Numerical Modeling of A New Virtual Trajectory Password Architecture

Yuanyuan Chen¹,*, Jing Chen² and Mingzhu Li³
¹,³Haikou University of Economics, Haikou, China
²Qingdao City University, Qingdao, China

*Corresponding author email: 252009674@qq.com

Abstract. With the development of digital technology, Computer technology, communication technology and multimedia technology gradually infiltrate into each other and become the main core of information technology. In information technology, digital, text, graphics, images, sound, video, animation and other information carriers are spread through computers and the Internet. Due to the openness, sharing, dynamic and other characteristics of the Internet, information security is threatened and interfered. Information security has become a strategic issue that people must pay attention to, which is related to social stability, economic development and national security. This paper studies a new kind of virtual track cryptography, which breaks through the traditional character memory method and transforms it into memory graphics by using mathematical modeling, and changes the surface memory method from memorizing numbers and characters to memorizing trajectory graphics, so as to make the traditional process of people memorizing passwords easier.

Keywords: Virtual trajectory, password, security, algorithm, numerical modelling.

1. Introduction
In the era of rapid development of the Internet, it is quite common to use mobile phones for online shopping, information inquiry, bank transfer, account recharge and other services. When users register and log in, they need to register account password for information security, that is, use password for security verification. Password is a tool to protect one's own privacy, property, information and important data. However, some criminals break the password, peep and steal other people's important information and data through technical means, causing data and property losses [1]. Due to the openness, sharing and dynamic characteristics of the Internet, information security is threatened and interfered[2]. Information security has become a strategic issue that people must pay attention to, which is related to social stability, economic development and national security. At the same time, in the verification operation through the mobile phone, it is often required to remember the passwords of various operations. There are many kinds of passwords, which are easy to cause memory confusion [3-4]. In view of this, people urgently need a password authentication method which can help memorize passwords, prevent peeping, and is difficult to decipher and protect password information security.

2. The Research Significance
There are several factors to develop this kind of virtual trajectory password.

2.1 The First Factor
At present, all kinds of widely used software passwords often use short 6-digit password (such as bank password) or the so-called security password with letters and numbers as the verification and login...
password[5]. This kind of short password is also vulnerable to the computing power of modern ordinary computers, and the super long password is not easy to remember.

2.2 The Second Factor
At present, in order to make the password not easy to be cracked illegally, people use many modern technology methods, such as displacement keyboard, "two-dimensional code" scanning verification, third-party platform verification, fingerprint verification, mobile phone verification code and so on[6]. But in the process of data storage and network transmission, it is inevitable to be illegally monitored, intercepted and stolen.

2.3 The Third Factor
With the rapid development of China's economy, network information security is an inescapable topic, and password security is the first problem. To develop a new password verification system and to simplify the long password memory method is in line with the current needs of China's national conditions.

In this paper, a new architecture of "virtual trajectory password" is studied, which breaks through the traditional method of memorizing characters, changes it into memorizing graphics, and automatically converts it into actual character cipher by our self-designed system, and changes the familiar surface memory method from memorizing numbers and characters to memorizing graphic trajectory, So that the process of people memorizing passwords becomes easier.

3. The Architecture Design
"New virtual trajectory password", hereinafter referred to as virtual trajectory password, provides a new method for people in password verification login means. It can help people remember and use complex super long password, and has the characteristics of preventing peeping and being difficult to decipher. The specific design is as follows.

3.1 Design of Encoder
In order to facilitate the user to remember the password, it is convenient for the user to remember the simple "input seed code" by generating a constantly changing random reference graph - "code disk". This seed code is a constant graphic code during the user's input and verification, and this simple seed code, is the lead that the system uses to generate the actual, extra-long, encrypted, "code base" covering the entire ASCII code table, which is the actual transmission and storage password.

It has designed a 36-digit alphanumeric figure with 6 rows and 6 columns. We call it the "code disk ", and the user's virtual trajectory password is to use the code salver as a reference graph to facilitate memory password. The graph of code salver is shown in Figure 1.

![Figure 1. A random code salver diagram.](image1)

![Figure 2. The diagram of mobile phone dial unlocking.](image2)
3.2 The Design Thought of Code Disk

In real life, the passwords that most people use are basically relatively simple, short passwords with definite meaning, this is because people overestimate the difficulty of hacking and decoding their passwords and underestimate the risk that their own passwords will be compromised. Therefore, the following aspects are not considered when using the password: ① the composition of the elements of the password (code base), and the use of a simple number type of password in the majority. ② Password length (number of digits) 6-8 passwords in the majority. Random scrambled passwords and passwords with more than eight digits are rare because they are hard to remember. However, these are also relatively secure passwords.

Inspired by the mobile phone dial unlocking method (as shown in Figure. 2), it is noted that the password is graphics. As we all know, it is easier for people to memorize specific graphics than abstract numbers and characters. However, this method is not very private when it is used, and it is easy to be peeped, and the number of its code base is only 9, and the generated password is not difficult to crack. Can we design a trajectory code that is easy to remember and can't be seen by others? The answer is yes. The design of the virtual trajectory password method, that is to solve the password "easy to remember" and "super long" contradiction.

Instead of memorizing a character password, people can simply remember a "virtual trajectory" on a code disk. When the system is running, click the password input box, and the system will automatically pop up the "code disk".

3.3 The Generation of “Code disk”

A 6 by 6 code disk is a two-dimensional matrix, and we define a two-dimensional array to describe it. Each array element can appear randomly in (0-36) code bases. The following is the instantaneous data of a random code disk, as shown in Figure.3.

| Scd(1,1)| Scd(1,2)| Scd(1,3) | Scd(1,4) | Scd(1,5) | Scd(1,6) |
|--------|--------|---------|---------|--------|--------|
| 4      | t      | j       | q       | 6      | w       |
| y      | b      | x       | m       | 3      | l       |
| i      | n      | 7       | h       | v       | f      |
| 9      | p      | z       | o       | 5      | d       |
| s      | w      | 2       | e       | r      |        |

The code disk is generated according to the continuous elements (code base) according to the randomly generated position, so as to ensure that all code base elements are placed on all code disks, and there are no duplicate elements, so as to ensure that when the selected password trajectory overlaps on the code disk, the system can still correctly distinguish without ambiguity path.

3.4 Two Dimensional Matrix Encoder and One Dimensional Matrix Encoder

Two dimensional matrix: the elements of the matrix are two-dimensional vectors, that is, two-dimensional matrix. We usually see code disks, such as 3 * 3 two-dimensional code disks on mobile phones. As shown in the figure below, the code disk contains 9 code bases.

![Figure 3. Two dimensional matrix of code disk elements.](image)

![Figure 4. The yellow is the virtual track of user memory.](image)
One dimensional matrix: the elements of the matrix are one-dimensional vectors, that is, one-dimensional matrix. We can convert the two-dimensional matrix into one-dimensional matrix. For example, the above two-dimensional matrix into one-dimensional matrix can be changed into:

\[
A = \begin{pmatrix}
A(1, 1) & A(1, 2) & A(1, 3) \\
A(2, 1) & A(2, 2) & A(2, 3) \\
A(3, 1) & A(3, 2) & A(3, 3)
\end{pmatrix}
\]

It can be transformed into:

\[
A = a(1), a(2), a(3), a(4), a(5), a(6), a(7), a(8), a(9)
\]

3.5 The Formation of Virtual Trajectory

As we can see from a random code disk in Figure. 4, each element in the array is the character displayed on the code disk. If the user selects an element and inputs it, the system will get its position on the code disk. When continuous or discontinuous points are selected, there will be a certain position trajectory. These selected positions are combined into a continuous (or discontinuous) position sequence to obtain its motion trajectory on the code disk, which is called "virtual trajectory".

4. The Generation of Actual Password and the Principle of Encryption

The password finally generated in the system is not stored in the form of the location of the trajectory pattern matrix, but only as a "seed", which is stored in the form of the password sequence generated by a series of mathematical transformations. When the track password is obtained by the system, it becomes a super-long password which covers the storage and transmission of the entire ASCII code table after encryption and base expansion.

We know that when the password is long enough and the code base is large enough, it is difficult to decipher (High timeliness cost) even if it is intercepted by others. This greatly enhances the security of the password. At the beginning of the design of "virtual track password", there is no limit on the number of digits of the password, which is also the case in the user's practical operation to realize the design idea. The walking track of the virtual track password is allowed to walk at will on the code disk continuously or discontinuously, cross or not. In order to enhance the security and reliability of virtual trajectory cryptography, we adopt the basic theory of chaotic cryptography; The excellent characteristics such as randomness, ergodicity, certainty and sensitivity to initial conditions are reflected in the chaotic characteristics in the range of its value distribution, and this chaotic characteristic just provides a guarantee for us to generate a super secure cipher sequence.

Logistic chaotic model (also known as insect-population model) was originally a mathematical model to describe the reproduction of biological population in ecology, but later evolved into a mathematical model to study random phenomena. See formula 1.

\[
x_{n+1} = ux_n(1 - x_n)
\]  

The letter n is a natural number (1,2,3,...), when X1 is fixed, the initial value is selected, the value of u is used to control the change of the whole function value, and an infinite repeatable random number sequence can be obtained through infinite iterations.

By observing Figure. 5, in the chaotic interval, we can see that a large number of initial values of real numbers can be selected differentially when u is between real numbers [1,4]. When the initial value is selected, a large number of random numbers can also be obtained when u is between 3.8-4.0 (except for some regions).
The generation of virtual trajectory password is the password sequence generated by using the chaotic sequence generated by the chaotic system and the reproducible random number generated by the user's seed trajectory code (initial value) after the selected formula transformation in the client, as shown in Figure 6.

In password verification, the same seed can be used to regenerate the previous password sequence through the chaotic system, and the same password stream can be generated through the same reverse process to verify the user; the seed cipher sequence input by the user is not transmitted, but the super long generated cipher is transmitted. The encryption end and decryption end of the chaotic cipher system are two independent and identical chaotic systems.

The chaotic stream encryption algorithm uses the perturbation algorithm based on the chaotic sequence itself to overcome the problem caused by its limited precision effect. At the same time, the coding algorithm and nonlinear transformation are used to further improve the randomness of the chaotic system and the output sequence. Theoretically, the period of the random sequence generated by the algorithm can reach at least $128^{60}$.

5. Conclusion
This paper designs a new architecture of virtual trajectory password, which breaks through the traditional method of memorizing characters and changes it into memorizing graphics. By generating a constantly changing random reference graph "code disk" as a means of auxiliary memory, it helps human beings remember some special extended passwords that cannot be memorized routinely. In the aspect of password verification and login, it provides a new method for people, which makes it easier for people to memorize the traditional process of password and complete it by memorizing the trajectory graph.

Acknowledgments
This research was supported by Hainan Provincial Natural Science Foundation of China (620QN285), Haikou University of Economics Scientific Research Project (HJKY (ZD) 20-10).

References
[1] Tsai, Jia-Lun; Wu, Tzong-Chen; Tsai, Kuo-Yu. New dynamic ID authentication scheme using smart cards International Journal of Communication Systems, 2010.
[2] Xie, Qi. A new authenticated key agreement for session initiation protocol International Journal of Communication Systems, 2012.
[3] S.Kumari; M.K.Gupta; M.Kumar. "Cryptanalysis and security enhancement of Chen et al. "s remote user authentication scheme using smart card," Central European Journal of Computer Science, 2012.
[4] Chen, Chun; He, Daow; Chan, Sammy; Bu, Jiajun; Gao, Yi; Fan, Rong. Lightweight and provably secure user authentication with anonymity for the global mobility network International Journal of Communication Systems, 2011.
[5] Cuiping Ma, Jiahui Liu. ”Design and Implementation of a Hash Algorithm Based on Chaotic Logistic Equation”. Harbin University of Science and Technology.

[6] Li Zhengtao. User Identity Authentication Technology for Mobile Social Network Applications, Nanjing University of Posts and Telecommunications, 2017.