Summary

Current technology is more than capable of providing a secure authentication process, but users are limited in their ability to remember difficult passwords and make judgments about security. In this thesis, both of these problems were addressed in the development of a new graphical password authentication system. Studies and references in the field of computer security, password usability, and the mathematical tools supported, them were referenced throughout the designing process. New image based password authentication schemes using many mathematical tools like MATLAB, principle component analysis, Fourier transformations, artificial neural network etc. are suggested here.

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized. The user is supposed to choose the kind of password which must be strong enough to be secure, but must be remembered by users. These two requirements present users with conflicting constraints. As password policies require users to include numbers, uppercase letters, and special characters in their passwords, the resulting strings become less meaningful and more difficult to remember. Since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics have been used.
Although, textual passwords are the most used authentication system, it has various disadvantages. The Studies have shown that users have a tendency to pick short passwords or passwords that easy to remember. For an attacker these passwords can easily be guessed or cracked. Many alternate authentication mechanisms have been introduced to conquer this problem but none of them accepted widely. The graphical passwords authentication is one of them. The cause of less usability of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections.

During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords. One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users.

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification. The objective of the thesis is to make graphical passwords more easy to use. The current research work is carried out with the help of following six chapters.

In Chapter 1, firstly we introduce the basic authentication process. We have discussed the problems with the existing authentication mechanisms. Further we have explored the particular
area of authentication i.e. graphical authentication mechanism. We have also discussed the limitations and disadvantages of available graphical authentication mechanisms and our objective of the current work. Some of the mathematical tools which may be used throughout the research work will also be discussed in this chapter.

In chapter 2 we shall review some of the important research work which has been carried out for graphical authentication purpose. Many user studies and survey have confirmed that people can recall graphical password more reliably than text-based password over a long period of time. This seems to be the main advantage of graphical passwords. The many researchers had put their efforts to make it more secure and easy to use by developing different mechanisms. But most of the existing methods have shown some significant drawbacks, therefore, they are not widely acceptable. The question of less implementation of image based authentication has to be answered on a case by case basis, depending on specific algorithms and implementations.

The variety of mathematical tools are available and successfully working to in the field of image processing. An image usually goes through some enhancement steps, in order to improve the extractability of interesting data and subside other data. The main problem with graphical authentication mechanism is that, the images are of large size, processing is slow. The user has to wait for long time to login, as the recall & authentication process takes more time. Therefore, the data reduction & image compression is playing an important role. As the low dimensional images are easy to recall then high dimensional images. For that purpose in chapter 3 we define an important image compression tool principal component analysis. The Principal Component Analysis (PCA) is one of the most successful technique that have been used in image recognition and compression. In this chapter we will discuss the technique in brief. We will also go through
the various steps involved to perform the method in MATLAB to compress a high dimensional image.

In chapter 4 we demonstrate an innovative approach for a fundamental problem in computer vision to map real-time a pixel in one image to a pixel on another image of the same scene, which is generally called image correspondence problem. It is a novel real-time image matching method which combines Rotational Invariant Feature Selection for real-time images and optimization capabilities of Hopfield Neural Networks. The stability of the network has been checked by Lyapunov function. The most invariant image matching features are extracted from the reference image. Finally, the image matching process is optimized by Hopfield neural networks, where image matching problem is treated as minimization of energy function of the Hopfield neural networks.

In Chapter 5 we propose and evaluate the usability and security of Click to Zoom-inside (CTZ); a new graphical password authentication mechanism. Users have to click six times on one point in some given specific regions (pass regions) shown with dotted lines in a theme image displayed on the screen. The selected region is then zoom to create a next image. Exactly, we are not going to zoom the region object of the theme image up to six times; rather we are replacing the image with another image of the same object in big size. The next image is based on the previous click-region. We secure our scheme from shoulder surfer attacking by using WIW scheme with our scheme. We also present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors in recognizing the images.
Since the beginning of computer science, information technology or to be particular image processing to enhance security system in cyber world the mathematics is working as backbone of all. Image processing consists of a wide variety of techniques and mathematical tools to process an input image. In chapter 6 we have proposed a new authentication mechanism which involves principal Component analysis as image compression. For image matching various edge deduction algorithms can be used. We have given MATLAB commands for image combination, image compression, and image matching purpose. The neural network tool may also be used as an alternative process for password authentication. As future work the accuracy in terms of speed and validity may be compared by using neural network for recognition purpose.

Many references have been used to design the thesis, which had been given at the end of each chapter & arrange in the sequence as they appear in the respective chapter. The research papers published during the formulation of the thesis has been attached at end of the thesis.