Chapter 1: Introduction

With an increase in number of services provided over internet, the demand for securing users sensitive data has also increased. The service provider companies are using various authentication methods. In this chapter we are providing an overview of existing authentication mechanisms. We will discuss the limitations and disadvantages of available authentication mechanisms and our objective of the current work. Further we will explore the particular area of authentication i.e. image based authentication mechanism. Some of the mathematical tools which may be used throughout the research work will also be discussed in this chapter.

1.1 Historical Background

As the increasing security reason almost every service provider using various authentication processes to utilize their services [1]. 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. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system. Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. Due to the simplicity of single factor (username/password) authentication mechanisms, most of the web based services have been employing this mechanism. But these mechanisms are now not being considered secure enough for various reasons [2] such as:

- There is a sharp increase in number of attacks on ID/password based mechanisms
- Users registered with various no. of online services have to remember pairs of ID/passwords for their respective accounts.
Therefore 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. Thus a large portion of customer service calls are related to one’s forgetting his or her password. Studies showed that 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 [3]. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics [4, 5] have been used.

1.2 Problem Definition & Motivation

Secure alphanumeric passwords are more difficult to remember because they incorporate more randomness. Users are either choosing easy to remember passwords which are weak & are susceptible to dictionary attack, or are choosing hard to guess alphanumeric passwords which are hard to remember & which leads them to write it on paper [6]. So, in order to provide secure and user friendly authentication, the security experts are strongly recommending the online financial service providers to deploy two factor authentication mechanisms to strengthen security without compromising user convenience.

In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement. An example of this type of authentication process is the use of user ID and password. The second process involves a user ID, password and a key value generated with time and which changes constantly at fixed intervals. A user is authenticated only if all three values are right. This is better and more secure than the basic authentication process as the user has to be there physically to use the changing key. An example of this process is use of smart cards. The third authentication process uses biometrics. Biometrics can measure finger prints, retinal scan, facial image scan and many more. In this case, a user always has these credentials on him. User has to present physically for authentication. The most widely used authentication process uses user ID and a password. Our authentication
system can be classified under the simple authentication process which is more secure and powerful than the password based system.

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Text based authentication

- Picture based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted [8]. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The most common knowledge based authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [8]. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [9]. On the other hand, passwords that are hard to guess or break are often hard to remember. The graphical password can be one of the possible alternatives of text-based passwords because humans can remember images better than a string of characters.
In this thesis, we will focus on a non-traditional authentication method: using pictures as password. Graphical password systems are based either on

(1) pure recall, (2) cued recall, or (3) recognition.

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using pure recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. With cued recall there is a hint, for example a picture, which helps the user to remember the graphical password. Recognition involves identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory.

Draw-A-Secret (DAS), [10] is a pure recall-based graphical password scheme, which allows the user to draw a unique password on a 2D grid. The full password space of DAS is larger than that of the full text password space in a 5×5 grid. DAS passwords of length eight or larger on a 5×5 grid are less susceptible to dictionary attack than textual passwords [13]. However, the registration and the authentication process with DAS takes much longer than with text-based passwords. Typing in a password can be done very fast, while drawing a picture, depending on its complexity, is likely to be more time-consuming.

Passlogix and PassPoints [14] are both cued recall-based graphical password systems. They follow the first idea of graphical passwords described by Blonder [11]. His approach was to let the user click on a few previously chosen regions with a mouse or stylus in an image that appeared on the screen. The problem with Passlogix is that the number of predefined regions is small; just a few dozen in a picture. The password may have several clicks for adequate security and more clicks than characters in a secure password. The PassPoints system extended Blonder’s idea by eliminating the predefined boundaries. As a result, a password can be any arbitrarily chosen sequence of pixels in the image. This guarantees a very large password space, larger than the password space of alphanumeric passwords.
Deja Vu [12] and Passfaces [13] are recognition-based authentication techniques. The user must recognize previously chosen images in several rounds. Deja Vu uses random images whereas Passfaces uses pictures of faces. Results from a user study [12] showed that 90% of all participants succeeded in the authentication using graphical authentication mechanism of Deja Vu, while only 80% succeeded using text-based passwords and PINs. However, the probability for a brute force search to be successful is greater than with text based passwords. Passfaces, which has shown to be very memorable over long intervals [13], has similar security issues. To obtain security similar to that of an eight-character alphanumeric password over an alphabet of 94 characters, 16 or 18 rounds with nine faces each would be required. This would make the log-in slow and tedious. Every graphical password scheme has its strengths and weaknesses. Speaking of security, most graphical passwords are more difficult to break using the traditional attack methods such as brute force search, dictionary attack, and spyware.

Keystroke dynamics is a biometric authentication mechanism and defined as the process of analyzing the way users type by monitoring keyboard inputs and identifying them based on patterns in their typing rhythm [14]. Keystroke dynamics can be used for verification and identification. In case of verification the identity of the user is verified by measuring the typing pattern when writing the username and the password and comparing measurements to a previously stored profile. In the identification case a larger amount of keystroke dynamics data is collected, and the user of the computer is identified based on previously collected information of keystroke dynamics profiles of all users. Verification is easier to implement than identification and is far more studied. However, this is not an alternative to password-based authentication mechanism since username and password are still required. Thus, keystroke dynamics enhance the traditional authentication scheme and provide an additional layer of security.

1.3 Problems with Text Based Passwords

The password problem arises because passwords are expected to comply with two conflicting requirements, namely:
Passwords should be easy to remember, and the user authentication protocol should have the ability to be executed quickly and easily by humans.

Passwords should be secure, i.e. they should look random, be hard to guess and changed frequently. Passwords should be different on different accounts of the same user and not be written down or stored in plain text.

It is almost impossible for users to fulfill both requirements [15]. Today, from a security point of view, the ideal password is a string of eight or more random characters, including digits, letters with a mixture of upper and lower case, and special characters, is not a dictionary word and is not related to relevant data, such as social security number, street address, or birth date. A random password has no content, context, and should not be familiar. It can only be learned by using it over and over again. However, since repetition is a weak way of remembering, users often completely ignore the recommendations for pseudo-random passwords. Surveys show that frequent passwords are the word ‘password’, personal names of family members, names of pets, and dictionary words. Passwords also tend to be too short.

The password problem arises mainly from fundamental limitations of human long-term memory. Once a password has been chosen and learned the user must recall it to log in. However, people regularly forget their passwords. Users are expected to learn a password and remember it over time. However, other items in memory compete with the password and make it more difficult to recall correctly. If a password is not used regularly it will be especially vulnerable to forget. Research has shown that when users fail to recall a password, they are still often able to recall parts of it correctly [16]. However, recalling of only parts of the password has no value for authentication. Having multiple passwords also increases the chance of interference among similar passwords. This is especially true for systems that are not used frequently.

In addition, some computer systems require frequent password changes, with the endeavor to increase security. Passwords that change frequently are more difficult to crack by brute force search because of the time such attacks require. If the intruder does not act immediately, the password may soon become worthless, even if the user does not know that the password has
been stolen. Common techniques require that passwords are changed every 30 or 90 days. However, the more frequently a password has to be changed, the harder it will be to remember. These frequent password changes increase potential interference and are likely to lead either to forgetting passwords or forgetting which system a password is associated with. Secondary, frequent password changes create additional workload. Users must think of new passwords that conform to all of the organization’s requirements but that are also easy to remember.

There are no systems that can prevent a user from writing down their password. To a single user in an office environment, the costs of forgetting a password are fairly slight. The user will call the helpdesk and ask to have his password re-seted. Many systems will allow users to reset their own passwords by asking for additional other information, for example the mother’s maiden name or the city of birth, and sending the new password to a known e-mail address. No matter how easy the process, the user will experience some frustration and loose some productivity. However, to the whole organization forgotten passwords have significant costs. Most commonly, the user will write down passwords, raising the potential of compromise of the passwords. In the case of multiple systems, users may choose only one password for all systems. This reduces security and if the password is broken for one computer system, every single computer system is compromised. Alternatively, users create their own rules to generate multiple passwords that have something in common, for example adding a digit to a base word for each new password, which is also an unsafe method. Weak passwords can be broken by dictionary attacks or attacks based on knowledge about the password owner. Because of password-cracker programs, users need to create unpredictable passwords, which are more difficult to memorize. There are several ways for attackers to break a user’s password.

1.3.1 Overview of different techniques to crack passwords

A simple way to obtain a user’s password is to watch them during authentication. It is called shoulder surfing. Computers located in public area are especially susceptible, for example, in internet cafes, or a laptop on an airplane. Of course, snooping can also be done electronically.
by a small video camera which records finger movements. Spyware is also able to record a
user’s keystrokes and interactions.

Spyware is software that records information about users, usually without their knowledge. In a typical case, users unintentionally install spyware when they visit certain websites or install unapproved software. Spyware may be used in conjunction with social engineering techniques to trick users into installing the spyware. The software then spies on the user’s sensitive data.

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies. Using this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. Phishing is social engineering via e-mail or other electronic means. It is characterized by attempts to get sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

The term phishing is derived from password harvesting and the use of increasingly sophisticated lures to ‘fish’ for users’ financial information and passwords. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage. Spoofing is often used in conjunction with phishing. In a typical spoof, the target receives an email alleging to be from a trusted source. The e-mail may look completely legitimate, containing graphics and logos from the trusted source.

Despite being prohibited by most password security policies, people use common words for their passwords. The words they choose are often easy to guess, such as the name of a family member, a birth date, or even just ‘password’. A potential intruder may try to break into a system by guessing several likely candidates.

In a brute force attack, an intruder tries all possible combinations of cracking a password. The more complex a password is, the more secure it is against brute force attacks. Even if an
intruder could try 100 million combinations per second, it could take almost two years to obtain a password by brute force if the full password space is used. Though, according to the laws of probability, the intruder has a decent chance of finding the password within the first year. However, users often use weak passwords. As a result, the search space for the brute force attack is actually much smaller.

A dictionary attack is a technique for defeating authentication mechanism by trying to determine its passphrase by searching a large number of possibilities. In contrast to a brute force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Protection against dictionary attacks is the main reason that many security policies prohibit the use of words. Avoiding dictionary attacks also inspires policies to break up words with numbers or symbols as in ‘myp8ssword’. Dictionary attacks are mainly successful because of cognitive pressures on the users. It is easier to remember a word than it is to remember random letters, so users naturally choose words.

### 1.3.2 Recommended solution

The majority of solutions to the problems of weak alphanumeric passwords fall into three main categories:

- The first types of solutions are proactive security measures that aim at identifying weak passwords before they are broken, by constantly running a password cracking programs.

- The second type of solution is also technical in nature, which utilizes techniques to increase the computational overhead of cracking passwords.

- The third class of solutions involves user training and education to raise security awareness and establish security guidelines and rules for users to follow.

However, the mismatch between the requirements for good passwords and human capabilities remains. In fact, most knowledge-based user authentication systems rely on perfect memorization. A better way to solve the password problem is to develop authentication systems which reduce fundamental memory problems while preserving
security. The passwords using images is one of the important alternative to overcome these problems. In next section we will understand this method in brief and try to understand the less popularity and realization of this technique.

1.4 An Alternative Authentication Mechanism: Image Based Authentication

Alternatives to password-based authentication mechanisms already exit, but, however, are not widely accepted and adopted in today's complex systems. There are several reasons for this, such as user resistance to change, costs for additional hardware or a poor level of security. Therefore, in the following, requirements are composed which are believed to be important for an authentication mechanism in order to be considered as an alternative to a password-based authentication system.

Talking about secure alternatives to password-based authentication mechanisms the most important question is what the ideal or perfect authentication system would look like. The ideal solution to strong authentication is built primarily around two factors: End user requirements and effective security. The ideal solution should meet the following criteria:

1.4.1 No additional hardware required

It is unreasonable to assume that users will embrace the idea of carrying multiple tokens with them everywhere they go. The average user will not be feeling comfortable to add hardware such as smart card readers or biometrics to all of their systems. Biometric-based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems are expensive since they need additional hardware. Not only are there high initial costs associated with buying the hardware and implementation, there are ongoing maintenance and support expenses. Lost or broken hardware must be replaced. But even more important, users with broken authentication devices cannot access their accounts. Hardware must be replaced or repaired immediately and this burden will involve and affect the end user. Therefore the alternative authentication mechanism should not require additional hardware.
1.4.2 Higher security

Text-password-based authentication schemes are popular means of authenticating users in computer systems and are widely used. However, standard security practices that were intended to make passwords more difficult to crack, such as requiring users to have passwords that look random (high entropy) and frequent password changes, have made password systems less usable and paradoxically, less secure. Compared to password-based authentication mechanisms the alternative scheme should be more secure. For example, it should have a larger password space or be more resistant against brute force or dictionary attacks. Not being able to write the alternative password down or passing it to somebody else can also be considered as a gain of security. Therefore the alternative authentication mechanism should provide a higher level of security.

1.4.3 Better memorability

From a human point of view, the problem of creating a password is to make it memorable so that the user can retrieve it later. This is especially difficult if one wants to create and memorize a secure password. Pointed out as the password problem it is impossible for a human to create secure and memorable passwords at the same time. Therefore, the alternative password should be easier to memorize or in the best case there should be no password to memorize at all.

1.4.4 Simple and easy to use

Until recently the security problem has been formulated as a technical problem. However, it is now becoming more and more recognized that security is also fundamentally a human-computer interaction (HCI) problem [18]. Security mechanisms cannot be effective without taking the user into account. HCI functions in two ways: the usability of the security mechanisms themselves and the interaction of the security mechanisms with user practices and motivations. Therefore, the process of enrollment, training and authentication in the alternative authentication mechanism should be easy and quick. The ideal solution is based on something the user already knows or does, and is not overwhelmingly technical.
1.4.5 Large area of application

Password authentication systems are used widely, to log-on to a PC, to switch on a mobile device, to access a banking application on the internet, to retrieve email or to collect money from an ATM machine. The traditional text-based password authentication scheme is used on different platforms and is not limited to any special application or area. Therefore, the alternative authentication mechanism should have the same large application area and should not be limited to a special application or area. The ideal alternative authentication mechanism should meet all above requirements simultaneously. It is believed that only if all requirements are satisfied the authentication scheme can be considered as an alternative to password-based authentication systems and has the ability to be deployed to today’s computer systems. To address the problems with traditional password authentication researchers have developed alternative authentication mechanisms such as graphical passwords and keystroke dynamics.

1.4.6 Security issues

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of $94^n$, where $n$ is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords [18] Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords. It is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack.
More research is needed in this area. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe’s study [19] revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Except for a few exceptions, key logging or key listening spyware not be used to break graphical passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing [18]. None of the recall-based based techniques are considered should-surfing resistant. Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

1.4.7 Usability issue

Finally, the usability of graphical passwords has to be addressed. A major complaint among the users 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. The 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.

1.4.8 Recommended solutions

As the images occupy more space then alphabets, therefore, the process of graphical authentication may take longer time then alphanumeric passwords. As far as security and memorability concern the image based authentication is more useful than text based authentication. However, to overcome the above listed problems with image based authentication the following points are suggested:

The image with Low dimensionality may be used for passwords. So that they may take less time to load on the screen.

- Compress the images which had been selected by the user using some mathematical compression tool e.g. principle component analysis etc. So that storage and communication issue may be solved.

- Security issues such as shoulder surfing, Brute force attack, guessing etc. may be solved by using distinct password selection mechanisms and many similar type of images.

In the present research work we will try to overcome with these problems using the suggested new password authentication mechanisms.
1.5 Objective of the Current Work

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 [8]. For an attacker these passwords can easily be guessed or cracked [18, 19]. Many alternate authentication mechanisms have been introduced to conquer this problem but none of them accepted widely. The image based authentication is one of them. The objective of the thesis is to make graphical passwords more easy to use. The following points are the main objectives of our research work;

- To develop new mechanisms for graphical authentication which are easily adoptable i.e. they should be easy to use and easy to remember by the user.

  (During the study the research paper entitled “Click to Zoom inside graphical authentication” has been published in IEEE computer society, pp 238-242, 2009)

- To optimizing image matching process using Hopefield neural network.

  (During the study the research paper entitled “On convergence of Hopfield neural network for real time image matching” published in International Journal on emerging Technologies, I(2) pp 1-4, 2010)

- Mathematical modeling to compress the image which is selected by the user as a password using principle component analysis. MATLAB shall be used for the purpose.

  (During the study the research paper entitled “Mathematical modeling to enhance security features for password authentication using MATLAB” published in International Journal of Interactive Computer Communication I(1), pp 1-7, 2011)

1.6 Mathematical Preliminaries

Image processing consists of a wide variety of techniques and mathematical tools to process an input image[20, 21]. An image is processed as soon as we start extracting data from it. The data of interest in object recognition systems are those related to the object under investigation. An image usually goes through some enhancement steps, in order to improve
the extractability of interesting data and subside other data. Lots of mathematical tools and software based on mathematics are behind all these[22]. Extensive research has been carried out in the area of image processing over the last 30 years. Image processing has a wide area of applications. Some of the important areas of application are business, medicine, military, and automation.Image processing has been defined as a wide variety of techniques that includes coding, filtering, enhancement, restoration registration, and analysis [23, 24].

In image processing it is quite common to use simple statistical descriptions of images and subimages. The notion of a statistic is intimately connected to the concept of a probability distribution, generally the distribution of signal amplitudes. For a given region which could conceivably be an entire image we can define the probability distribution function of the brightnesses in that region and the probability density function of the brightnesses in that region. In this chapter we are highlighting one by one some of the mathematical tools which are helpful to increase security and safety wherever required.

1.6.1 Factor analysis

Factor analysis is a method for investigating whether a number of variables of interest are linearly related to a smaller number of unobservable factors; the parameters of these linear functions are referred to as loadings. Factor analysis usually proceeds in two stages. In the first, one set of loadings is calculated which yields theoretical variances and covariance that fit the observed ones as closely as possible according to a certain criterion. These loadings, however, may not agree with the prior expectations, or may not lend themselves to a reasonable interpretation. Thus, in the second stage, the first loadings are rotated in an effort to arrive at another set of loadings that fit equally well the observed variances and covariance, but are more consistent with prior expectations or more easily interpreted. A method widely used for determining a first set of loadings is the principal component method. This method seeks values of the loadings that bring the estimate of the total communality as close as possible to the total of the observed variances [25].
1.6.2 Principle component

The Principal Component Analysis (PCA) is one of the most successful techniques that have been used in image recognition and compression. Principal Component Analysis is the general name for a technique which uses sophisticated underlying mathematical principles to transforms a number of possibly correlated variables into a smaller number of variables called principal components [28,28]. The detail method shall be discussed in chapter 3.

1.6.3 The Fourier transform

The Fourier Transform is used in a wide range of applications, such as image analysis, image filtering, image reconstruction and image compression. The Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components [29]. The output of the transformation represents the image in the Fourier or frequency domain, while the input image is the spatial domain equivalent. In the Fourier domain image, each point represents a particular frequency contained in the spatial domain image. The Fourier transform is among the most widely used tools for transforming data sequences and functions (single or multi-dimensional), from what is referred to as the time domain to the frequency domain. The corresponding inverse transformation which turns a Fourier space description back into a real space one is called the inverse Fourier transform. Before we discuss Fourier Transform we introduce a term called Convolution.

1.6.3.1 Convolution

Convolution is a mathematical way of combining two signals to form a third signal. It is the single most important technique in Digital Signal Processing. Using the strategy of impulse decomposition, systems are described by a signal called the impulse response [30]. Convolution is important because it relates the three signals of interest: the input signal, the output signal, and the impulse response. It is commutative, distributive, associative and possessing identity elements δ (dirac delta function). The convolution of two continuous functions f(t) and g(t), written f(t)*g(t), is defined by the integral

$$ f(t) * g(t) = \int_{-\infty}^{\infty} f(u)g(t-u) \, du $$

(1.1)
1.6.3.2 One dimensional Fourier transform

Considering a continuous function f(t) of a single variable t. The Fourier transform of that function is denoted F(u), where u represents spatial frequency is defined by

\[ F(u) = \int_{-\infty}^{\infty} f(t) e^{-2\pi i ut} dt \]  \hspace{1cm} (1.2)

In general F(u) will be a complex quantity even though the original data is purely real. The meaning of this is that not only is the magnitude of each frequency presents important, but that its phase relationship is too. The inverse Fourier transform for regenerating f(t) from F(u) is given by

\[ f(t) = \int_{-\infty}^{\infty} F(u) e^{2\pi i ut} du \]  \hspace{1cm} (1.3)

which is rather similar, except that the exponential term has the opposite sign.

If f(x,y) is piecewise continuous a function, for example the brightness in an image, its 2D Fourier transform is given by

\[ F(u_x, u_y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x,y) e^{-2\pi i (u_x x + u_y y)} dx dy \]  \hspace{1cm} (1.4)

and the inverse transform, as might be expected, is

\[ f(x,y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} F(u_x, u_y) e^{2\pi i (u_x x + u_y y)} dx dy \]  \hspace{1cm} (1.5)

1.6.3.3 Discrete Fourier transforms (DFT)

As we are only concerned with digital images, we will restrict this discussion to the Discrete Fourier Transform (DFT) which takes such regularly spaced data values, and returns the value of the Fourier transform for a set of values in frequency space which are equally spaced
[31]. The DFT is the sampled Fourier Transform and therefore does not contain all frequencies forming an image, but only a set of samples which is large enough to fully describe the spatial domain image. The number of frequencies corresponds to the number of pixels in the spatial domain image, i.e. the image in the spatial and Fourier domains are of the same size.

In 1D it is convenient how to assume that \( x \) goes up in steps of 1, and that there are \( N \) samples, at values of \( x \) from 0 to N-1. So the DFT takes the form

\[
F(u) = \sum_{t=0}^{N-1} f(t) e^{-2\pi i u t / N}
\]  

while the inverse DFT is

\[
f(t) = \sum_{u=0}^{N-1} F(u) e^{2\pi i u t / N}
\]

Minor changes from the continuous case are a factor of \( 1/N \) in the exponential terms, and also the factor \( 1/N \) in front of the forward transform which does not appear in the inverse transform. The 2D DFT works is similar. So for an \( N \times M \) grid in \( x \) and \( y \) we have

\[
F(u,v) = \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) e^{-2\pi i (ux+vy)/N}
\]

And

\[
f(x,y) = \frac{1}{N^2} \sum_{u=0}^{N-1} \sum_{v=0}^{M-1} F(u,v) e^{-2\pi i (ux+vy)/N}
\]

Image 1.1: Original and Fourier transform of Images
The algorithm for fast DFT, is known as the FFT (the Fast Fourier Transform). It takes advantage of symmetry properties of the complex roots of unity and uses repeated clever partitioning of the input sequence into two equally long subsequences, each of which can be separately (and quickly) processed [32]. The FFT algorithm gives rise to an efficient convolution algorithm, due to the duality between convolution in the time domain and multiplication in the frequency domain. Convolution can be implemented by applying the FFT to the original sequences, multiplying the results, and performing the inverse FFT to obtain the results of the convolution [33]. The canonical example for using the FFT in computer science is for fast multiplication of polynomials.

A very different use of the FFT was recently demonstrated for fast retrieval of an explicitly given sequence, from a large database of stored sequences. The problem addressed in this case is the need to compare the whole given query sequence to each of the whole stored sequences, retrieving the sequences which are within a certain Euclidean distance from the query. The DFT can be used for reducing noise from data, to filter out noise from the observation vectors before further processing them, a transformation is applied to each vector, which eliminates the high frequency components of the data. The Fourier transform calculations were done in order to obtain the low-pass filter matrix, and multiplying a vector by this matrix has an equivalent effect to that of applying the FFT, multiplying by a sequence that eliminates high frequency components, and applying the inverse transform [34, 35].

1.6.4 Mathematical Modeling

Modeling is the process of representing a real system in an abstract manner, in order to study its different features[36]. It is widely used in all fields of engineering. In control engineering, for example, a mathematical model of a physical system is extracted to facilitate the study of its performance under different circumstances. In object recognition, a model is created for the object under investigation. This model is then compared to different models that are stored in a database. If this model matches one of the available models, say, the model of object A, then the investigated model is classified as object A. In an airplane recognition system, for example, the database contains models of different types of airplanes.
1.7 Artificial Neural Network

Artificial Neural Networks (ANN) is another computing paradigm on mathematical models that unlike traditional computing have a structure and operation that resembles the functionality of the mammal brain that originated in the biological world. The foundation of neural networks in a scientific sense begins with biology[38]. The human brain consists of an estimated 10 billion neurons (nerve cells) and 6000 times as many synapses (connections) between them. All information taken in by a human is processed and assessed in this particular part of the body. Thus the brain operates as nothing less than a complex, non-linear and parallel computer. With this notion present we are ready to describe a neural network mathematically[38].

A neural network consists of a number of nonlinear computational elements called neurons or nodes. The neurons are interconnected with adaptive elements known as weights and operate in parallel environment. The structure of neural networks is similar to simplified biological systems. Recently, neural networks have become a prime area of research because they possess the following characteristics:

- Highly parallel structure; hence a capability for fast computing
- Ability to learn and adapt to changing system parameters (e.g., inputs)
- High degree of tolerance to damage in the connections
- Ability to learn through parallel and distributed processing

Neural Computation does not have to be the computation carried out by nerve cells. An artificial system can emulate a simplified version of a neural computational system. ANN is an example of such an artificial neural system. Artificial neural networks are fairly rudimentary electronic models based on the neural configuration of the brain. The brain on the whole learns from experience. Artificial Neural Networks try to replicate only the most basic elements of the complicated, versatile, and powerful organism-brain. The neural network minimizes the energy function formed by the mean square error constructed by the difference between the actual training signal and the signal estimated by the network.
This brain modeling also promises a less technical way to develop machine solutions. Artificial neural networks can easily do various natural tasks. When a test pattern is presented, the stored pattern or pattern pair corresponding to the test pattern is recalled, it is the pattern association task. Storing and recalling of patterns is called autoassociation task while storing and recalling of pattern pairs is called a hetroassociation task. In pattern classification task, given a set of patterns and the corresponding class label, the objective is to capture the implicit relation among the patterns of the same class, so that when a test pattern is given, the corresponding output class label is retrieved. Pattern classification tasks display accretive behavior. In pattern mapping task the objective is to capture the implicit relationship between the input and the corresponding output patterns, so that when a test input pattern is given, the pattern corresponding to the output of the generating is retrieved. Pattern mapping generally displays interpolative behavior [39].

![Artificial Neuron](image)

**Figure 1.2 : Artificial Neuron**

At present, neural networks are the simple clustering of the primitive artificial neurons. This clustering occurs by creating layers, which are then connected to one another. Basically, all artificial neural networks have a similar structure or topology as shown in figure 1.2. In this structure some of the neurons interface to the real world surroundings to receive the inputs. Other neurons provide the real world with network’s outputs. This output might be the picky character that the network thinks that it has scanned or the finicky image it thinks is being viewed. All the rest of the neurons are hidden from our view.

A neural network comprises the neuron and weighted building blocks. The behavior of the network depends on the interaction between these building blocks. Two layers of neuron
communicate via a weight connection network [40]. Lines of communication from one neuron to another are important aspects of neural networks. They are the glue to the system. They are the connections, which provide a variable strength to an input. There are four types of weighted connections. First type of connection is feed forward connection. In most networks each neuron in a hidden layer receives the signals from all of the neurons in a layer above it, usually an input layer. After a neuron performs its function it passes its output to all the neurons in the layer below it, providing a feed forward path to the output. Second type of connection is feedback connection. This is where the output of one-layer routes backs to a previous layer.

The way that the neurons are connected to each other has a significant impact on the operation of the network. Third type of connection is lateral connection. There are various methods of learning for artificial neural networks [40]. Neural networks can learn in two ways-supervised or unsupervised [41]. Supervised training involves a mechanism of providing the network with desired output either by manually “grading” the network’s performance or by providing the desired outputs with the inputs. Unsupervised training is where the network has to make sense of the inputs without outside help. Unsupervised training is used to perform some initial characterization on inputs. However, in the full-blown sense of being truly self-learning, it is still just a shining promise that is not fully understood, does not completely work, and thus is relegated to the lab. One of the examples to the supervised learning procedure is back propagation learning algorithm. Now we look at this supervisory learning algorithm in brief.

**1.7.1 Back propagation**

Back propagation is one of the most popular supervised training methods for neural networks. The back-propagation method is a learning procedure for multilayered, feed forward neural networks. By means of this procedure, the network can learn to map a set of inputs to a set of outputs. During the learning process, an input vector is presented to the network and propagated forward to determine the output signal. It is the actual output for the network. This actual output is then compared with the target output and the resulting error signal, which is back propagated through the network in order to adjust the coupling
strengths. This learning process is repeated until the network responds for each input vector with an output vector that is sufficiently close to the desired one.

The general formula for the activation $A$ of each unit in the network (except for the input units whose activation is clamped by the input vector) is given by

$$A_j = \frac{1}{1 + \exp\left\{-\left(\sum_{i} w_{ji} y_i + h_j\right)\right\}}$$ \hspace{1cm} (1.10)

where $w_{ji}$ is the strength of the coupling between unit $j$ (for which the activation is calculated) and unit $i$ in the next lower layer, $N$ is the total number of units in that layer, $y_i$ is the activation of unit $i$, and $h_j$ is the threshold or bias for unit $j$. This bias can be conceived of as a coupling to a unit with full activation, and is in practice treated just like $w$. Here we consider a three-layered network consisting of a layer of input units (represented by $x$), a layer of hidden units ($y$), and a layer of output units ($z$). In practice, back-propagation has proved to be a suitable algorithm in establishing a set of coupling strengths that enables the network to perform certain input-output mappings. The convergence, however, tends to be extremely slow. Several acceleration techniques have been proposed such as dynamically modifying the learning parameters, and rescaling the partial derivatives in the consecutive layers [42].

The other type of training is called unsupervised training. In unsupervised training, the network is provided with inputs but not with desired outputs. The system itself must then decide what features it will use to group the input data. This is often referred to as self-organization or adaption. At the present time, unsupervised learning is not well understood. This adaption to the environment is the promise, which would enable science fiction types robots to continually learn on their own as they come across new situations and new environments.
1.7.2 Neural networks for image compression

Recently, neural networks have been used for image compression. Artificial neural network models called connectionist models or parallel distributed processing models have received much attention in many fields where high computation ratios are required. Many neural network approaches for image compression yield performance superior to that of the discrete traditional approaches [43]. The estimated output is compared with the actual one for learning. For back-propagation algorithms, image data compression is presented as an encoder problem. In fact, the weight matrices encode the principal components of the given image, that is, after convergence it decomposes the given image into an eigenvalue of decreasing variance. Back propagation is so powerful for image compression that singular value decomposition techniques will be quite appropriate. Figure 1.3 shows one possible application for neural network in image transmission. Digital image generated with an 8 bit imagery system may be reduced in size by feeding it to an 8-to-4 multilayer neural network. On the other end of the line, the compressed image is processed by a 4-to-8 neural network for reconstruction. Compressing images before transmitting them speeds up the transmission time substantially.

Figure 1.3. The use of neural networks for image compression and transmission.

1.7.3 Neural networks for pattern recognition

The neural network is an ideal tool for pattern recognition. Any recognition system needs to be trained to recognize different patterns, and training is the most important part in the design of neural network systems [44]. All pattern-recognition systems try to imitate the recognition mechanism carried out by humans. Since the neural network is a simplification of human neural system, it is more likely to adapt to the human way of solving the recognition problem than other techniques and systems. Finally, we can look at pattern recognition as a
classification problem, which is best handled by neural network systems. The design of the neural network system for pattern recognition starts with collecting data on each of the objects that is to be recognized by the system. A class is assigned to each object, and the collection of data and classes is used to train the system.

1.7 Summary

Graphical passwords require much more storage space than text based passwords. Network transfer delay is also a concern for graphical passwords. 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 have introduced 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
and user has to wait for long time to login, as the recall & authentication process takes more time. Therefore, the 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. Introduce. The Principal Component Analysis (PCA) is one of the most successful techniques 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 demonstrates 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 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.

In chapter 6 we have proposed a new authentication mechanism which involve principal Component analysis as image compression. We have given MATLAB programming tool for image compression and image matching purpose. one of the most successful mathematical
techniques that have been used in image recognition and compression. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. In this paper, we proposed a new scheme to enhance security issues using PCA as an image compression and authentication tool and MATLAB to perform the typical mathematical operations.

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.

1.9 Conclusion

To increase security issues over internet as well as in many other areas like banking services, defense organizations etc. the demand of distinct authentication methods has been increased. Since past few years the research area, especially in the field of enhancing security and to develop user friendly password authentication mechanism, had been gaining wide interest. The most commonly used authentication process is alphanumeric user ID and a password. These passwords are easy to guess or often hard to remember. To keeping the fact, we are exploring a particular area of password authentication i.e. image based authentication in present thesis. The picture based password techniques is not widely adoptable yet but current study [1-5] shows that the graphical password can be one of the possible alternative of text-based passwords because humans can remember images better than a string of characters.
References


