experiencing spectacular growth. Worldwide, there are over a billion Internet users at present. A big reason for the success of the Internet is the simplicity and that you can access the applications from anywhere. This growth in popularity has not gone unnoticed by the criminal element – the simplicity of the HTTP protocol makes it easy to steal and spoof identity. The business liability associated with protecting online information has increased significantly and this is an issue that must be addressed. Users with important accounts on the Internet face many kinds of attacks, e.g., a user ID and password can be stolen and misused. There are many reports on thefts on ATMs as well. The secure protocol SSL/TLS for transmitting private data over the web is well known in academic research, but most current commercial websites still rely on the relatively weak protection mechanism of user authentications via a plaintext password and user ID. Meanwhile, even though a password can be transferred via a secure channel, this authentication approach is still vulnerable to attacks as follows.

With the development of internet and multimedia devices, a huge amount of document has been used in many fields like Medical treatment, satellite data, still images repositories, digital forensics and surveillance system. Because of this reason, there is an on-going demand of systems that can store and retrieve documents in an effective way. Many Database storage and retrieval systems have been developed till now for catering these demands. The most common retrieval systems are Text Based Image Retrieval (TBIR) systems, where the search is based on automatic or manual annotation of information. A conventional TBIR searches the database for the similar text surrounding the document as given in the query string. The commonly used TBIR system is Google. However, it is sometimes difficult to express the whole visual content of information in words and TBIR may end up in producing irrelevant results. In addition annotation of document is not always correct and consumes a lot of time. For finding the alternative way of searching and overcoming the limitations imposed by TBIR systems more intuitive and user friendly content based image retrieval systems (CBIR) were developed. High retrieval efficiency and less computational complexity are the desired characteristics of CBIR systems. Content-based image retrieval (CBIR) [1] is a technique which uses visual contents such as colour, shape and texture for searching similar images from large scale image database according to user request in the form of query image. Colour, texture and shape features have been used for describing image content. Content-based image retrieval uses the visual contents of an image such as colour, shape, texture to represent and index the image. In typical content-based image retrieval systems shown in figure1, the visual contents of the images in the database are extracted and described by multi-dimensional feature vectors. The feature vectors of the images in the database form a feature database. To retrieve images, users provide the retrieval system with query image. The system then changes these examples into its internal representation of feature vectors. The similarities /distances between the feature vectors of the query image and those of the images in the database are then calculated and retrieval is performed with the aid of an indexing scheme. The indexing scheme provides an efficient way to search for the image database. Based on the same concept my new DBIR is designed.

1.1 Present Day Work

Passwords enjoy ubiquitous use for online authentication for Document Retrieval. Although many more secure (typically also more complex and costly) authentication protocols have been proposed, the use of passwords for Internet user authentication remains predominant. There are many approaches for Content Based Image Retrieval using different features such as colour, shape, and texture. Some of the published work which cover the more important CBIR Systems is discussed below.

Chin-Chin Lai et.al.[2] have proposed an interactive genetic algorithm (IGA) to reduce the gap between the retrieval results and the users' expectation called semantic gap. They have used HSV colour space that corresponds to human way of perceiving the colours and separate the luminance component from chrominance ones. They have also used texture features like the entropy based on the grey level co-occurrence matrix and the edge histogram. They compared this method with others approaches and achieved better results.

1.1.1 Phishing: Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. For example: A phisher can set up a fake website and then send some emails to potential victims to persuade them to access the fake website. This way, the phisher can

.

1.1.2 Password stealing Trojan: This is a program that contains or installs malicious code. There are many such Trojan codes that have been found online today, so here we just briefly introduce two types of them. Key loggers capture keystrokes and store them somewhere in the machine, or send them back to the adversary. Once a key logger program is activated, it provides the adversary with any strings of texts that a person might enter online, consequently placing personal data and online account information at risk. Trojan Redirector was designed to redirect end-users network traffic to a location to where it was not intended . This includes crime ware that changes host files and other Domain Name Service (DNS) specific information, crime ware browser-helper objects that redirect users to fraudulent sites, and crime ware that may install a network level driver or filter to redirect users to fraudulent locations.

1.1.3 Shoulder-surfing: Shoulder-surfing is a well-known method of stealing other's passwords and other sensitive personal information by looking over victims' shoulders while they are sitting in front of terminals. This attack is most likely to occur in insecure and crowded public environments, such as an Internet Café, shopping mall, airport, etc. It is possible for an attacker to use a hidden camera to record all keyboard actions of a user for both a computer and an ATM machine. Video of the user's actions on a keyboard can be studied later to figure out a user's password and ID.

1.2 Use of various securing mechanisms

Use of virtual keyboards can prevent the key logger attacks by enabling the user to enter a password without using the keyboard but still the system is open to attacks like phishing, shoulder surfing. Use of secure access images can prevent phishing attacks to an extent, but they are not safe from shoulder surfing.

1.3 The Challenge:

The security of an application is always a tradeoff between a high level of security and more usability. The more security is added to an authentication system (pass phrases instead of passwords, multiple authentication tokens), the lower will be the acceptance rate of the users and the usability will decrease. It is a big challenge to find the most secure authentication system which is Users always want new applications and features with easy to use interfaces. At the same time they are worried about the increasing dangers. Moreover, new legislations are pushing manufactures and companies to protect the privacy of their clients. These broad demands from the users create a wide range of attack vectors. Phishing, identity theft, spyware, malware, key loggers, JavaScript attacks, and generally untrusted consumer platforms all make the traditional means of password based authentication ever more complicated.

2. Authentication Architecture for Document Retrieval.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks and the Internet, authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each User registers initially or registered by someone else, using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. For example, a party wishing to admit a letter into evidence may ask the witness whether it is, indeed, the letter he received, does he recognize the handwriting, and similar questions. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen like phishing, key logger and shoulder-surfing attacks. For this reason, Internet business and many other transactions require a more stringent authentication process that is nothing but the password should not be static, it is always change at the time of authentication, by means the password should be generated dynamically at the time of login and instead of entering the whole dynamic password, the server will ask some question to the user if the user know the details then only the user will give the correct response to the server then the server identifies that user is valid otherwise the user is invalid. The present invention is related to communication networks and, in particular, to provide secure communications therein for providing access from a client computer over an insecure public network to one of a plurality of destination servers on a secure private network. Computer networks are known generally as including a wide variety of computing devices, such as client computers and servers, interconnected by various connection media. In particular, it is common place for an institution, such as a corporation, to provide such a network. Such network may include a multiplicity of servers executing a corresponding number of application programs ("applications"). The corporation's employees may use one or more of these applications to carry out the business of the corporation. Such a network may be characterized as a private, secure network, since it is accessible under normal, expected operating conditions only by suitably authorized individuals.

2.1 Authentication Architecture Description:

In Authentication system when the user want to authenticate with the system need to provide intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services these all effectively performed by Authentication, authorization, and accounting (AAA) is a term of a framework. These combined processes are considered important for effective network management and security.

As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

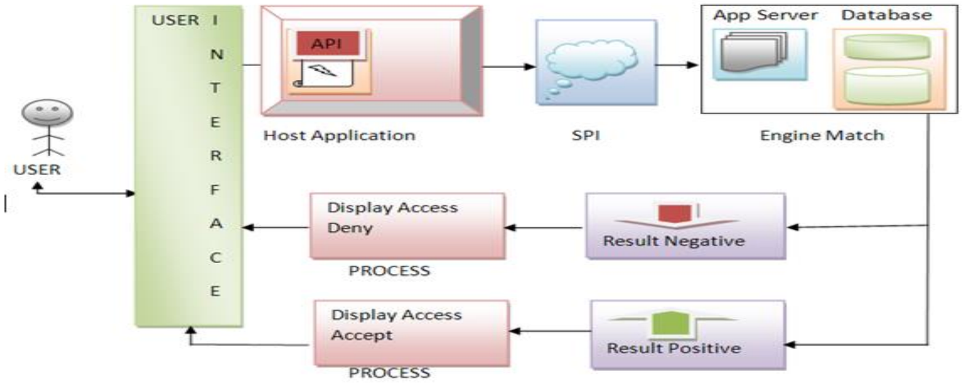
The final process in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

2.2 Authentication Model:

Authentication model describes when the user want to authenticate with the system, the user need to interact with host application. The host application is an application that integrates with the development framework that allows you to develop our own application by using the application program interface and provides implementation of the service provider interface. The user interact with host application with the help of user-interface, user-interface will provide the friendliness to the user in order to interact with the system. When the user will communicate with the host application will invoke the application program interface. The application program interface is an interface defined and implemented by the framework that is used by host application to invoke operations provided by framework .Service provider interface is an interface defined by the framework that is implemented by host applications. An application or contained will implement a number of service provider interfaces, in order to support the framework at the various support levels. Service provider interface will transfer the service to the application server. An application server is the kind of software engine that will deliver various applications to another device. It operates between the client and the database. It is the kind of computer found in an office or university network that allows everyone in the network to run software off of the same machine.

An authentication mechanism using different type of components for establishing the secure connection between the valid user and application system, Authentication model components are

- User
- Host Application
- User Interface
- Application Program interface
- Service Provider Interface
- Application Server
- Database
- COLOUR FEATURE EXTRACTION
- SHAPE FEATURE EXTRACTION
- TEXTURE FEATURE EXTRACTION
- COMBINING FEATURE



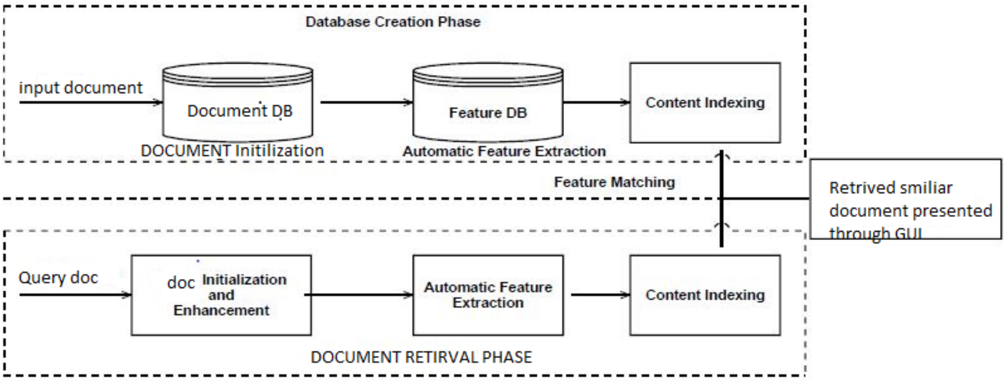


Fig. 1.Content Based Document Retrieval System Framework

2.3 Authentication Methods

The Authentication is the process of verifying the identity of a person or entity. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is part of most online applications. Before a user can access its email account, its online banking account or its favorite online shopping account, it has to identify and authenticate itself to the application.

Authentication technology provides the basis for access control in computer systems. If the identity of a user can be correctly verified, legitimate users can be granted access to system resources. Conversely, those attempting to gain access without proper authorization can be denied. Authentication is defined as the act of verifying the identity of a user. Once a user's identity is verified, access control techniques may be used to mediate the user's access to data. A variety of methods are available for performing user authentication.

The traditional method for authenticating users has been to provide them with a secret password, which they must use when requesting access to a particular system. Password systems can be effective if managed properly (Federal Information Processing Standard [FIPS] 112), but they seldom are. Authentication which relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. If passwords are generated from a random combination of characters, users often write them down because they are difficult to remember.

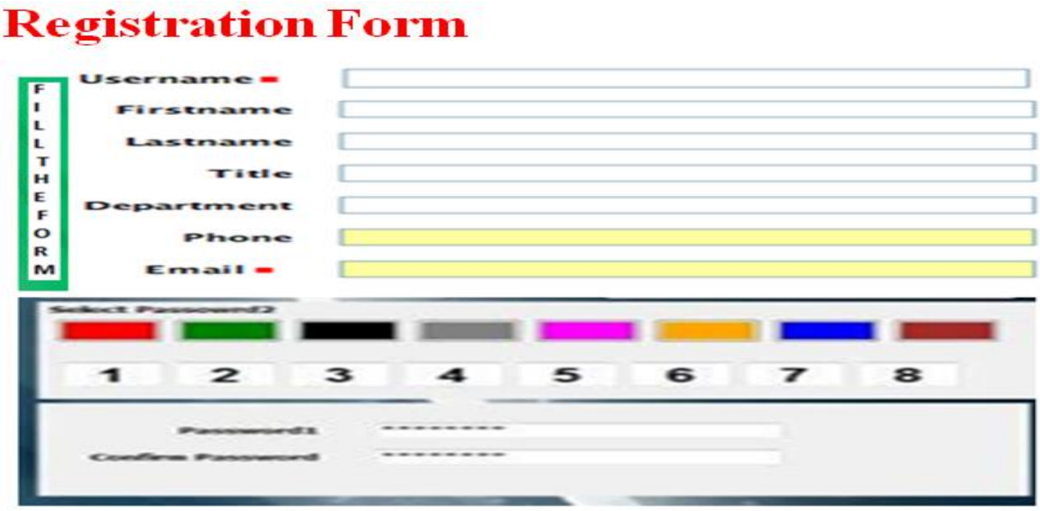
Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. The three generally accepted methods for verifying the identity of a user are based on something the user knows, such as a password; something the user possesses, such as an authentication token; and some physical characteristic of the user, such as a fingerprint or voice pattern. A variety of methods are available for performing authentication.

1) Password Authentication
2) Biometric Authentication
3) Security Token Authentication
4) Smart Card Authentication
5) Graphical Authentication

The Password-based authentication is the most widely used method for verifying the identity of persons requesting access to computer resources. Although many more secure (typically also more complex and costly) authentication protocols have been proposed like authentication tokens, Smart cards, biometrics, and other alternative methods for verifying the identity of system users can substantially increase the security of an authentication system, the use of passwords for Internet user authentication remains predominant. Due to the usability and ease of deployment, most financial transactions over the Internet are authenticated through a password. Hence passwords are a prime target of attackers, for economically-motivated exploits including those targeting online bank accounts and identity theft. Due to this reasons we are proposing new algorithm on Graphical Authentication.

3 Textual Authentication Scheme on colours:

During registration, the user gives rankings (1to8) to colours in the colour grid which is considered as the hybrid textual password. In primary level authentication, when the user selects the hybrid textual authentication scheme, an interface is displayed. The interface consists of 8X8number grid in which numbers from 1 to 8 are placed haphazardly. In addition to this, a colour grid is also displayed containing 4 pairs of colours. Both these grids changes for every session.



Registration Form

FILL THE FORM

Username
Firstname
Lastname
Title
Department
Phone
Email

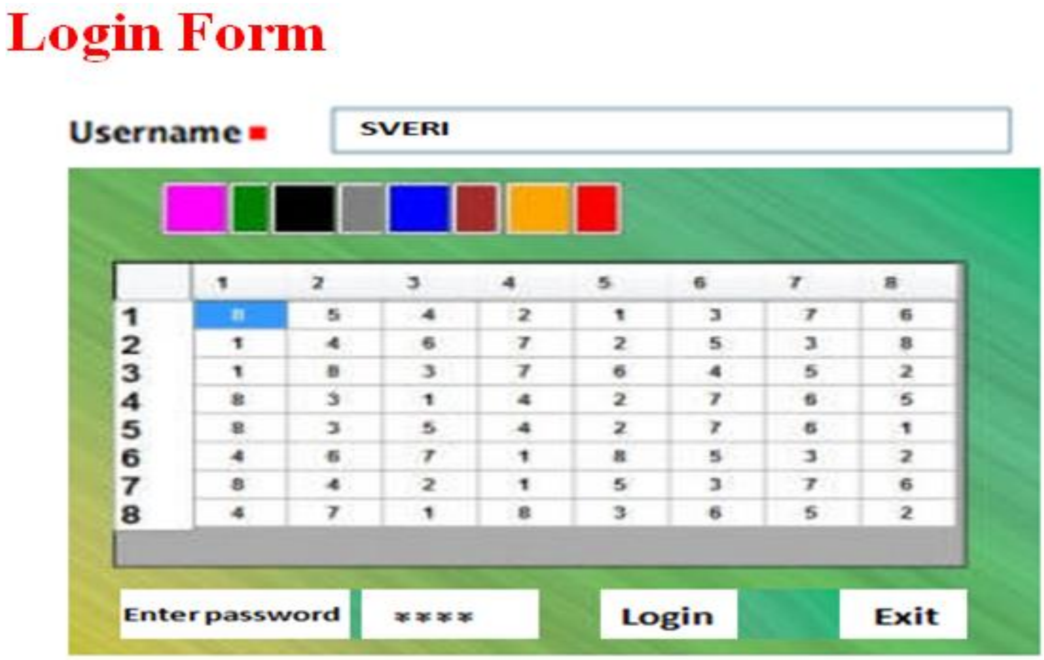
Select Password2

🟥	🟩	⬛	▨	🟪	🟧	🟦	🟫
1	2	3	4	5	6	7	8

Password1 *********
Confirm Password *********

Figure 2: Textual Registration Screen on Colours

The logic involved in this scheme is that the rating given to the first colour of every pair represents arrow and the rating given the second colour in that pair represents a column of the 8X8 number grid. The number in the intersection of the row and column of the grid is the part of session password. This procedure is repeated for the remaining colour pairs in the colour grid [4].In both the cases, if the session password entered by the user is correct, then he is permitted to face them secondary level authentication. Otherwise, the user is prompted to re-enter the session password according to the secret pass and hybrid textual password Authors are free to extend the main body text and sections as appropriate with suitable section/subsections. Do not include unnecessary spaces or indentations between or within paragraphs, sections or subsections other than what have been included in this template. Do not use additional styles or font settings other than the used. Please refer the Table1 for further details on font styles and sizes.



Login Form

Username ■ SVERI

🟪 🟩 ⬛ ⬜ 🟦 🟫 🟧 🟥

	1	2	3	4	5	6	7	8
1	8	5	4	2	1	3	7	6
2	1	4	6	7	2	5	3	8
3	1	8	3	7	6	4	5	2
4	8	3	1	4	2	7	6	5
5	8	3	5	4	2	7	6	1
6	4	6	7	1	8	5	3	2
7	8	4	2	1	5	3	7	6
8	4	7	1	8	3	6	5	2

Enter password ****

Figure 3: Textual Login Screen on Colours

3.1 Virtual Password Algorithm On TEXT and COLOURS:

- **Registration Phase**
  - i. User has to fill the details.
  - ii. User has to select Username.
  - iii. User has to select Colour precedence.

- **Login Phase**
  - i. Server generates 8 colours from selected colours.(Each two adjacent colours represent the pair of (x,y) co-ordinates).
  - ii. And it also generate the virtual Grid board (8x8 Grid, The Grid contains random numbers in between the range 1 to 8) .

- **Function calculation :**
  - i. Functionf(1)==Coordination(Colour(x1), Colour(y1);
  - ii. Functionf(2)== Coordination(Colour(x2), Colour(y2);
  - iii. Functionf(3)== Coordination(Colour(x3), Colour(y3);
  - iv. Functionf(4)== Coordination(Colour(x4), Colour(y4);

- **Virtual Password:**

  Virtual Password= f(1)f(2)f(3)f(4)

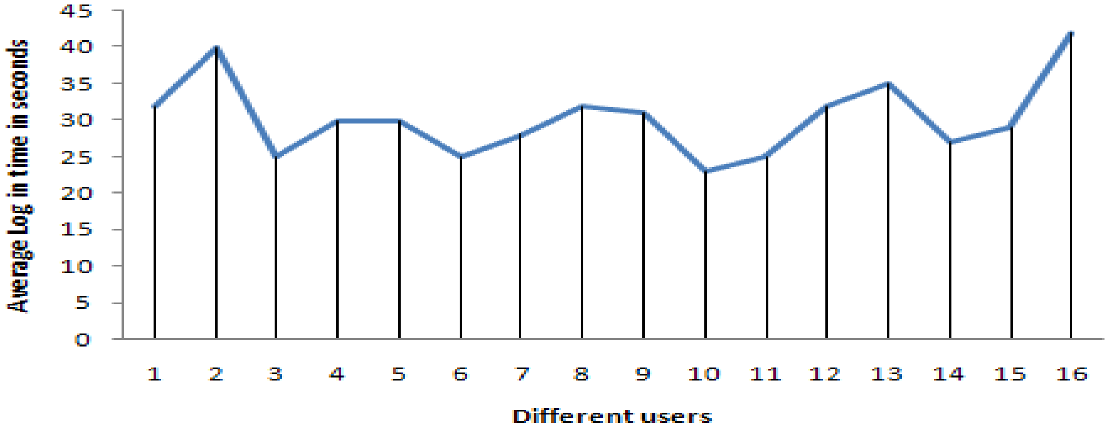
```
        Example :  f(1)=2,  f(2)=1,   f(3)=8,   f(4)=6

      Virtual Password==2186

▪       If    Virtual Password    Then
                      •  The user is the authorized user.
          else
                      •  The user is the unauthorized user.
        End if

▪ End
```

For this authentication, the users needed to calculate the password by themselves, with the help of their string part, secret number and operation precedence. We recorded the time how much time needed to complete the process. They completed each round 10 times and recorded the time it took them to complete their login. We can see that the user time to login to the system can vary depending on their ability to perform simple calculations. Some users will take around 25s to login to the system. Some other users will take around 50s to login the system.



The total users will take an average of 35s to login to the system. We examined the users that it is to take a little bit longer to login to the system, if such a login will be guaranteed secure. The login success rate is around 90%. We argue that it is worth it to take a little bit longer to login to the system, if such a login will be guaranteed secure. This is especially important when a user logs into some important system via the internet, such as an online banking account or credit card account, online shopping and government networks.

3.2 COLOUR FEATURE EXTRACTION:

Colour is perhaps the most expressive of all the visual features and has been extensively studied in the image retrieval research during the last decade. Colour is a basic visual attribute for both human perception and computer vision [6] and one of the most widely used visual features in image retrieval. The scalable colour descriptor (SCD) is defined in the hue-saturation-value (HSV) colour space with fixed colour space quantization, and uses a novel Haar transform encoding [7].The HSV colour space is a popular choice for manipulating colour. The HSV colour space is developed to provide an intuitive representation of colour and to approximate the way in which humans perceive and manipulate colour. RGB to HSV is a nonlinear, but reversible, transformation. The hue (H) represents the dominant spectral component—colour in its pure form, as in green, red, or yellow. Adding white to the pure colour changes the colour: the less white, the more saturated the colour is. This corresponds to the saturation (S). The value (V) corresponds to the brightness of colour. The coordinate system is cylindrical, and is often represented by a subspace defined by a six-sided inverted pyramid. The top of the pyramid corresponds to V=1, with the ―white at the centre. The hue is measured by the angle around the vertical axis, with red corresponding to 0. The saturation ranges from 0 at the centre to 1 on the surface of the pyramid. An inverted cone is also used to denote the subspace instead of the pyramid. The SCD addresses the interoperability issue by fixing the colour space to HSV, with a uniform quantization of the HSV space to 256 bins. The HSV space is uniformly quantized into a total of 256 bins. This includes 4 levels in H, two levels in S, and two levels in V. The histogram values are truncated into a 11-bit integer representation. So it generates the 256 histograms value stored in feature vector database. In similarity matching of histograms, the Canberra distance is used to usually result in good retrieval accuracy. We found, HSV colour space to be better than RGB colour space, from literature survey where each component is quantized in non-equal intervals, where H : 16 bins, S : 4 bins and V : 4 bins. Finally, these 16X4X4 bins are concatenated to obtain a 256 dimensional vector [8].

The following steps are followed to extract colour feature.

1. Read the query image from user.

2. Convert RGB colour space into HSV colour space.

3. Quantize each pixel in HSV space to 256histogrambins.

4. The normalized histogram is obtained by dividing with the total number of pixels.

5. Store the 256 values as colour feature vector in feature vector database.

6. Calculate the similarity measure of query image and the document present in the database using Canberra Distance.

7. Retrieve the images based on minimum distance

3.3. SHAPE FEATURE EXTRACTION

The group of image processing operations which process the image based on shapes is referred as Morphology [9].In morphological operations the output image is created with help of applying structuring element to input image. A morphological operation that is sensitive to specific shapes in the input image can be constructed by choosing the size and shape of the neighbourhood Dilation and erosion are the most basic morphological operations. Dilation creates the effect of swelling of shapes of the objects by adding pixels to the boundaries of objects in an image, while erosion forms the object shape shrinking effect by removing pixels on object boundaries. The size and shape of structuring element decide number of pixels added or removed from the objects in an image. In the morphological dilation and erosion operations, the state of any given pixel in the output image is determined by applying a rule to the corresponding pixel and its neighbours in the input image. Shapes are often determined by first applying segmentation or edge detection to an image [10]. Other methods use shape filters to identify given shapes of an image [11,12]. In some cases accurate shape detection will require human intervention because methods like segmentation are very difficult to completely automate [13]. Here the paper discusses shape texture extraction using morphological operations like erosion, dilation.

The following steps are followed to extract Shape feature.

1. Read the query image from user.
2. Convert RGB query image to Grey Scale image.
3. Calculate 4 morphological gradients of edge maps are generated.
4. Calculate seven moment invariants for each edge map,totally28 features are stored.
5. Compare similarity matching with database image with query image using distance metrics.
6. Retrieve the top ten images based on minimum distance.

3.4. TEXTURE FEATURE EXTRACTION

Grey Level Co-occurrence Matrix (GLCM) is a widely used texture descriptor and it is proven that results obtained from the co-occurrence matrix are better than the other texture discriminations methods [17]. GLCM computes the statistical features based on grey level intensities of the image. It enhances the details of image and gives the interpretation. The GLCM is a tabulation of how often different combinations of pixel brightness values (gray levels) occur in an image. The advantage of the co-occurrence matrix calculations is that the co-occurring pairs of pixels can be spatially related in various orientations with reference to distance and angular spatial relationships, as on considering the relationship between two pixels at a time. As a result the combination of grey levels and their positions are exhibited apparently.

Therefore it is defined as ―A two dimensional histogram of grey levels for pair of pixels, which are separated by a fixed spatial relationship‖. However, the matrix is sensitive to rotation. With the change of different offsets define pixel relationships by varying directions (rotation angle of an offset) and displacement vectors(distance to the neighbour pixel: 1, 2, 3 …), different co-occurrence distributions are resulted from the same image of reference.

The following steps are followed to extract texture feature.

1. Read the query image from user.
2. Convert RGB query image to Grey Scale image.
3. Compute four GLCM matrices for each direction
4. For each GLCM matrix compute the statistical features such as Energy, Homogeneity, Contrast and Correlation.
5. Compare similarity matching of database image with query image using distance metrics.
6. Retrieve the top ten images based on minimum distance.

3.5. COMBINING FEATURE

The retrieval result using only single feature may be inefficient. It may either retrieve images not similar to query image or may fail to retrieve images similar to query image. Hence, to produce efficient results, we use combination of colour, shape and texture features. The similarity between query and target image is measured from three types of characteristic features which includes colour, shape and texture features. So, during similarity measure, appropriate weights are considered to combine the features.

4 EXPERIMENTAL RESULTS

All colour, shape and texture retrieval algorithms are implemented in MATLAB with the database of 1000images. All the images are stored in JPEG format with size 384 × 256 or 256 × 384. There are ten different categories.

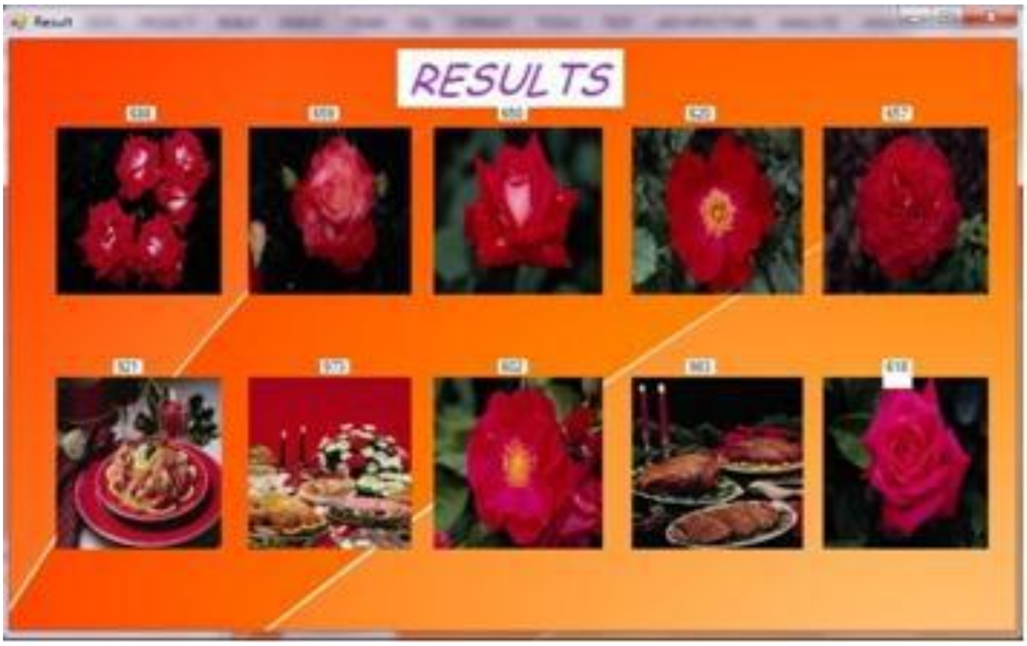


Fig.4. CBIR output using HSV colour space Histogram

We have given the query image to CBIR system and we got some images which are related to query image based on the colour technique. But the result which has obtained is not satisfactory. So we go for shape retrieval technique.

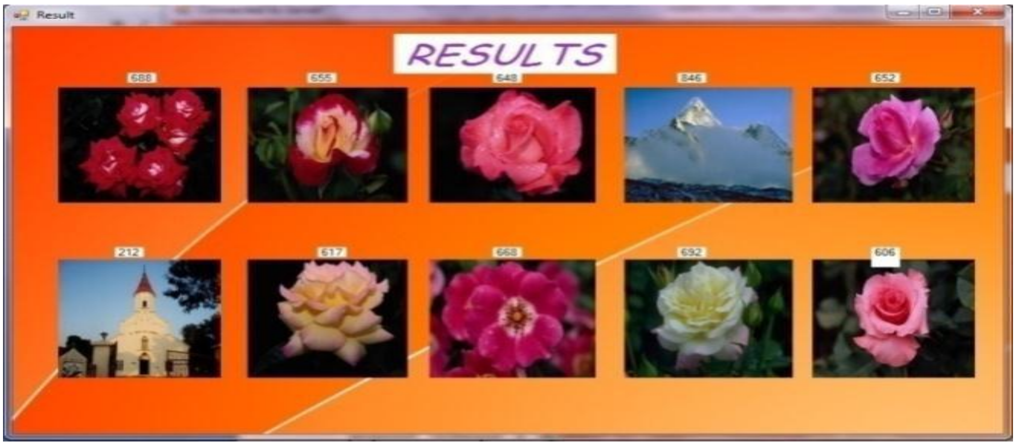


Fig.4.1 CBIR output using shape.

We have given the query image to CBIR system and we got some images which are related to query image based on the Shape technique. But the result which has obtained is not satisfactory. So we go for Texture retrieval technique.

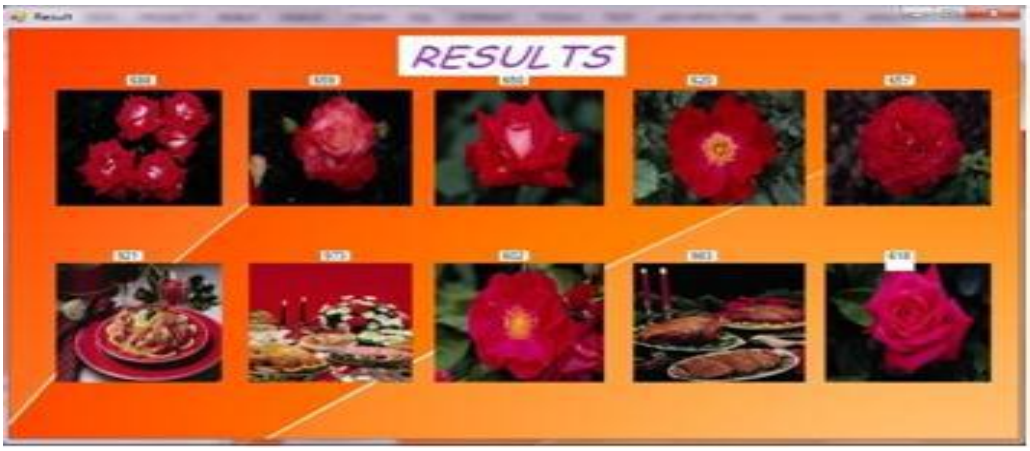


Fig.4.2 CBIR output using texture.

We have given the query image to CBIR system and we got some images which are related to query image based on the Shape technique. But the result which has obtained is not satisfactory. So we go for Image retrieval using combination of Colour, Shape and Texture.

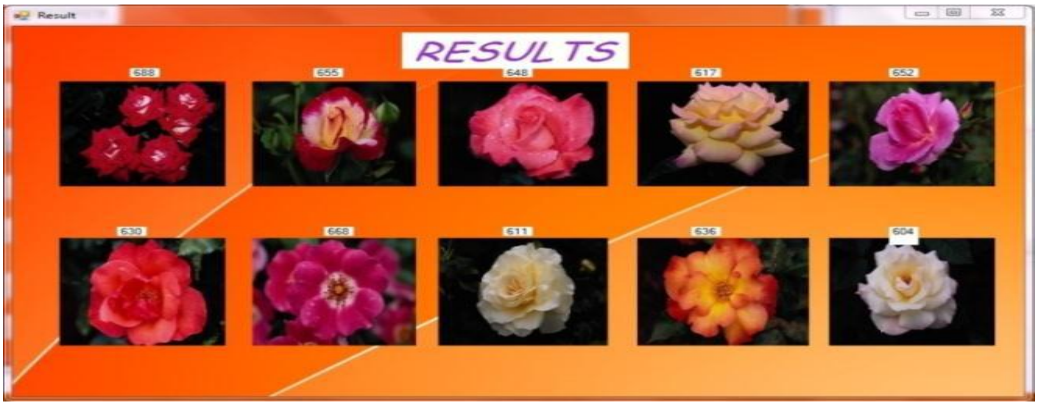


Fig.4.3 CBIR output using combination of colour, shape and texture.

When we have used the colour, shape and texture features we have got better result.

EVALUTION OF RESULT

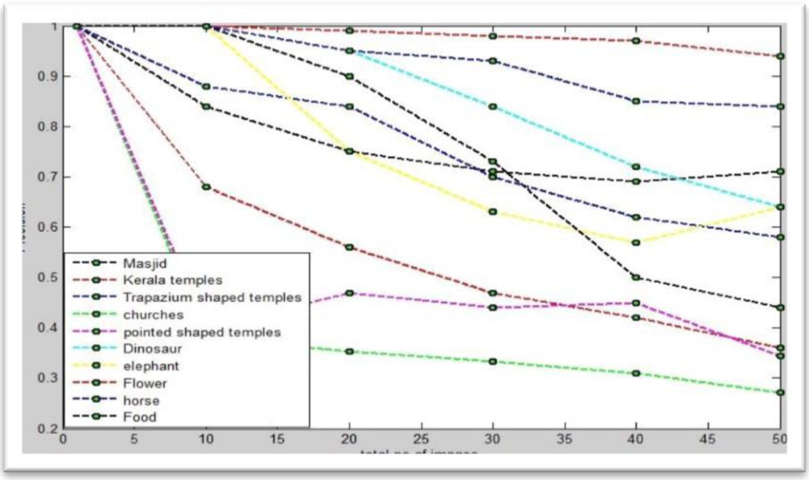


Fig.5 Graph shows average precision Vs no. Of images The above graph shows the effectiveness of the image retrieval using colour, shape and texture. There are 10 categories of images. X axis represents the no. of images average precision we have chosen randomly 5 images from each category and took average precision based on no. of images such as 10,20,30,40 and 50 images.

Conclusion:

We proposed a new algorithm to prevent user's password from being stolen by adversaries. We introduced a new mechanism of authentication using a virtual password For Retrieving Document involving a small amount of human calculation to secure user's password in online environments and ATM's. We analyzed how the proposed scheme defends against phising, key-logger and shoulder surfing attacks.

REFERENCES

[1] Ming Lie,Yang Xiao,Susan V. Vrbsky,Chung-Chih Li:Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing. Computer Communications 31(18): 4367-4375 (2008)

[2] C.Herley, D.Florencio, How to login from an Internet Cafe without worrying about Key-loggers, : in proceedings of Symposium on Usable Privacy and Security (SOUPS)’2006.

[3] Modern access control based on eye movement analysis and keystroke dynamic’2006. Adrian Kapczynskil, Pawel Kasprowski, Piotr Kuzniacki.

[4] Zero Knowledge Protocols and Small Systems -Hannu A. Aronsson, Department of Computer Science Helsinki University of Technology, haa@cs.hut.fi

[5] B. Ross, C. Jackson, N. Miyake, D. Boneh, J. Mitchell, Stronger password authentication using browser extensions, in: Proceedings of 14th USENIX Security Symposium.

[6] E. Gaber, P. Gobbons, Y. Mattias, A. Mayer, How to make personalized web browsing simple, secure, and anonymous, in: Proceedings of Financia Crypto’97, LNCS, vol. 1318, Springer-Verlag, 1997.

[7] E. Gabber, P. Gibbons, D. Kristol, Y. Matias, A. Mayer, On secure andpseudonymous user-relationships with multiple servers, ACM Transactions on Information and System Security 2 (4) (1999) 390–415.

[8] E. Damiani et al., Spam attacks: P2P to the rescue, in: Proceedings of Thirteenth International World Wide Web Conference, 2004, pp. 358–359.

[9] V.A. Brennen, Cryptography Dictionary, vol. 2005, 1.0.0 ed., 2004.

[10] M. Abadi, L. Bharat, A. Marais, System and method for generating unique passwords, US Patent 6 (141) (1997) 760.

[11] RitendraDatta, Dhiraj Joshi, Jia Li and James Wang, ―Image Retrieval: Ideas, Influences, and Trends of the New Age‖, Proceedings of the 7th ACM SIGMM international workshop on Multimedia information retrieval, November 10-11, 2005, Hilton, Singapore

[12] Chih-Chin Lai, Member, IEEE, and Ying-Chuan Chen,‖ A User-Oriented Image Retrieval System Based on Interactive Genetic Algorithm‖, IEEE transactions on instrumentation and measurement, vol. 60, no. 10, october 2011

[13] A.Kannan, Dr.V.Mohan, Dr.N.Anbazhagan ―Image Clustering and Retrieval using Image Mining Techniques‖ 2010 IEEE Conference.

A Brief Author Biography

Prof. S. S. DESAI is working as Assistant Professor in BLDECET,S college of engineering and technology in Bijapur, Her research interests are in the area of Networks, Network Security, Data Mining, Web Technology, Artificial Intelligence, Robotics and Image Processing.

.

DATTATRYA. T. HUVINAHALLI received B.E. degree (Computer Science & Engineering) in 2008 from GIT, Belgum and M.Tech (Pursuing) (Computer Science & Engineering) in 2015.His research interests are in the area of Networks, Network Security, Data Mining, Web Technology, Artificial Intelligence, Robotics and Image Processing.