CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Review of CaRP Scheme Based on Chebyshev Polynomial Chaotic Map

by

Nilma Aziz

A thesis submitted in partial fulfillment for the degree of Master of Science

in the

Faculty of Computing

Department of Mathematics

2018

Dedicated to my beloved parents and dear brothers.

CAPITAL UNIVERSITY OF SCIENCE & TECHNOLOGY
ISLAMABAD

CERTIFICATE OF APPROVAL

Review of CaRP Scheme Based on Chebyshev Polynomial Chaotic Map

by

Nilma Aziz

MA141004

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Maria Samreen	QAU, Islamabad
(b)	Internal Examiner	Dr. Dur e Shehwar Sagheer	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
April, 2018

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
April, 2018

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
April, 2018

Author's Declaration

I, **Nilma Aziz** hereby state that my M.phill thesis titled "**Thesis Title**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my M.phill Degree.

(Nilma Aziz)

Registration No: MA141004

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "*Thesis Title*" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of M.phill Degree, the University reserves the right to withdraw/revoke my M.phill degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Nilma Aziz)

Registration No: MA141004

Acknowledgements

All praise be to almighty ALLAH who has been bestowing me with his great bounties and enabled me to complete my dissertation.

I would like to express my deep gratitude to my supervisor Dr. Rashid Ali for his valuable guidance, enthusiastic encouragement and useful critiques of this thesis work. The same acknowledgement should go to Dr. Sagheer, head of the mathematics Department (CUST), I deeply appreciate the insight I gained through my association with him.
I would also like to thank Dr. Dur e Shehwar and Dr. Samina for their valuable cooperation and assistance in keeping my progress on schedule. I would also, like to thank Dr. Afzal, Dr. Kashif Rehman, Dr. Shafqat Hussain for their motivations. I would also thank to the technicians of the laboratory of the mathematics department for their help in offering me the resources in running the program.
I also feel honored to have such supporting friends and class fellows and in return for their support, I would also like to thank my friend Saba Majeed for her help in learning software Latex. I would also, like to thank my friend Ummarah Sadaf Sara Raja and Saba Majeed for being my shadow in every up down and provide me the strength to get focused toward my main objectives.
Finally, without the backbone and prayers of my family it was impossible to make this thesis in practical existence, so, I feel obliged to thank my family for being always with me and bringing all the support for my career. I am grateful to my parents, who have given all the love and care and brought me up in this stage, always helping me to differentiate between evil and virtue. I also would like to express my gratitude to my elder brothers Qamar Aziz and Tamur Aziz, who are always here to care of my problems.

Abstract

Information and computer security is supported by passwords. Password is the principal part of authentication process. Captcha technology as a new security primitive, aiming to provide the mutual authentication for legal users having the ability to differentiate the human and computer within the use of a turing test. Captcha converts into graphical Captcha which is more suitable for touch screen devices. We know that, all the servers must store the password table and some other secret information to authenticate the users. The password tables, can lead to few drawbacks, for example, maintained fee and centralized security. So, once password table disclosed to the third party, both the users and servers suffer large losses.

We focused on detailed study of the novel security authenticated scheme based on Graphical Captcha with no password tables with privacy protection, introduced by Zhu et al. Its objective is to provide convenience for the user login and at the same time stay clear against password guessing attack. The scheme is based on a hard AI problem together with a chaotic system to achieve mutual authentication. The use of a chaotic system has many advantages like unpredictability, sensitivity to initial parameters etc.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advance Encryption Standard
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
RSA	Rivest-Shamir-Adleman
CAPTCHA	Complete Automated Public Turing test to tell Computers and Human Apart
CaRP	Captcha as Graphical Password
AI	Artificial Intelligence
PW	Password
ID	User Identity

Symbols

ID_A : the identity of Alice

ID_S : the identity of the server

B, a, D, C : noneces

$(x, T_k(x))$: public key of server based on Chebyshev chaotic maps

K : secret key of server based on Chebyshev chaotic maps

$E_K \bigcirc D_K \bigcirc$: a pair of secure symmetric encryption—decryption functions with key K

H : A secure one-way hash function

$\|$: concatenation

L : An algorithm to transfer an image into fixed output bits (such as (128))bits

$\mathbb{Q}$: Set of rational numbers

$\mathbb{C}$: Set of complex numbers

$\mathbb{Z}$

$\mathbb{R}$: Set of real numbers

$P| \equiv X$: P believes that the current run of the protocol that the formula X is true

$P| \equiv X$: P believes that the current run of the protocol that the formula X is true

$P \triangleleft X$: P sees or hold formula X.

$P \Rightarrow X$: P has complete control over the formula X. This can be used to express certificate a

$P|\ X$: P has once said the formula X.

$\#(X)$: The formula X is fresh, which means formula X is currently used or it is nonces.

$P \longleftrightarrow Q$: P and Q share a secret key K. The secret key is only known to P and Q and only

X_K : The formula X is encrypted with key K.

(X, Y) The formula X or Y is one part of the formula (X, Y)

$\langle X \rangle_Y$ The formula X combine with the formula Y

$(X)_K$: The formula X is hash with key K.

SK : Session key is used in the current session.

Chapter 1

INTRODUCTION

1.1 Cryptography

Cryptography is the science of secret communication in which message is converted in secret codes during the transmission over a public network in the presence of hackers. The original message is called plaintext and the converted message is called ciphertext. To convert the plaintext into ciphertext an algorithm is needed and this is called an encryption algorithm. The algorithm that converts the ciphertext back into plaintext is called the decryption algorithm. For encryption and decryption, cryptographic schemes need special information which is shared between sender and receiver, and is called a key. A cryptographic scheme that consists of a message space, a ciphertext space, a key space, an encryption algorithm and an decryption algorithm is called a cryptosystem. On behalf of these schemes cryptography is divided into two main areas, one is known as symmetric key cryptography and the other is asymmetric key cryptography.

In **Symmetric Key Cryptography**, only one key is used for both the data encryption and decryption. Sender and receiver are bound to share the key with each other for encryption and decryption of the data. For example, (DES), Data Encryption Standard [22] and Advanced Encryption Standard [3] (AES).

In **Public Key Cryptography**, two keys are used in which, one is for data encryption and the other is used for decryption. A person generates two keys one is kept secret, called secret key, and the other key is made public, called the public key.

Examples of public key cryptography are (RSA) [22], Diffie Hellman [3] and Elliptic Curve cryptography [22].

One of the very recent security primitive is the "Captcha technology". Its aim is to provide mutual authentication for the availability of "legal users" and helps in distinguishing computer and human by using some kind of 'Turing test' based on artificial intelligence problems.

1.2 Captcha In Cryptography

Captcha stands for "Complete Automated Public Turing test to tell Computer and Humans Apart" [18]. Its purpose is to confirm that a user trying to login a system is a human and not a robot. Nowadays, a lot of researchers are working on Captcha-based cryptography to make the security protocols. Captcha is a program or algorithm which clarify the presence of human and computer [6]. Test which takes by the Captha based system is easily solvable by humans and difficult to solve by computers, for example, identification of distorted figures etc. In 2003 Luis et al [27] first time discussed the new model of Captcha using the hard AI (Artificial intelligence) problems to ensure the security of data transmitting on a public network [9]. At that time, this new model caught the attention of the public.

Zhu et al, [26] further polished the work of Luis et al [27] and introduced a new security primitive [9] which is based on hard AI problems and called it CaRP [9] which means Captcha as graphical password. CaRP resists many attacks such as relay and online guessing attack. Captcha has many types of which (1) text Captcha [12] and (2) image Captcha are famous. On the basis of these types, many researchers worked on face Captcha [19], orientation of cropped images and character image based Captcha [19].

In all the types of Captcha, a user needs a computer, with suitable screen, a mouse and a keyboard rather than touch screen devices. In addition, some enhanced Captcha technology [6] only increases the distortation and fuzziness of the characters. As a result, users identification are becoming more difficult, yet insoluble the basic issues [25]. Therefore, based on these motivations, constructing an optimal Captcha technology becomes more important [14]. Graphical Captcha [11] is the comprehensive application of Captcha, and it based on touch screens and it works to convert the ordinary Captcha into graphical Captcha for every login. In this setting, a user has to click only on the image that is transmitted by the server [27]. Here, we point out some benefits of using Graphical Captcha.

1. The main purpose of a Captcha is to prevent users from automatic registration process performed by robot [9] (Computer programs). This is achieved by forming a Captcha that takes numbers or letters together with other interference pixels, that are difficult to recognize by the robots. This does not avoid spams [19]. For example, in the e-banking and tieba. If computer is bound to use the Graphical method, then it goes through more cumbersome calculations, which will minimize the spam traffic.

2. Since the fame of touch screen devices and online payments, few Captcha schemes force a user to see the message first and then enter numbers [27], it is very difficult to users login each time.
   For example, in Graphical Captcha users merely only need to click on the screen directly according to the prompt. Also, it does not need a huge number of the grounding in the languages and common senses [21].

3. Now the railway system use the Graphical Captcha [13] to distribute the tickets online to the buyers having the aim to provide better security. For example, no matter the user login an account or submits ticket orders, all should play a little game, only click on the corresponding text images can easily complete the process [13].

Information and computer security is supported by passwords. Password is the principal part of authentication process [9]. But there exists an obvious loophole that each legal server requires to store password table for authentication [27]. Once the password table is disclosed, an attacker, will easily get a registered [21] user information and act like a legal user to communicate with the server. Since the user identity in clear text transmission over public network which is insecure channel and any attacker will Catcha it easily [19]. Today, there are many schemes which are based on password table. As we know, password table is like a root directory stored in the server, which contains every registered users password and other secret informationis. Once password table is disclosed to the third party, both the user and server suffer a lot [27]. CSDN stands for "Chinese Software Developer Network" from which Chinese software programmers seek advice. In history, the password table had stolen number of times. In 2011 six million legal user's information is leaked on CSDN website. As users registered mailbox and their passwords were in plaintext form and an attacker, got user ID and users had suffered the password guessing inevitably [27].

Google [19] and Gmail [9] users also missed their passwords in 2014. There is no doubt remained that all these losses were happend due to security issues. To avoid these types af attacks, a new Graphical Captcha scheme using public key encryption and hash algorithm, with no password table in the server side to achieve the mutual authentication, is introduced recently by Zhu et al [27]. Users are maintained anonymously in the whole communication in their proposed scheme over the public network.

1.3 Objective Of The Thesis

In this thesis, we did a detailed study of the novel security authenticated scheme which is based on Graphical Captcha with out password tables having privacy protection, introduced by Zhu et al [27]. Its objective is to provide convenience for the user login and at the same time stay clear against password guessing attack.

The scheme is based on a hard AI problem together with a chaotic system to achieve mutual authentication. The use of a chaotic system [8] has many advantages like unpredictability and very sensitive to initial parameters etc.

The rest of the thesis is organized as follows, Chapter 2 contains some preliminary material. A general framework for Graphical Captcha is discussed in Chapter 3. Chapter 4 includes the review of the new Graphical Capcha scheme, its example, comparison of CaRP with other well known schemes, efficiency of CaRP and security analysis.

Chapter 2

Preliminaries

In this chapter, we recall some basic definitions and concepts from cryptography primitives. Due to importance of information security, we will also discuss various methods to accomplish the process of authentication.

2.1 Cryptography

From the ancient time, the security of communication remained a big problem. In about 500 B.C Greece developed a device called Scytale, which was used to send and recieve secret messages [23]. With the passage of time, new methods were introduced that provide more security.

"Cryptography is the practice and study of techniques for secret communication in the presence of adversaries or hackers"[3].

Plaintext and ciphertext are typically opposite of each other. Plaintext is the any message before it has been encrypted and ciphertext is the output information of an encryption technique [23]. There are many encryption techniques which carry many layers of encryption, in which ciphertext output becomes plaintext input to another encryption layer. Decryption process takes ciphertext and converts it back into the original plaintext.

The main context of encryption and decryption program implementation is the creation of encryption and decryption key [23]. Some special techniques are used by the cryptographic schemes to make a complex algorithm which is known as a cryptosystem.

On the basis of a cryptosystem structure the cryptography is divided into two main areas:

1. Symmetric key cryptography
2. Public key cryptography

2.1.1 Symmetric key cryptography

In this process user and sender use the single key for transmitting the message over a public network. Symmetric encryption is the oldest and best-known technique. A secret key which can be a number, a word, or just a string of random letters is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and receiver know the secret key, they can encrypt and decrypt all messages that use this key [22]. Examples of symmetric key cryptosystem include (DES), Data Encryption Standard [22] and (AES) Advanced Encryption Standard [3].

2.1.2 Public key cryptography

The major drawback of the symmetric key is the management of the single key between sender and receiver. That is why the communication area needs such a secure system in which security and key management issue does not occur.

Public key cryptography depends on two type of keys in which one is used for encryption and the other key is used for decryption. One key is called the public key and it is easily approachable and the second key is called secret or private key and it is kept secret and not reachable unless the owner of the key disclose it [3]. Public key encryption has the following features.

1. Plaintext: It is basic and understandable information or code that is put into the algorithm as input data [22].
2. Encryption Algorithm : Various transformations are performed on plaintext through an encryption algorithm [22].
3. Public and Private Keys : A pair of public and private keys is selected. In this pair one key is used for encryption and the other is used for decryption. The exact transformations which are performed by the algorithm depends on public or private key that is provided as input [3].
4. Ciphertext: Ciphertext is the scrumbled type of data used as output [3].
5. Decryption Algorithm : Decryption algorithm meets the coded text and the matching key and generates the original information which is plaintext [22].

Figure 2.1, shows the typical model of public key cryptography. Few steps which are essential for public key cryptography are as follows:

1. Every user must produce a pair of keys which should be used for data encryption and decryption[22].
2. From the two keys every user placed one key in public register for an easy approach. This is called public key. The second key must be kept secret. As the Figure shows that every participant maintains a set of public keys which are obtained by others [3].
3. If Bob wants to send a secret message to Alice, Bob will encrypt the message using his own private key and Alice's public key [22].
4. When she receives the data from the Bob, she will use her private key to decipher the data. Only Alice can decrypt the message because, she has a secret key[3].

In Figure 2.1 we consider Alice as the sender of message and Bob as the recipient of the message. For security program, information security is the important factor

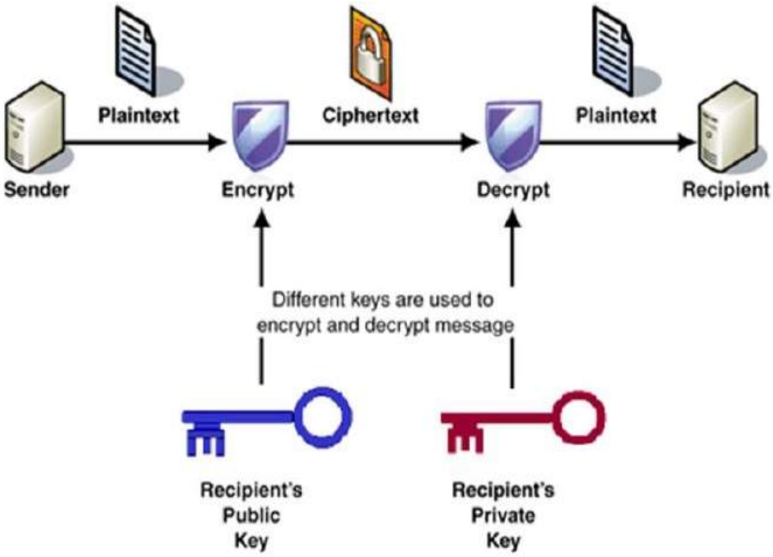


FIGURE 2.1: Public Key Cryptograpghy

and authentication is the convenient method for this security [9]. Recall that, authentication is a process of recognizing or verifying the identity of a legal user. The most famous method is password authentication. Passwords authentication has two types.

1. Text-Based Password
2. Graphical-Based Password

Definition 2.1.1. (**Text-Based Password**).
"Text-based or textual passwords are also called alphanumeric passwords. Typically, such passwords are strings of letters and digits" [9].

A lot of inadequacy is present in this scheme. Because, in text-based passwords schemes a user used such type of passwords which are easily used and able to remember. It can be personal names, dictionary words date of birth and mobile number etc. There are many attacks on the text-based passwords such as:

1. Dictionary attack: "In this type of attack, an attacker, uses a dictionary of normal words and all possible try to recognise the user password" [27]
2. Guessing attack: "Password guessing attack is the type of network attack. Here a legal user who has access rights to a computer and internet sources

are exposed by recognising the user identity and password compactness of the legal user"[27].

3. Shoulder surfing attack: "In this type of attack an attacker, tries to judge the movement to get the users passwords".

4. Social engineering attack: This type of attack is about confidential information.

5. Spyware attack: Automated programmers apply the spyware attack to collect the information about computer use and share that information to the third parties.

Nowadays, users need passwords for their personal laptops, email and more, and for all types most of them use the easy and same password which minimizes the security. So, if users use the complex passwords then they are difficult to remember and if kept easy then they are easy to break [9]. So, a new way is introduced to overcome the difficulties in text-based passwords and this new technique is called graphical password.

Definition 2.1.2. (**Graphical Password**).
"In graphical passwords, images or shapes are used as passwords because people can remember images easily than text, the psychological studies support such assumption [2]. It is an easy task for humans beings to remember the places, which they visit, things they have seen and faces of different humans" [2].

For example images used in graphical password schemes are in large sizes that makes the graphical password space big enough. If we compare both the password space of text-based passwords and graphical password than graphical based password space exceed as compare to the text-based passwords. Graphical password schemes resisted to all those attacks which are possible in text-based passwords [9]. Graphical password schemes makes the passwords which are difficult for guessing attack and are easy to remember. Now, we discuss the graphical password technique from the literature point of view [9].

2.1.3 Graphical Password Techniques

These techniques are proposed to overcome the limitations of text-based passwords. In graphical passwords both the text and images together are used. There are number of graphical schemes which have been discussed in literature. It is categorized into the following three types according to the purpose of memorizing and entering the password [9].

1. Recognition-based scheme
2. Cued-based scheme
3. Recall-based scheme

Definition 2.1.3. (**Recognition-based Scheme**): In this scheme, a number of images are provided and user has to choose the image as password from the set of images. User is asked to select that image which he or she selected already in the time of registration [2].

Passface: Passface is the example of recognition-based scheme and this method is developed in 2000. Human faces are used as password in this scheme. In this scheme, there are several rounds and in each round user have to select the face image which is selected in the registration phase already. It has a very prominent drawback which is the probability of a guessing attack and is high within the few authentication rounds. This scheme is also predictable and guessable [2].

Definition 2.1.4. (**Recall based scheme**): At the time of authentication, in this scheme a user is asked to regenerate that thing which he or she already chosen at the time of registration [2].

Draw-A-Secret Scheme: Draw a secret is the example of recall based scheme and this scheme was proposed in 1999. In this scheme, user draw something on the 2D grid. In the authentication phase user have to touch and redraw the same grid

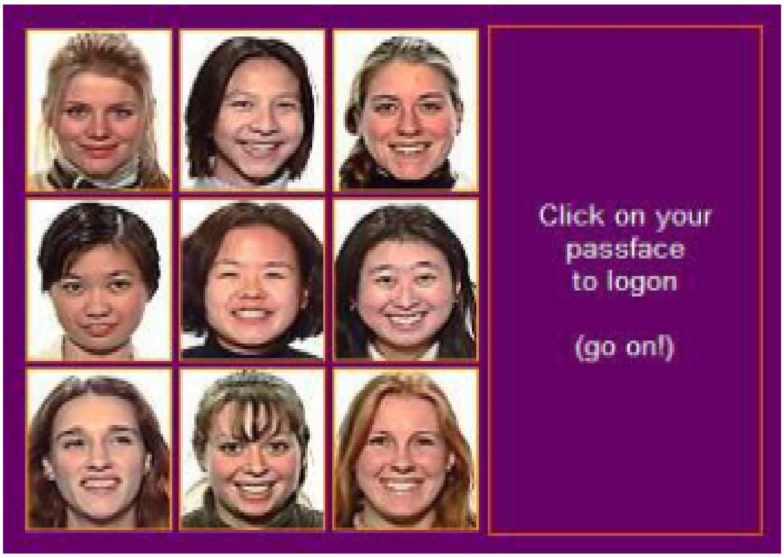


Figure 2.2: Passface scheme

in the same sequence as in registration phase. To draw the password is difficult to remember as compare to other schemes and it is the drawback of this scheme [9].

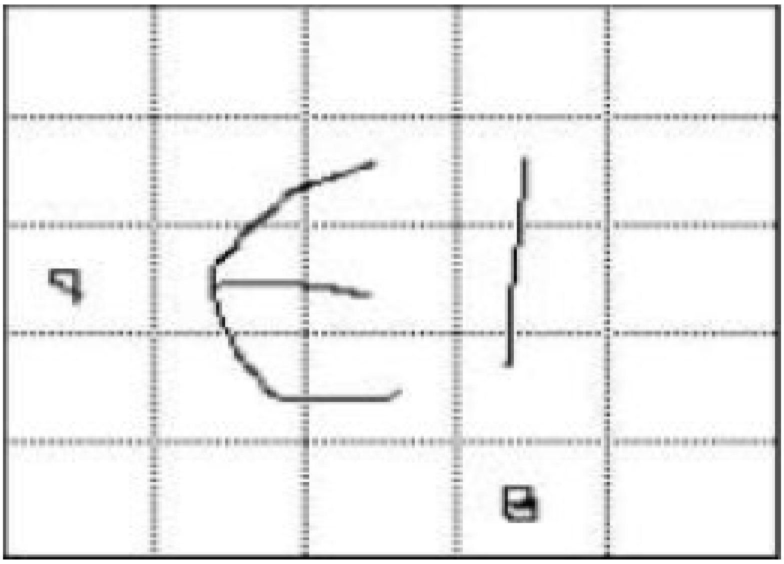


Figure 2.3: Draw a Secret scheme

Definition 2.1.5. (**Cued-based scheme**): Cued-based scheme is also called the click-based scheme. User is presented with set of images and from this set images user have to choose click point on the particular image which is chosen as password. If click points are matched then authentication is successful [2].

Blonder: It is the example of cued-based scheme and proposed by Greg blonder. In this scheme, prestored images are used and user is presented with these prestored images and have to tap area by pointing the locations on the image. Clicking a area is small so, it is simple and easily crackable. This is the drawback of cued based scheme [2].

The benefits of graphical password are listed below:

1. This scheme provides a way in which much user-friendly passwords are made.
2. Graphical password schemes have greater security as compared to text-based passwords [19].
3. Graphical passwords schemes resist many attacks like brute force and dictionary attacks which are always possible in text-based passwords [9].
4. Spyware attack: Spyware attacks like key logging and key listening cannot be used to break the graphical password schemes [19].
5. It is more time consuming if the attackers set the phishing websites to achieve the graphical passwords [9].

Here, we, discuss the limitations of graphical password.

1. This scheme takes long time for passwords registration and log-in process [9].
2. A large space is needed for this scheme as compared to text-based passwords [9].
3. Shoulder surfing: "As name implies, shoulder surfing means watching over people's shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are vulnerable to shoulder surfing "[9].

2.2 Captcha

Graphical password schemes were proposed to minimized the deficiencies of text-based passwords. Both the schemes graphical password and text-based password are threatened to spyware attacks. Spyware works as a software and it collects the information about computer's use and share that information to adversaries. Nowadays spyware has become the security threat for computer systems. Password collection by spyware has rapidly increased. So, a new technique is developed to resist spyware is known as Captcha.

The word Captcha was firstly introduced by John langford [19] of Mellon University, but it is said that the groundwork on Captcha is done already in 1996 by Mani Noar with the introduction of the idea of the turing test. The purpose of turing test is to distinguish between humans and robots [2]. Captcha stands for"Complete Automated Public Turing Test to Tell Computers and Human Apart"[20].

The area of computer science that deals with the creation of intelligent machines which seems to be think like human and react like a human is called artificial intelligence. Captcha is a test which is used to differentiate human users from automated programmers. It acts like a defense mechanism between the humans and internet. An excellent Captcha is that which is easy for humans but impossible for machines to solve. Captcha based systems depend on artificial intelligence

(AI) [20]. The main purpose of Captcha is to make the communication secure in the public network. Users have to face the Captcha challenge daily. A number of websites offer free registrations such as Gmail, Google, Facebook, Twitter, Yahoo and so many others. It is also used in conducting online polls and money transaction etc [20]. These websites incorporated the Captchas, to protect the registration process. Captcha test guarantees that in the online polling systems votes are casted by the humans, not by robots. Captcha check that the money transaction is done by the humans, not by the robots [19].

Captcha has a lot of applications and we discuss few of them here.

1. **Free Email Services**: A lot of companies such as Google, Yahoo, Rediff, Microsoft provide the users free email services, and in this way, they suffer from some special type of attack. As robots that sign up for thousands of email accounts every time [16]. To avoid this situation websites use the Captcha challenges and ask the users to prove that they are humans before get a free email account. For example Rediff uses Captcha to stop the robot to downloading the files from the account. Yahoo stops the robots from automatic registration from email accounts [19].

2. **Worms and Spam**: Captcha provides the valuable solution against the email worms and spam. In this way a user can adapt the criteria such as user only accepts an email if he knows that it is a human and from where this particular email is sent [19].

3. **Online Polls**: Captcha also provide the valuable solution for online voting system. IP address of voters is recorded and single user is not allowed to cast multiple votes [19].

4. **Online Games**: Online game is the another application of Captcha. It stops the web robots from playing games [19].

5. **Preventing Dictionary Attack**: In this application Captcha is used to stop a computer from iterating through the whole space of passwords by

hiring the humans to type the password. In password based system Pinkas [9] and Sander suggested the use of Captchas to prevent the dictionary attack.

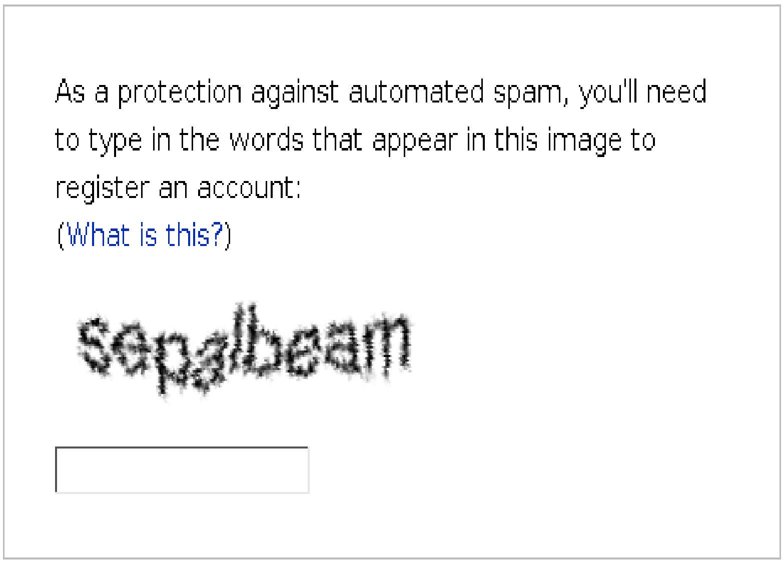
Captcha has many types but we discussed here two types only. We give a Figure here for the protection against the robots and for registration process we have to first fill the showing text into box [20]

2.2.1 Types of Captcha

1. Captcha as text type
2. Captcha as image type

Definition 2.2.1. (**Captcha as Text**).
This type of Captcha deals with the text which is not solvable by robots because, its shape is fuzzy and only humans can type this text into boxes. Firstly, humans have to judge the letters which are shown in the screen. A wrong guess of Captcha text changes the text and gives new text to type. Alphabets are used in text Captcha [19].

Example: For example Figure 2.4 is the example of Captcha as text in which we can see a distorted letter and a text box in which user is asked to fill the text correctly.

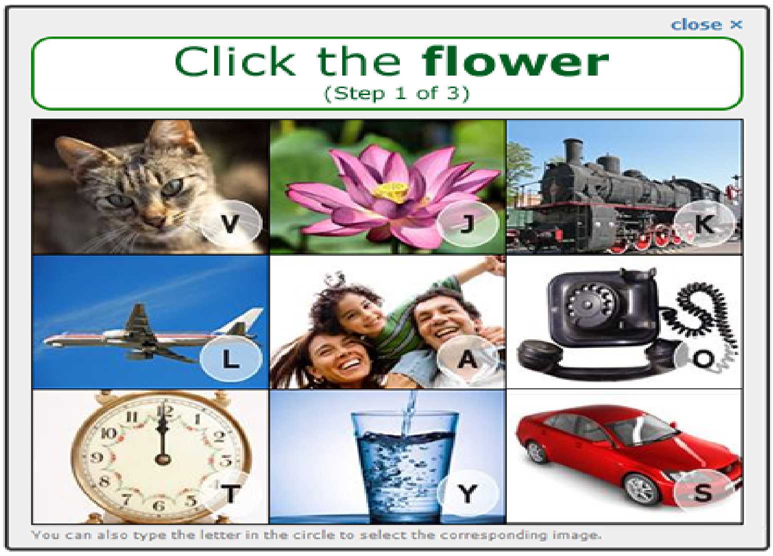


As a protection against automated spam, you'll need to type in the words that appear in this image to register an account:
(What is this?)

Figure 2.4: Captcha as Text

Definition 2.2.2. (**Captcha as Image**).
In this type of Captcha users are facilitated with an image and users have to guess those pictures that have some similarity. For example visual puzzles [19].

There are three rounds in image-based Captcha and in each round user have to guess that image which he or she selected in the registration phase. Face



close ×

Click the **flower**
(Step 1 of 3)

You can also type the letter in the circle to select the corresponding image.

Figure 2.5: Captcha as Image

Captcha, sound Captcha, audio Captcha and video Captcha are also the examples of Captcha. As graphical password, Captcha has also few drawbacks which we discuss here

1. Sometimes Captcha texts are in too much fuzzy shape that makes the text difficult to read.
2. Users with disabilities as like weak eye sight cannot judge the letters of the text. [9].
3. Sometime it is very difficult to get the particular information because of time consuming by Captcha to complete the authentication process.
4. May greatly enhance the artificial intelligence [19].

Cryptanalysis Attack.

Any attempt which is made to break the cryptosystem without the knowledge of key is called cryptanalysis [22].

A number of attacks are existing in the field of network security. Here we discussed the few attacks which are helpful for our study such as :

Definition 2.2.3. (**Guessing Attack**). "Password guessing attack is the type of network attack. Here a legal user who has access rights to a computer and internet sources are exposed by recognising the user identity and password compactness of the legal user"[27].

Password guessing attacks may be further classified into two types.

Definition 2.2.4. (**Brute force attack**).

"It is a type of password guessing attack in which brute force tries every possible key, combination, or password to get the original or true information . Attacks like that takes time long to fulfill the process. Difficult password may put the brute force in hurdle and it takes the very long time to guess it correctly" [22].

Definition 2.2.5. (**Dictionary attack**).
"In this type of attack, an attacker, uses a dictionary of normal words and all possible try to recognise the user password" [27]

Definition 2.2.6. (**Machine Learning Attack**).
"Machine learning is the application of artificial intelligence (AI) that provides a system an ability to automatically learn and improve the experience without being explicitly programmed. Machine learning focused on the development of computer programs that can access data and use it for themselves"[27].

Definition 2.2.7. (**Active Passive Attack**).
"In the passive attack, an attacker is tried to eavesdropped the message or monitor the message during the transmission of the message. In active attack, an attacker is tried to modify the message or re create the message "[4].

After discussing the attacks there are some definitions which are necessary to include here.

2.3 Mathematical Background

Definition 2.3.1. (**Group**). "A non-empty set G equipped with a binary operation $*$ is called a group if [7]

1. $*$ is associative, i.e
   $a * (b * c) = (a * b) * c \ \forall a, b, c$ belongs to G
2. $*$ has an identity element, that is there exist an element e belongs to G such that $a * e = e * a = a$ ∀ a belongs to G.
3. Each element of G has an inverse with respect to $*$, that is, for every a belongs to G. there exists some b belongs to G such that
   $a * b = b * a = e$
   b is called an inverse of a and is denoted by a^{-1}".

Example 2.3.2. Let us discuss some examples of some sets with binary operations that make groups [7].

1. The familiar multiplicative properties of rational, real, and complex numbers show that the sets $\mathbb{Q}^+$ and $\mathbb{R}^+$ of positive numbers and same set of nonzero numbers under multiplication are abelian group [7].

2. The set $\mathbb{Z}^+$ under addition is not group. There is no identity element for $+$ in $\mathbb{Z}^+$.

3. The familiar additive properties of integers and of rational, real and complex numbers show that $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ and $\mathbb{C}$ under adition are abelian group [7].

4. The set $\mathbb{Z}^+$ under multiplication is not a group. There is an identity 1, but no inverse of 3 [7].

Definition 2.3.3. (**Semi-Group**)

"A non-empty set G equipped with a binary operation $*$ is called a semi-group if $*$ is associative i.e $a * (b * c) = (a * b) * c \; \forall \; a, b, c \; \varepsilon \; G$ " [7]

1. $\mathbb{R}$ is set of real numbers is a semi-group under binary operation $+$, since $+$ is associative, $\mathbb{R}$ is also semi-group under multiplication. These two semi-groups are not same, since the binary operation is different.

2. $\mathbb{R}$ is not semi-group under subtraction [7].

Definition 2.3.4. (**Turing Test**).

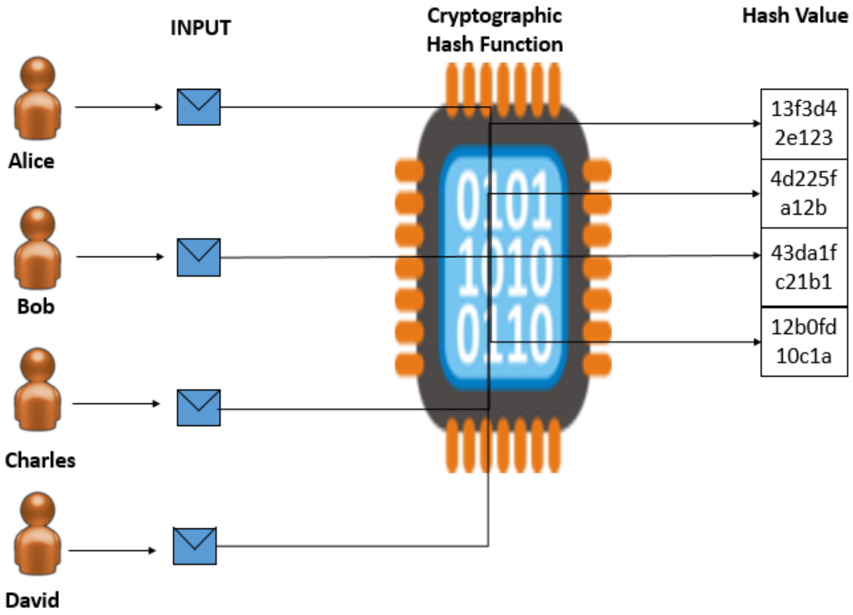
A test developed by Alan Turing in 1950 is known as a Turing Test. Its purpose was that whether a machine can think like a humans brain or not.

Definition 2.3.5. (**Hash Function**).

"A hash function is any function that can be used to map data of arbitrary size into fixed size. The values returned by a hash function is called hash values, codes or hashes. For most types of hashing functions, the choice of the function depends strongly on the nature of the input data, and their probability distribution in the intended application" [3]

A cryptographic hash function is a special class of hash function that has certain properties which makes it suitable for use in cryptography.
The ideal cryptographic hash function has the following five features.

1. It is deterministic so the same message always results in the same hash value.
2. It is quick to compute the hash value for any given message [22].
3. It is infeasible to generate a message from its hash value except by trying all possible messages a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value [3].
4. It is infeasible to find two different messages with the same hash value.



HashFunction

Chapter 3

Literature Review

In this chapter, we will discuss the graphical Captcha authentication, an overview of CaRP (Captcha as graphical password) and also discuss the examples and drawbacks of traditional scheme of CaRP. Before discussing the overview of CaRP we will discuss the framework of graphical Captcha authentication.

3.1 Graphical Captcha Authentication Framework

Authentication is the process between the server and user. Basic authentication process can be divided into three types.

1. **Knowledge-based authentication**: Knowledge-based authentication technique refers to the meaning that 'what you know' and it is just like passwords i.e, alphanumeric passwords[4]. This type of systems include both text type and image-based passwords. Image based passwords are also known as graphical passwords. It also tells that human beings have the great tendency to remember an image as compared to numbers or text. These type of systems also provide a security against many attacks. Also a big password space is provided as if it compared with text-based password [4].

2. **Token or possession-based authentication**: This technique of authentication means ‘what you have’ type of authentication. This technique includes key cards, smart cards, etc and are widely used to authenticate a system. A lot of applications are using this technique for authentication e.g. ATM cards are used together with PIN number[4].

3. **Biometric-based authentication**: This technique refers to ‘what you are’ type of authentication. In this technique user can use his or her finger prints as physical traits and use these traits as password authentication. The main demerit of this technique is that they are very costly [4].

3.2 CaRP: An Overview

Captcha has some limitations such as: sometime Captcha text is very difficult to read and technical difficulties with certain internet browsers etc. So, a new security primitive which is based on hard AI problem is developed and it is the combination of both Captcha and graphical passwords. It is called as CaRP (Captcha as graphical passwords).

CaRP is called clicked-based graphical password. To derive a password from an image a seriers of clicks is used. CaRP schemes are different from graphical passwords, images which are used in CaRP are like Captcha challenges and in this scheme every time different image is generated [9].

Captcha is an independant entity, which is used together with text or graphical password. For the same user, a new image is generated in every log-in attempt in CaRP. CaRP uses the visual objects, objects may be an alphabet(e.g, alphanumerical characters, similar animals) to generate a CaRP image, which are also called Captcha challenges. A very major difference between CaRP and Captcha is that all the visual objects which are appeared on the user screen, a user can click any input as a password in CaRP image but it is not necessarily happend in the Captcha image. Many Captcha schemes are converted to CaRP schemes [9].

CaRP schemes are classified into two types.

1. Recognition-Based CaRP

2. Recognition-Recall CaRP

3.2.1 Recognition-Based CaRP

"In this scheme, a sequence of visual objects in the alphabet is used as password. As per view of traditional recognition-based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects" [2].

There are three techniques under this scheme.

1. **ClickText**: "In Clicktext, Captcha system will generate image of alphanumeric character and user have to click on that image and enter password in the same order. It uses 2D (two dimensional) grid" [2].

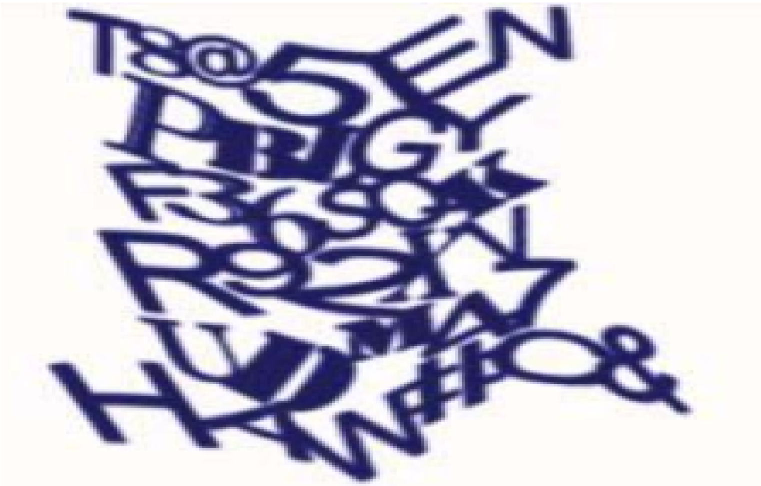


FIGURE 3.1: ClickText Image

2. **ClickAnimal**: "ClickAnimal is a recognition-based CaRP scheme built on top of Captcha zoo. Here an alphabet consists of similar animals e.g dog, horse, pig etc. For every animal $3D$ model is used. By using a Captcha generation process, ClickAnimal images are generated. Here $3D$ models are used to generate $2D$ animals by using different views, colors, textures,

lightning effects and if require distortions. The resulting $2D$ animals are placed on cluttered background. In the $2D$ model of ClickAnimal image, sometimes it is possible that some animals may be covered by other animals in the image, but their core parts are not covered so that humans can easily identify them but it is difficult for robot to identify such covered images as shown in figure 3.2" [2].

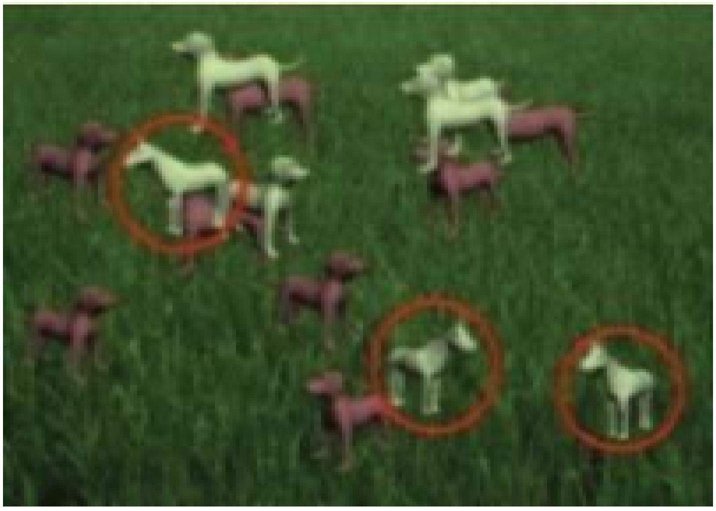


Figure 3.2: ClickAnimal Image

3. **AnimalGrid**: "It is a combination of Click A Secret (CAS) and ClickAnimal. In this system, firstly ClickAnimal image is displayed, after the animal is selected, an image of $n * n$ is appears" [2].

3.2.2 Recognition-Recall CaRP

"In this type, the password is the sequence of some invariant points of objects. An invariant point of an object is a point that has fixed relative in different interactions of object and thus can be uniquely identified by humans. No matter how the object appears in the CaRP images" [9].

A user must have to identify the object and have to click the invariant points on the image. Clicked points are used to match the password. These are the necessary steps to complete the authentication process. A user has to complete the process according to the given conditions [9].

There are two techniques under this scheme such as:

1. **TextPoint**: Characters contain invariant points in this technique. All the characters in the image has defined clickable points. To locate clickable points character recognition is must [2]. Robots have no capability to recognize the characters. In this technique, a password is used as a sequence of clickable points on a character. Single character can have many clickable points. That is why it is said that this technique has a biger space than ClickText [2].

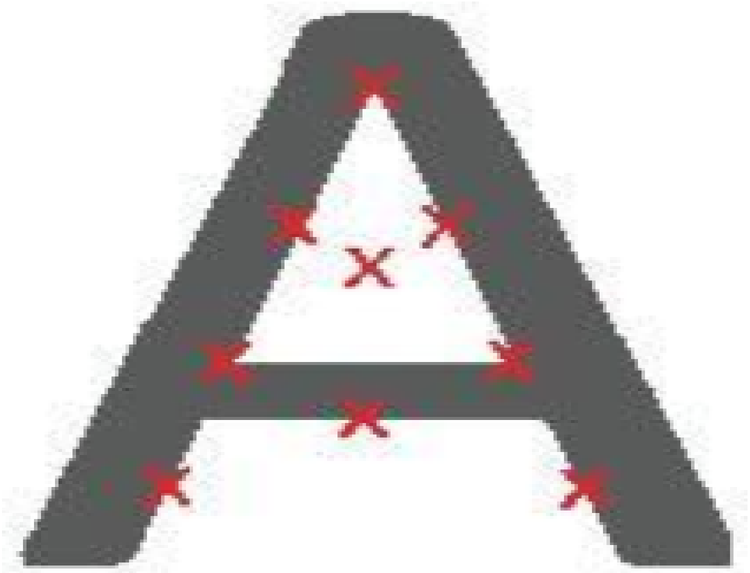


Figure 3.3: TextPoint Image

2. **TextPoint4CR**: In the Textpoint technique, hash value of password and salt is stored for every user and salt is some sort of secret information for every user. Password is directly stored by the server in TextPoint4CR technique. This is the major difference between these two techniques. It also has a difference that in TextPoint single character generate many time but in TextPoint4CR every character generate just once. A shared secret between server and user in TextPoint4CR is robust because no repetition of characters. Instead of password's hash values the server stores the password

directly and passwords are enciphered with a master key. Only server knows the master key and password is deciphered only when authorized account tries to log-in [2].

3.2.3 Traditional Framework of CaRP

In the traditional scheme, CaRP authentication server takes few steps for every user. Authentication server stores some information for every user the server stores a data like in this scheme authors used (s) as secret data and also stores the calculated hash value of password PW and data (s) in the form $H(PW, s)$ for every user. PW is the password and it is not stored.
A user selects a sequence of visual objects or clickable points as a CaRP password. When the server received the login request from the user side server will immediately produce an image and records the locations of the object and after that send this image to user. Server sends this image to user and user have to click on his or her password. Click point coordinates are recorded and send to the server along user ID.

The new points which the user clicked on the image are his or her password and these are denoted by PW'. The server put the received coordinates into the CaRP image to get the visual object ID_S or clickable points which the user select as his or her password PW'. Now the server has to recover the data s which is stored for the account, and the server calculates the hash value of PW' with the data and and compared this hash value with the stored hash value. If the hash value matches then the authentication procedure is successful otherwise terminates the procedure automatically [27].

3.2.4 Example of Traditional Scheme of CaRP

1. To minimized the unwanted emails a CaRP is used. A spam robot if it knows the password of the account can not be entered in to email account because

User	PW:Password(e.g,chars): s:data,H: secure Hash	Authentication server $\{UserID, H(PW, s), s\}$ (1) has a password table
	1: $\xrightarrow{\text{Authentication Request}}$	
	2: $\xleftarrow[\textbf{(2) no privacy protection}]{\text{Image}}$	Generate a CaRP Image
Click on Image $< x_1, y_1 >, < x_2, y_2 >, \cdots$	3: $\xrightarrow[<x_1,y_1>,<x_2,y_2>,\cdots]{\textbf{User ID}}$	
	4: $\xleftarrow[\text{Success or fail}]{\textbf{(3) one way authentication}}$	1. Recover PW' from $< x_1, y_1 >, < x_2, y_2 >, \cdots$ 2. $H(PW', s) = H(PW, s)$? : Yes success, No; fail

TABLE 3.1: Traditional CaRP Authentication

email service provider used the CaRP [9].

2. A CaRP is helpful for the secure internet applications like e-business, e-commerce, e-banking[5].

3. A password typing is complex on touch-screen devices and CaRP can be helpful here[9]

4. Now railway department uses the graphical Captcha as practice to avoids the access of robots[9].

   There is selling of 4.5 million tickets per day in China and China Railway is the one of the world's largest railway and it is the country with over 1 billion people and as a railway operator to maintain the security is a big issue. This rate can increase as 15 thousands tickets per minute during the peak days. www.12306 is a Chinese website and from this website users buy tickets for China railway trains [24].

   There is a lot of demand for tickets so, this website become a compulsory target for sophisticated attacker, because these attackers uses the automated attacks to buy big numbers of tickets and their purpose behind this is to resell them for high profit. So it is must for a Chinese railways to protect the Chinese users from fraud it is crucial duty of Chinese railway authority to higher or design a powerful Captcha. To handle these hurdles China railway system design a Captcha which is same as Google's reCaptcha. Users when want to buy a ticket, a buyer is facilitate within a phrase, which is written in unshaped Chinese characters, and eight pictures [24].

So buyer must have to select all of the pictures that are linked to the given phrase. To making this task complex for automated attackers the system has some special features. Text which is used in other Captchas unlike that text relevant phrase is really a unshaped, low resolution pictures of Chinese characters. Low resolution mean a screen shoots or pictures which is not seen clearly. After that, we will transfer the pictures of the phrases as codes or secrets and its purpose is to ignore confusion with the other pictures drawn in the captcha [24].

In addition to the secrets or codes, the given pictures are of a cheap quality and is subject to random noise. The low quality of both types of images make it difficult to develop effective algorithm. There is a complete absence of labeled data for both the codes and images . Its very important aspect of this type of security. [24].

3.2.5 Drawbacks of traditional Scheme of CaRP

1. CaRP technique is threatend by some attacks such as phishing attack is possible if clicked points are catched during the conversation between user and server [9].

2. In traditional CaRP authentication scheme the stolen verifier attack will become a big issue due to stolen password table [27].

3. In traditional CaRP the user ID is transmitted over the public channel which can lead to some potential attacks, such as the adversary can take in the history of user as least.

4. Only the server authenticates the user, but there is no any other way in which user authenticates the server, which can lead any adversary to start the impersonation attack [27]

Chapter 4

Review of CaRP Scheme Based on Chebyshev Polynomial Chaotic Map

In this chapter, we review the new CaRP scheme introduced by Zhu, Zhang and Xia [27] which is based on Chebyshev polynomial chaotic map. In their scheme, they used the public key encryption and hash algorithm with no password table in the server side to achieve the mutual authentication and privacy protection. After that, we discuss the example of proposed scheme [27].

4.1 New Framework of Captcha as Graphical Password

The scheme is based on hard AI problems and chaotic maps to achieve mutual authentication. So, we take start with Chebyshev chaotic maps.

4.2 Chebyshev chaotic maps

In this section, we firstly described the Chebyshev polynomials. The definition of Chebyshev polynomials [8] is given as follows:

Definition 4.2.1. "Let n be an integer and let x be a variable with the interval $[-1, 1]$. The Chebyshev polynomial
$T_n(x) : [-1, 1] \longrightarrow [-1, 1]$ is defined as $T_n(x) = \cos(n \cos^{-1}(x))$.
Chebyshev polynomial map $T_n : R \longrightarrow R$ of degree n is defined using the following recurrent relation: $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$,
where $n \geqslant 2, T_0(x) = 1$ and $T_1(x) = x$ " [27].

Here are some examples of Chebyshev polnomials:
$T_2(x) = 2x^2 - 1;$
$T_3(x) = 4x^3 - 3x;$
$T_4(x) = 8x^4 - 8x^2 + 1;$
$T_5(x) = 16x^5 - 20x^3 + 5x;$
Chebyshev polynomials satisfy the following important features [8].
(1) Semigroup property. Semi-group property is the very important property of Chebyshev polynomials.
"It states that: $T_r(T_s(x)) = T_s(T_r(x))$.
Infact,
$T_r(T_s(x)) = T_r(\cos(s \cos^{-1}(x)))$
$T_r(T_s(x)) = \cos(r.s \cos(x))$
$T_r(T_s(x)) = T_{rs}(sr \cos^{-1}(x))$
$T_r(T_s(x)) = T_{sr}(x)$
$T_r(T_s(x)) = T_sT_r(x)$.
where r and s are two integers and x belongs to $[-1, 1]$"[27].
"In 2008, to increase the security Zhang proved that Chebyshev polynomial also defined for the semi-group on the interval $[-\infty, +\infty]$ using the relation
$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) (\mod N)$,
where $n \geqslant 2$, $x \in (-\infty, +\infty)$ and N is a large prime number. Obviously,

$T_{rs}(x) = T_r T_s(x))$"[27].

We get the $T_0(x) = 1$ and $T_1(x) = x$, when $n \geq 2$ and putting in the relation $T_n(x) = 2xT_{n-1}(a) - T_{n-2}(x)$.

We fixed $n = 3$ and $N = 31$ and proceed as follows:

When $n = 2$

$T_2(x) = 2xT_{n-1}(x) - T_{n-2}(x) \mod 31$

$T_2(x) = 2xT_{2-1}(x) - T_{2-2}(x) \mod 31$

$T_2(x) = 2xT_1(x) - T_0(x) \mod 31$

$T_2(x) = 2x(x) - 1$

$T_2(x) = 2x^2 - 1$

When $n = 3$

$T_3(x) = 2xT_{3-1}(x) - T_{3-2}(x) \mod 31$

$T_3(x) = 2xT_2(x) - T_1(x) \mod 31$

$T_3(x) = 2x(2x^2 - 1) - x \mod 31$

$T_3(x) = 4x^3 - 2x - x \mod 31$

$T_3(x) = 4x^3 - 3x \mod 31$

Now, we put $x = 7$, in

$T_n(x) = 4x^3 - 3x \mod 31$

$T_3(7) = 4(7)^3 - 3(7) \mod 31$

$= 4(343) - 21 \mod 31$

$= 1372 - 21 \mod 31$

$= 1351 \mod 31$

$= 18 \mod 31$

Using semi-group property of Chebyshev polynomials

$T_r(x)T_s(x) = T_s(x)T_r(x)$.

And in the above example we put $x = 7$ and $T_3(7)$

These are equal to $(7, 18)$ and are public parameters [2].

(2) Chaotic property.

When $n > 1$, the Chebyshev polynomial map $T_n(x) : [-1, 1] \longrightarrow [-1, 1]$ of the degree n is a chaotic map. Chebyshev polynomials are oftenly used to solve the following two types which are infeasible to solved within polynomial time.

Definition 4.2.2. (**Chaotic Map-Based Discrete Logarithm** (CDL) **Problem**).
Let us consider an equation
$y = x^s \mod N$
Given s, x and N, it is very easy to compute y. We repeat the value of s to get the value y. However, two elements (x) and (y), it is infeasible to find the integer s, such that $T_s(x) \mod N = y$ it is called a chaotic map based discrete logarithm problem [8].

Definition 4.2.3. (**Chaotic Map -Based Diffie Hellman** (CDH) **problem**).
Given three elements $x, T_r(x) \mod N$ and $T_s(x) \mod N$, it is infeasible to find $T_{rs}(x) \mod N$ [8]. The security of the Diffie Hellman key exchange is lies in the fact that, it is relatively easy to calculate the exponentials modulo prime, it is very difficult to calculate discrete logarithms. So, an attacker, forced to calculate the discrete logarithm and this is not possible for an attacker in chebyshev chaotic map and this is known as a chaotic map based Diffie Hellman problem [8].

Due to drawbacks in the traditional scheme of CaRP Zhu [27], Zhang and Xia introduced a new framework. Author's new CaRP scheme is based on two phases:

1. Registration phase.
2. Authentication phase.

4.2.1 Registration phase

In the registration phase, author's aim is to achieve the risk diversification and for the sake of risk diversification authors shift the passwords from server to users. So, the authentication server must have the long key pair in the form of public and private keys and the server will have to use his own secret key to generate a proof which will help the user to prove herself in the future.

User	PW: password (e.g, chars): H: Secure Hash	Authentication server $\{publickey/\ privatekey\}$ (1) has no password table
stores proof v in a secure way	1: $\xrightarrow{\text{Register Request}}$ 2: $\xleftarrow{\text{Proof v}}$	compute a proof v using his secret key
Recover messages to authenticate the server, then click on image $< x_1, y_1 >, < x_2, y_2 >$, Authenticates itself with proof v. if holds, user recovers another proof v^*.	1: $\xrightarrow{\text{Authentication request with temporary key information}}$ 2: $\xleftarrow{E_{sk}\text{(serverID, image with coded method)}}$ 3: $\xleftarrow{E_{sk}(userID\|v*\|L(image)\|H(v*)\|L\{(image))}$ 4: $\xleftarrow{\text{success or fail}}$	Generate a CaRP image use secret key to recover enciphered data and compute v^{**}. compare $H(v^{**}\|L(image)) = H(v^*\|L(image))$ yes success, No fail.

Table 4.1: Enhanced CaRP Authentication Scheme

Table 4.1 shows that H a secure hash as a public parameter and PW as a password and the user send the register request with her password and identity to server. The authentication server, at the same time, eliminates password table and will use the private key to compute a proof v and send it to the user. The user stores the proof in a secure way in the form of $((PW)$ and or biometric). This proof help the in the future.

4.2.2 Authentication Stage

In this phase, we have to take the full advantage of proofs which includes the secret key of server and the proof v which is stored by the the user in the registration phase. Table 4.1 illustrates that, for the sake of authentication, server has not stored any type of information for any user. So if any user wishes to login to the server then he or she must have to send an authentication request to the server. The authentication request includes some temporary key information. Only between server and user, this information can produce the session key.

After receiving the authentication request, from the user, server will immediately generate a new CaRP image and transfer the image along with coded method to the user. Coded method means that a new algorithm that records the locations of the objects which are in image and the numbers or characters, so, in the result of getting the image from the server side user can click on the image and can recover his or her password and user authenticate herself on the basis of proof v which he or she already stored in the registration phase.

Table (4.1) also shows that, if the user can decipher the enciphered information, from the server side then we can judge that the user authenticates the server, because we know that the session is computed with the secret key of the server. When the user authenticates himself, or herself than, she computes another proof v^* for the sever validation. Now user used the public key of the server, and generate a new session key and encipher his ID, some necessary information and transfer to server.

At the last, server uses his secret key to decipher the data and calculates another proof v^{**}. Now server check the calculated hash values of both $H(v^{**}||L(image))$ and $H(v^*||L(image))$ and compares, if both give the same result then it is successful otherwise process terminates automatically.

Remark 4.2.4. "L is an algorithm and it transfer an image into fixed output bits (such as 128 bits). The CaRP image can be find quickly for humans, it can be classified as numbers, characters and special characters"[27].

Now we will discuss the example [27] that consists of three stages.

1. Registration Phase

2. Authentication Phase

3. Password Update Phase

The process of registration and authentication is almost, the same as they discussed in Section 4.1. We add a stage in the author's scheme and named it Initialization stage.

4.2.3 Initialization Stage

Parameter generation phase is also called the initialization stage. Server initially generates the system parameters, including the secret key K with the length of at least 128 bits, a random number $x \in (-\infty, +\infty)$ and one way hash function $H(.)$ [8]. We will discuss them, one by one.

Definition 4.2.5. (**Secure Channel**) A secure channel is a channel in which a message or secret information is free from overhearing and tampering. So here in this example [22] a secure channel is used in registration process and registration from secure channel make the process secure and costly [3].

Definition 4.2.6. (**Privacy Protection**) Privacy protection mean when some thing is personal and its secure from alternation and anyone cannot read it. In this example both the parties shared their information on public network and their information is protected from the adversaries [19].

Definition 4.2.7. (**Mutual Authentication**).
Mutual authentication, is a authentication process in which both sender and receiver have to give authentication of their identities. Its also called two way authentication. Mutually authenticates the both parties before starting the work or any type of data transfer over the public network [22].

4.2.4 Registration Stage

Stage 1: Registration is the process by which we enter the information to reach a specific destination. Here information is something about password or identity of user and destination mean a server to which we want to communicate. Alice is any user she wants to become a new legitimate user, to the server. For the sake of registration, user Alice selects her PW_A password, and password may be street number, house number, or anything else, B be any random number and uses her identity as ID_A which may be her name, mobile number etc.

After that, she concatenates the password with the random number B which she has selected and calculates the hash value and send this hash value within her identity ID_A using the secure channel towards the server. Figure 4.1 shows the registration stage.

Stage 2: Server receives the identity and hash value from the user, server used his secret key K based on Chebyshev polynomial chaotic map and concatenate it with the user identity after that server calculates the hash value of his secret key with the user identity. Now server used the XOR operation and then calculates the hash values and give it a name V, and $V = H(PW_A \Vert B) \oplus H(ID_A \Vert K)$ and sends V to user.

Stage 3 : User receives V and stores V, B safely. She stores the information into smart card and then completes the registration process.

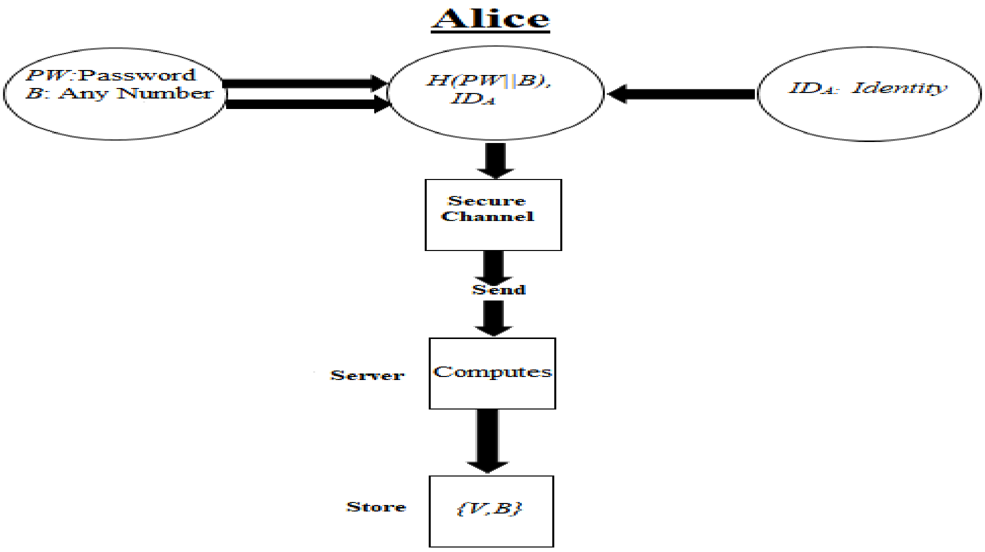


FIGURE 4.1: Registration Stage

	Secure channel	
Alice		Server
Compute $H(PW_A \Vert B)$	1: $\xrightarrow{(ID_A, H(PW_A \Vert B))}$	$V = H(PW_A \Vert B) \oplus H(ID_A \Vert K)$
	2: $\xleftarrow{(V)}$	
Stores $\{V, B\}$		

TABLE 4.2: Registration Stage

4.2.5 Authentication Stage

Now we will discuss the authentication stage in which the register user, Alice and sever both want to authenticate each other. So, in general when the parties entering into communication over a public channel then these parties have to send their identities to each other before going to transmitting any important information. Authors used the semigroup property of Chebyshev polynomial for the computation of session keys. User Alice, having the smart card can establish the authorized and secure session with the server. When the user Alice want to request some services, she firstly carry out mutual authentication after that, she consult for session key that will be used in the future for the secure transmission of data.

Stage 1: In the authentication phase, with the valid smart card the registered user Alice, wants to login to the internet server, then, she must have to choose any large random number a and calculates $T_a(x)$.

Then she refers the calculated value of $T_a(x)$ as authentication request to the server.

Stage 2 : When authentication server receives the authentication request which is the calculated value of the polynomial $T_a(x)$, server will immediately draw an image with coded method. Authentication server used his private key K for further computations and calculate

$T_K T_a(x)$, the authentication server encrypt

$C_1 = E_{T_K T_a(x)}(ID_S||$ image with code method

and transfer

C_1 to Alice. Where $T_K T_a$ are calculated using the semigroup property

$T_r(x)T_s(x)$.

Stage 3 : When the user Alice receives the image with coded method from the authentication server, Alice will take the few steps which we described below.

Firstly : She will use her impermanent and private key which is a and calculates the value of

$T_a T_K(x)$, using the semigroup property and checks the result of $T_K T_a(x)$ and $T_a T_K(x)$

and if both gives the same result then, she can decrypt C_1 to achieve the server's identity ID_S and a image with coded method. If the user is successful to get the server identity ID_S from the encrypted information, then we say that she authenticates the server.

Secondly: Using her memorable password, she clicks the image : which looks like $< x_1, y_1 >, < x_2, y_2 > .., ...$

Thirdly: Image with coded method which is send by authentication server, user Alice device can recover her password from the image $< x_1, y_1 >, < x_2, y_2 > ..., ...$ N is any number like V which we used in registration stage .

Fourthly: User used the proof V of the registration stage and apply XOR operation between V and hash value of PW and B . After that user checks the result of both $H(ID_A \| K)$ and $V \oplus H(PW_A \| B)$ and if the results are same then, she calculates a proof and give it a name N. User calculates

$$N = H(ID_A \| K) = V \oplus H(PW_A \| B),$$

Alice, encrypts the

$$C_2 = E_{T_a T_K(x)}(ID_A||N||L(image)||H(N||L(image))),$$

and transfer this C_2 towards authentication server.

Stage 4 : This is the mutual authentication step. When authentication, server receives the information C_2 from the user, the authentication server do the following steps. The authentication server used the calculated value of $T_K T_a(x)$ and recovered the encrypted information for the sake of getting the

$$(ID_A||N||L(image)||H(N||L(image))).$$

On the basis of identity ID_A the authentication server calculates

$$N^* = H(ID_A||K).$$

lastly the authentication server, calculates the result of both

$$H(N||L(image) = H(N^{*}||L(image).$$

If both are giving the same result then both are authenticate each other and the process will be successful otherwise, it terminates automatically. Figure 4.2 shows the authentication procedure completely

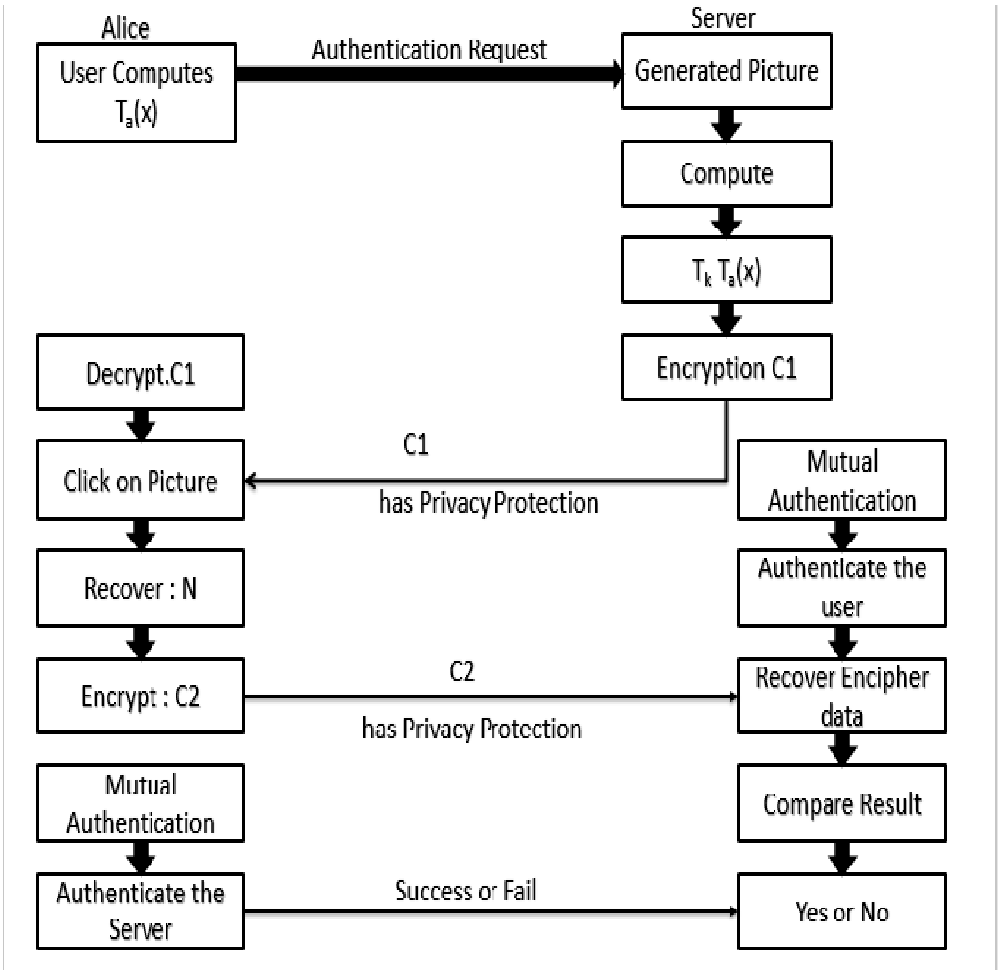


Figure 4.2: Authentication stage

use password to protect the proof	public parameters $H, (x, T_K(x))$	no password table
Bob		server
Select a large and random integer a		
compute $T_a(x)$		
	$\xrightarrow[T_a(x)]{\text{(Authentication request)}}$	
		Generate a new CaRP image with code method.
		compute $T_K T_a(x)$
		$C_1 = E_{T_K T_{a(x)}}(ID_S \vert\vert imagewithcodemethod)$
	$\xleftarrow[C_1]{\text{(has privacy protection)}}$	
Decrypt C_1 to get key information.		
Based on password to click on image:		
$< x_1, y_1 >, < x_2, y_2 >$		
Recover		
$N = H(ID_A \Vert K) = V \oplus H(PW_A \Vert B)$		Mutual authentication:
Compute		
$C_2 = E_{T_K T_{a(x)}}(ID_A \Vert N \Vert L(image)$		authenticate the user
$\Vert H(N \Vert L(image)))$		1: use$T_K T_a(x)$
		to recover a encipher data.
	$\xrightarrow[C_2]{\text{(has privacy protection)}}$	: Based on ID_A the sever computes N^*
		3: compare.
		$H(N \Vert L(image)) = H(N^* \Vert L(image))$?
		Yes: success, No: fail
	$\xleftarrow{\text{(success or fail)}}$	
mutual authentication:		
authenticate the server		

Table 4.3: Authentication Stage

4.2.6 Password Update stage

After the authentication stage we will discuss the password update phase in which any user, want to update her or his password with the server.

Stage 1 : In this stage, we discuss how a legal user Alice update her password with the server. So, if user, Alice has the wish to update her password with the server let say it to be A. User will have to select new memorable password which is PW^* and a new random number B^*. Then device of Alice again choose large and random integer a and calculate the value of the polynomial $T_a(x)$ together with

$$N = H(ID_A \Vert K) = V \oplus H(PW_A \Vert B)$$

and using the encryption technique and calculates

$$C_1 = ET_aT_{K_A(x)}(ID_A||H(PW^*\|||B^*)||H(N||H(PW^*\|||B^*))).$$

After this, user Alice transfer the $C_1, T_a(x)$ towards the server A where she firstly registers on.

Stage 2 : When the server A gets the information $\{C_1, T_a(x)\}$
from the user, the server takes the following steps.

Firstly : The server uses his secret key K and decrypt the C_1 for receiving the encrypted information

$$(ID_A||H(PW^*\|B^*)||H(N||H(PW^*\|B^*))).$$

On the basis of the identity ID_A, of the user, Alice the server computes another proof and gave the name as N^*. In this proof, table 4.4 shows that the server calculates the

$$N^* = H(ID_A||K) \text{ and } H^*(N^*||H(PW^*\|B^*)).$$

Lastly the server take the step of comparability and compare both the
N and N^*. Server checks whether the

$$H^*(N^*||H(PW^*\|B^*)) = H(N||H(PW^*\|B^*))$$

If server, achieves the same values then authentication process will be successful otherwise, it terminates immediately. If the process is successful then, sever calculates the another proof and named it V^*. Server concatenates the new password PW^* and new random number B^* and calculates the hash value of password and new random number. And apply the XOR operation between

$$H(PW^*||B^*) \text{ and } H(ID_A||K_A).$$

And completes the proof as

$$V = H(PW^*||B^*) \oplus H(ID_A||K_A),$$

Alice		Server
Inputs PW_A to get $H(ID_A\Vert K)$ Choose a new password PW^* and a random number B^* Select a large and random integer a. compute $T_a(x)$. $N = H(ID_A\vert\vert K) = H(PW_A\vert\vert B) \oplus V$, $C_1 = E_{T_a}T_{K_A}(x)(ID_A\vert\vert H(PW^*\vert\vert B^*)$ $H(N\vert\vert H(PW^*\vert\vert)))$	$\xrightarrow{(C_1, T_a(x))}$	Use K to decrypt C_1
		Compute $H(ID_A\vert\vert K)$ and authenticate Alice. If holds, the server computes $V \ = H(PW^*\vert\vert B^*) \oplus (ID_A\vert\vert K_A)$, $C_2 = E_{T_K}T_a(x)(ID_S\vert\vert V^*\vert\vert H(V^*\vert\vert H(PW^*\vert\vert B^*)))$
	$\xleftarrow{(C_2))}$	
Use a to decrypt C_2 and authenticate the server. If holds, replace the $\{V, B\}$ by $\{V^*, B^*\}$		

Table 4.4: Password Update Stage

Server encrypts the

$$C_2 = ET_KT_a(x)(ID_S||V^*||H(V^*||H(PW^*\|B^*)))$$

and transfer C_2 to user.

Stage 3 : When user, received the encrypted information from the server, user uses a to decrypt the C_2 and get the $(ID_S||V^*||H(V^*||H(PW^*\|B^*))$.

Then the device of user Alice will calculates the $H^*(V^*||H(PW^*||B^*))$ and verifies $H(V^*||H(PW^*||B^*))$.

If the values are matched then, user replaced $\{V, B\}$ by $\{V^*, B^*\}$. User Alice updated her password and the information or proof which she stores as $\{V, B\}$ changed within $\{V^*, B^*\}$.

This is the password update stage from which we choose the password as our wish.

4.3 Security Consideration

Local authentication : **AI problems security analysis**. Captcha depends on the difference of capabilities among humans and rebots in solving many hard

AI problems. Image Recognition Captcha (IRC) depends upon the recognition of non character objects. Security of IRC was found to be susceptible to machine learning attacks. On binary object classification the IRC based objects is likely insecure. Multi label classification problems are referred more better then binary classification problems.

[9] A CaRP image contains 30 or more characters ,and in our defined protocol a CaRP contains all the numbers and characters bec ause the server has no idea of the password of the user.

For making the better user experience, a CaRP image can be divided as numbers, characters and special characters in different area of the image. Because there is no theoretic security paradigm has been made, we just estimate the difficulty of image partition.

[19] It is seen in the setup that set C is exponentially depends on the number M of the objects which are used in the challenge, and polynomially depends on the size N of the Captcha alphabet $C = a^M P\langle N\rangle$, where $a > 1$ is a parameter, and $P\langle\rangle$ is a polynomial function. Typically a Captcha challenge contains 6 to 10 characters. A CaRP image contains 68 or more characters in their proposed protocol. The complexity to break a Click Text image is about $a^{68}P\langle N\rangle a^{10}P\langle N\rangle\rangle = a^{68}$ times the complexity to break a Captcha challenge generated by its underlying Captcha scheme. Th is is a big space which is tough enough [19].

Protocol Interaction: "A protocol is simply a set of rules or instructions that determine how to act or interact in a given situation. A cryptographic protocol is designed to allow secure communication under a given set of circumstances" [8].

Authentication proof based on the BAN logic.

Formal logic analysis is called the BAN logic and it based on the belief, and it achieves from the initial belief to the final purpose of the operation through sending and receiving of message during the running of the message. It is well known formal model used to analyze the security of authentication and key agreement schemes [8]. Firstly, based on hard AI problems, we can judge that the user can recover the authentication proof $N = H(ID_A||K) = V \oplus H(PW_A||B)$ securely.

For convenience, we discussed the notations, rules, goals and assumptions. Then we verify the validity of our protocol[8]. We discussed them one by one.

Notations and Rules First of all, let us define that P and Q are participants, and X is a formula. When we used BAN logic we have to use some notations and rules to analyse the BAN logic and these are as follows [8]

RULE 1 : The message meaning rule(N_1) (for shared secret keys)

$$\frac{P| \equiv P \longleftrightarrow Q, PX_K}{P| \equiv Q|\ X}$$

When Q send message X to p then he apply the encryption using the shared key K.

RULE 2 : The freshness rule (N_2).

$$\frac{P| \equiv (X)}{P| \equiv (X, Y)}$$

This shows that if one part of message X is fresh then its look that all the message must also be fresh [8].

RULE 3: The nonce verification rule (N_3)

$$\frac{P| \equiv\neq (X), P| \equiv Q|\ X}{P| \equiv Q| \equiv X}$$

In this rule if P believes that X is current message and that Q once said X,then P believes that Q believes X [8].

RULE 4: The jurisdiction rule (N_4)

$$\frac{P| \equiv Q \nRightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$$

If P and Q both have the jurisdiction over X, and P believes that Q believes the X then P believes X [8].

RULE 5 : The belief rule (N_5)

$$\frac{P| \equiv Q| \equiv (X, Y)}{P| \equiv Q| \equiv X}$$

This shows the believes and all of these rules show that how principal handles many messages [8]

The idealized form of our protocol is as shown.

1. Message 1: $(\text{Alice} \longrightarrow S)m_1 : S \triangleright T_a(x)$
2. Message 2: $(S \longrightarrow \text{Alice})m_2 :$ $\text{Alice} \triangleright C_1, ID_S, imagewithcodedmethod_{\text{Alice}} \longleftrightarrow S(T_K T_a(x)),$
3. Message 3: $(\text{Alice} \longrightarrow S)_{m_3}$:
   $S \triangleleft C_2, \{ID_A, N, L(image), (H(N||L(image))\}_S \longleftrightarrow \text{Alice}(T_a T_{K(x)})$ [27].

First of all, we convert the process of our protocol to the following idealized form.
$(\text{Alice} \longrightarrow S)m_1 : S \triangleright T_a(x)$ with authentication request.
$(S \longrightarrow \text{Alice})m_2 : \text{Alice} \triangleright P_1, ID_s, imagewithcodedmethod_{\text{Alice}} \longleftrightarrow S(T_K T_a(x)),$
Goals : According to analytic set up of BAN logic and the demands of authentication agreement, our agreement should fulfill the following goals in table 4.5 .

According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our agreement in Table 4.6 .

Goals
Goal 1: Alice $\mid\equiv$ Alice $\overset{N}{\leftrightarrow} S$, Goal 2: Alice $\mid\equiv S\mid\equiv$ (Alice $\overset{N}{\leftrightarrow} S$
Goal 3: $S\mid\equiv$ (Alice $\overset{N}{\leftrightarrow} S$), Goal 4: $S\mid\equiv$ Alice$\mid\equiv$ (Alice $\overset{N}{\leftrightarrow} S$)
Where S means authentication server, N means the recovered or computable proof:

Table 4.5: Goals of proposed Scheme

Verification

Now authors use the rules and assumptions which are based on BAN logic for the analysis of their proposed protocol. The main features of the proof is described as:[8]

For m_2 :

Because m_1 is just a easy and impermanent cipher text, we set m_2 is the starting of the proof. According to the message m_2 and M_1, M_4 and dimensions of chaotic

Initial states	
M_1 : Alice$\mid\equiv\xleftrightarrow{T_K(x)} S$	M_2 : Alice$\mid\equiv\#(a)$
$M_3 : S\mid\equiv\#($ image with code method $)$	M_4 : Alice$\mid\equiv$ Alice $\xleftrightarrow{T_aT_K(x)} S$
$M_5 : S\mid\equiv$ Alice $\xleftrightarrow{T_KT_a(x)} S$	

Table 4.6: Assumption

maps, and relating with N_1, we could get $S_1 : S\mid\equiv Alice\mid\ m_2$

S_2 : Alice$\mid\equiv\#m_2$

Combine S_1S_2, M_4, M_5 and N_3, we get:

$S_3 : S\mid\equiv$ Alice$\mid\#ID_S$ Image with coded method

Based on N_5, we take away S_3 and get:

$S_4 : S\mid\equiv$ Alice$\mid\equiv\#$ image with coded method

Next, Alice will use her password to click the new image to recover the evidence $N = H(ID_A||K)$

For m_3 :

Based on m_3 , and relating with M_1,M_2 and N_1 , and relating with dimensions of chaotic maps, we could achieve: S_5 : Alice$\mid\equiv S\mid\ m_3$

Based on N_2 and M_2, M_3 , we could get $S_6 : S\mid\equiv\#m_3$

Based on N_4 achieve: S_6 : Alice$\mid\equiv S\mid\ m_3$

Based on N_2 and M_2, M_3 , $_4$,N_5,M_4, M_5 , we take apart S_6 and get:

$S_7 : S\mid$Alice$\mid\equiv\#\quad imagewithcodedmethod, S_8 : S\mid\equiv($Alice $\longleftrightarrow S)(N)$,

$S_9 : S\mid$Alice $\equiv S\longleftrightarrow$ Alice(N)

Combine: Because of the two party Alice, S communicate each and other few minutes ago, now they ensure the second one is online. Moreover, since the user can detect ID_S from the C_1

$H(N||L(image)) = H(N)||L(image))$ and based on $S_8, S_9M_1M_4M_5$

with chaotic maps problems, we could achieve:

Goal 1.Alice$\mid\equiv($Alice $\longleftrightarrow S)(N)$, Goal 2.Alice$| \equiv S| \equiv (\text{Alice} \longleftrightarrow S)(N)$,

Goal 3.$S| \equiv (\text{Alice} \longleftrightarrow S)(N)$,

Goal4.Alice$| \equiv (\text{Alice} \longleftrightarrow S)(N)$

According to (Goal 1 to Goal 4), we know that the both Alice and S_i achieve the mutual authentication based on the new time being a and the new image with code method.

4.4 Efficiency Analysis

4.4.1 The comparison among different algorithms

If we compared the scheme, which we have discussed in previous section to RSA [22] and ECC,[22] Chebyshev polynomial[22] computation problems offer smaller key sizes, efficient computation, as well as memory, energy and proxy savings. Chaotic map encryption algorithm, as a special form of motion, chaos means that in a certain non linear system can appear similar to the behavior of random phenomena without needing any random factors [28]. Chaotic system has the qualities of certainty, boundedness, sensibility to starting parameters and unpredictability, etc.

Chaotic maps encryption algorithm, based on two complex problems such has as chaotic maps Diffie Hellman [3] problem and the chaotic maps discrete logarithm problems. It has the unique semi group property of Chebyshev chaotic maps [3]. Chaotic maps encryption algorithm very nicely improves the efficiency and avoids the scalar multiplication and modular exponentiation when it compared with ECC [22] encryption algorithm. However Wang [3] proposed many procedures to solve the Chebyshev polynomial computation problem.

4.4.2 Efficiency of CaRP

To judge the efficiency of CaRP, we check the functions and competence and make a comparison between the CaRP and other Captchas in this section. We use the standard, for evaluation is easy to use, able to remember, trends of applications and safety escapes. They invited up 50 (30 males and 20 females) from different ranks of young people and their aged between 25 and 30, who living in much contact to network , and asked them to test the use of different Captchas respectively.
According to this experiment, we establish a comparison among Kim et al.s scheme [11], Olalere et al.s scheme [15], Rusu scheme [17], Athanasopoulos scheme [1] and Kim et al.scheme[10] and the proposed scheme. Table 4.7 shows that:

1. Kim at al.s scheme: A new image-based Captcha using the orientation of the polygonally cropped sub-images. In author's proposed scheme, we can see that among the 10 people 7.6 people said it easy to use and 6.5 people said it is able to remember and 4 people said it has a lot of scope of application and 9 people said it has safety loopholes [11].

2. Olalere et al.scheme: Investigating the effects of sound masking on the use of audio Captchas. In this scheme, we can see that from 10 people 7.5 people said it is easy to use and 5 said it is able to remember and it has a scope of application and 8 people said it has safety loopholes [15].

3. Rusu scheme: Generation and use of handwritten Captchas. In this scheme, we can see that 7 people ou of 10 people said it is easy to use and 4.5 said it is able to remember and only 1 said it has a scope of application. 6 people said it has safety loopholes [17].

4. Athanasopouloss scheme: Enhanced CAPTCHAs :Using Animation to Tell Humans Computers Apart. In this scheme, 6.5 people out of 10 people said it is easy to use and only 4 said it is able to remember. 4 people said it has a scope of application and 6 people said it has safety loopholes [1].

5. Kim et al scheme: A Captcha that identifies the gender of face images unrecognized by existing bender classifiers. We can see that, in this scheme, 8.3

people out of 10 said it is able to use and 6 people said it is able to remember. 4 said it has scope of application and 7 said it has safety loopholes [10].

6. CaRP: We can see from the author's scheme, that 10 people out of 10 people said it is able to use and 10 out of 10 said it is able to remember. 10 people out of 10 said it has a lot of applications and 10 out of 10 said it has safety loopholes [27].

They asked 1 to 10 to tell Captchas superiority, where only 1 indicates its difficult to use, would not be able to remember, few ranges of applications, a lot of safety escapes, while 10 shows the opposite results. Based on the experiment analysis, they can summarize it as that CaRP not only has vast use, but it also can achieves much human interests. That's why CaRP become the emphasis object for useful study. Testing results are given in table [27].

Scheme	[18]	[23]	[25]	[1]	[17]	CaRP
Easy to use	[7.6]	[7.5]	[7]	[6.5]	[8.3]	[10]
Able to remember	[6.5]	[5]	[4.5]	[4]	[6]	[10]
Scope of applications	$4(C)$	$4(MP)$	1	$4(C)$	$4(C)$	$10(C, MP, T)$
Safety loopholes	9	8	6	6	7	10
Note: C:computers, MP: mobile phones T: tablets						

Table 4.7: Efficient between CaRP and other Captchas

4.5 Security Analysis

Number of attacks are existing in the field of network security. Here we discussed the few types of attacks and security analysis on new scheme of CaRP such as :

1. **Anonymity**: User anonymity means if any attacker is there then makes it impossible for his or her to find out any information. Here it means that attacker $Alice^*$ can not find the information of the enlisted user Alice from the transmitted information. In our proposed authentication, stage the login request is $T_a(x) \mod N$ through the public channel. If the attacker $Alice^*$

want to forge the Alice, information he or she must solve the KA which is the shared keys.
However, computationally it is impossible to calculate the $T_aT_K(x) \mod N$ direct from the $T_a(x) \mod N$ which is based on CMDHP. Moreover, the log in request $T_a(x) \mod N$ is independent and different in every session, KA and the random number B is randomly selected and changed in every session. In the end we can say that our scheme, can get the user anonymity.

2. **Man-in-the-middle attack**: In this type of attack, an attacker makes a connection between the user and the server and it seems like that conversation is carried out them directly and relays the message between them. In our proposed scheme, an attacker would not be able to calculate the $H(ID_A\|K)$ which is related to the identity of user and private key of the server. Also, an attacker can not compute the value of
$KA = T_a(T_K(x) \mod N$ Because, a is temporarily selected random number in each session. So, an attacker do not sit between user and server as legal user. That's why we say, that our scheme resist to man in the middle attack.

3. **Mutual Authentication**: Mutual authentication refers to the meaning that the server and user can verify each other, and develop a mutual trust between them before they visiting the privacy information. In our work, only the legal user, who have the correct password and authenticated information can have the right to send the login request to the server and the server who has the correct key can verify the user request only. Therefore, we can say that this scheme can provide the mutual authentication between the legal user and the trusted server.

4. **Replay Attack**: This attack means that an attacker catches the message before starting the protocol or being a start and attack the current agreement. Both the user,s request $T_a(x) \mod N$ and the server response
$C_1 = E_{T_kT_a(x)}(ID_S\|imagewiththecodemethod)$ have change new random

number. So this scheme resists the replay attack because in every important message contains the fresh random number.

5. **Perfect Forward Secrecy**: Perfect forward secrecy means that if the current private keys of both server and user are compromised then the previously used session keys must be safe. In our scheme if the current keys are disclosed then the previous session keys SK $= T_K T_a(x)\ modN$ remains same, because different sessions have different random numbers, and computationally it is in feasible to solve $T_K(x)$ from $T_a(x)$ directly.

4.6 Conclusion

In this thesis, we conduct a comprehensive and traditional study about CaRP authentication scheme using the chebyshev polynomial chaotic maps [27]. Nowadays, most of researchers working about Captcha or CaRP scheme having password table in the server side [9]. They ignore the impersonation attack, stolen verifier attack, privacy protection and mutual authentication problems. However, through author's exploration, firstly, we give a traditional framework of enhanced CaRP authentication [27] scheme. If we choose different algorithms, which are based on new framework, numbers of enhanced CaRP authentication schemes can be designed [27]. Later, we discuss an example of enhanced CaRP authentication scheme in author's work. Overall, author's work is one step advanced in the security protocol of using hard AI problems for catching most existing security requirements [9]. It has reasonable security and usability and practical applications, So, new CaRP scheme in which we need no password table in the server side to get the mutual authentication has good potential for refinements, which call for useful future work [27].

Bibliography

[1] E. Athanasopoulos & S. Antonatos, "Enhanced captchas: Using animation to tell humans and computers apart". In *IFIP International Conference on Communications and Multimedia Security*, pages 97–108. Springer, 2006.

[2] S. S. Banne & K. Shedge, "CaRP: Captcha as a graphical password based authentication scheme". *International Journal of Advanced Research in Computer and Communication Engineering*, 5(1):2278–1021, 2016.

[3] L. M. Batten, "Public key cryptography: applications and attacks", volume 16. John Wiley & Sons, 2013.

[4] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, & P. Bhogle, "Comparison of graphical password authentication techniques". *International Journal of Computer Applications*, 116(1), 2015.

[5] S. Chiasson, P. C. van Oorschot, & R. Biddle, "Graphical password authentication using cued click points". In *ESORICS*, volume 7, pages 359–374. Springer, 2007.

[6] M. J. M. Chowdhury & N. R. Chakraborty, "Captcha based on human cognitive factor". *arXiv preprint arXiv:1312.7444*, 2013.

[7] J. B. Fraleigh, "A first course in abstract algebra". Pearson Education India, 2003.

[8] G. Gao, X. Peng, Y. Tian, & Z. Qin, "A chaotic maps-based authentication scheme for wireless body area networks". *International Journal of Distributed Sensor Networks*, 12(7):2174720, 2016.

[9] A. Gokhale & V. Waghmare, “A study of various passwords authentication techniques”.

[10] J. Kim, S. Kim, J. Yang, J.-h. Ryu, & K. Wohn, “Facecaptcha: a captcha that identifies the gender of face images unrecognized by existing gender classifiers”. *Multimedia tools and applications*, 72(2):1215–1237, 2014.

[11] J.-W. Kim, W.-K. Chung, & H.-G. Cho, “A new image-based captcha using the orientation of the polygonally cropped sub-images”. *The Visual Computer*, 26(6-8):1135–1143, 2010.

[12] Y.-L. Lee & C.-H. Hsu, “Usability study of text-based captchas”. *Displays*, 32(2):81–86, 2011.

[13] P. Newswire, “Ticketmaster launches new”. *Innovative CAPTCHA Solutions, Making The Fan Experience Better, PR Newswire US*, 2013.

[14] C. Obimbo, A. Halligan, & P. De Freitas, “Captchall: an improvement on the modern text-based captcha”. *Procedia Computer Science*, 20:496–501, 2013.

[15] A. Olalere, J. H. Feng, J. Lazar, & T. Brooks, “Investigating the effects of sound masking on the use of audio captchas”. *Behaviour & Information Technology*, 33(9):919–928, 2014.

[16] Y. Rui & Z. Liu, “Artifacial: Automated reverse turing test using facial features”. *Multimedia Systems*, 9(6):493–502, 2004.

[17] A. Rusu, A. Thomas, & V. Govindaraju, “Generation and use of handwritten captchas”. *International Journal on Document Analysis and Recognition (IJDAR)*, 13(1):49–64, 2010.

[18] S. B. Sahu, “Secure user authentication & graphical password using cued click-points”. *arXiv preprint arXiv:1505.01594*, 2015.

[19] B. S. Saini & A. Bala, “A review of bot protection using captcha for web security”. *IOSR Journal of Computer Engineering*, 8(6):36–42, 2013.

[20] V. Saxena, “A study on user friendly approach: Captcha”.

[21] Y. Soupionis, R.-A. Koutsiamanis, P. Efraimidis, & D. Gritzalis, “A game-theoretic analysis of preventing spam over internet telephony via audio captcha-based authentication”. *Journal of Computer Security*, 22(3):383–413, 2014.

[22] W. Stallings, “Cryptography and network security: principles and practices”. Pearson Education India, 2006.

[23] S. Waghmare, S. Sikhwal, S. Nimje, & T. Pawar, “History of cryptography”.

[24] H. Ya, H. Sun, J. Helt, & T. S. Lee, “Learning to associate words and images using a large-scale graph”. *arXiv preprint arXiv:1705.07768*, 2017.

[25] T.-I. Yang, C.-S. Koong, & C.-C. Tseng, “Game-based image semantic captcha on handset devices”. *Multimedia Tools and Applications*, 74(14): 5141–5156, 2015.

[26] B. B. Zhu, J. Yan, G. Bao, M. Yang, & N. Xu, “Captcha as graphical passwordsa new security primitive based on hard ai problems”. *IEEE transactions on information forensics and security*, 9(6):891–904, 2014.

[27] H. Zhu, Y. Zhang, & Y. Xia, “Enhanced graphical captcha framework and applications to strong security authenticated scheme without password table”. *Journal of Information Hiding and Multimedia Signal Processing*, 6(6):1295–1309, 2015.

[28] H. Zhu, Y. Zhang, Y. Xia, & H. Li, “Password-authenticated key exchange scheme using chaotic maps towards a new architecture in standard model.”. *IJ Network Security*, 18(2):326–334, 2016.