Validation of the Parameters Used in the TFinger System to Generate Cryptographic Keys and Passwords with Fingerprint and Safety Assessment of this System

Tigran, Andreasyan

National Polytechnic University of Armenia
Yerevan, Armenia
e-mail: tandreasyan@gmail.com

ABSTRACT

By fingerprint, certain parameters have been used to create cryptographic keys and passwords when developing the TFinger system [1], the changes of which have a significant impact on the accuracy of the results obtained from the system. The accurate selection of the parameters was carried out through experiments. The size of M, in the case of which, by spending the least amount of time, the greatest result of accuracy can be obtained, will be the most optimal, and the size is $M = 16$, as the number of segments, it is necessary to select number K, which is as large as possible and, at the same time, ensures the maximum output accuracy: $K = 6$. The deviation value on the number axis [a] should be as small as possible, since the greater it is, the greater will be the probability of getting the same data from different numbers: $a = 8$. Key information created by the TFinger system to generate cryptographic keys and passwords through fingerprints must be safe to confront the possible attacks. Three different attacks have been observed to assess the stability of the system: the attack with unique segments, the direct brute force attack, the interval brute force attack. The attack with unique segments is the attack, when the hacker should find out the configuration between the received segments. In the result $n \approx 10^{27}$. The direct brute force attack is to show how many possible variants the distances between the unique segments can be distributed in the digital range. In the result $q \approx 10^{25}$. The interval brute force attack is to show how many variants there are between the distances of unique segments to get statistical data. In the result $p \approx 3 \cdot 10^{11}$.

Keywords

Fingerprint, password, data, security, information, attack.

1. DETAILS

By fingerprint, certain parameters have been used to create cryptographic keys and passwords when developing the TFinger system [1], the changes of which have a significant impact on the accuracy of the results obtained from the system. These parameters are: the size of the picture (NxN), the dimensions of the segment (MxM), the number of unique segments (K) and the digital axis deviation value (a). The accurate selection of the parameters was done through experiments. 2000 experiments were performed.

The size of the picture depends on the choice of the fingerprint scanner, which depends on the size of the image the scanner returns. For example, for Targus PA460, $N = 192$.

Now let's present the reasons for the $M = 16$[1] size selection. The change in M has two types of effects on the system. First, depending on M, the accuracy of the result of creation of key information is changed, that is the percentage ratio of the general experiments carried out and the key information as a result. The results obtained from the experiments are shown in Fig. 1.

The latter clearly shows that almost exactly the right result is obtained between the 12…16 interval of M. That is, M must be chosen from that interval.

The second type of impact is the change of M on the performance of the system, is the operating speed. The smaller is M, the greater is the number of paces of software cycles during the operation of the system, the result of which is the following dependency (Fig. 2). The size of M, in the case of which, by spending the least amount of time, the greatest result of accuracy can be obtained, will be the most optimal, and the size is $M = 16$. And indeed, in the case of 16, the maximum output accuracy and relatively the optimal operation speed are obtained.

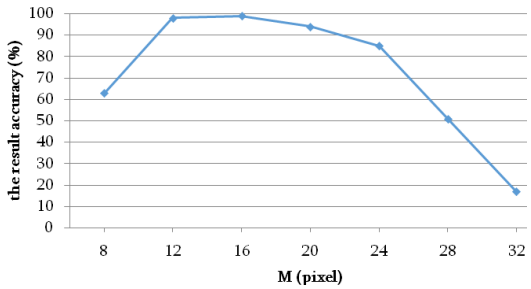

Fig. 1. The dependency of the accuracy of key information on the segment size obtained in the result of the system operation

Therefore, it is rational to take the $M = 16$ pixel as the optimal size of the fingerprint section in the TFinger system.

Experiments. Now, let`s study the sections that are maintained and used to create key information. The greater the number of these segments is, the greater is the chance to create secure key information (as the key information is created on the basis of mutual disposition of each of these segments). But, at the same time, the accuracy of the system's performance depends on the number of these segments. That is, as the number of segments, it is necessary to select number K, which is as large as possible and, at the same time, ensures the maximum output accuracy. Now, based on the results of the experiments, let us study the choice of that number. The graphical image of the data obtained in the result of experiments is illustrated in Figure 3.

It is clear from the graph that the high accuracy of the result (99%) is obtained with the maximum K value of 6. Therefore, as a unique number of segments, $K = 6$ was chosen.

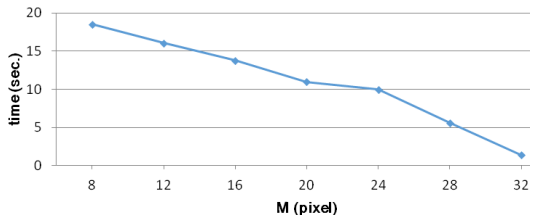

Fig.2. The dependency of the operating time of the system on the size of the segment

The deviation value on the number axis, [a] [1], should be as small as possible, since the greater it is, the greater will be the probability of getting the same data from different numbers. Obviously, the accuracy of the system performance depends on the value of a. It is necessary to choose such a, which should be at least minimal and at the same time, the accuracy of the system performance - maximum. As a result of experiments, it becomes clear that $a = 8$ (Fig. 4), as $a = 8$ is the minimum value, in which the high accuracy of the result (99%) is obtained.

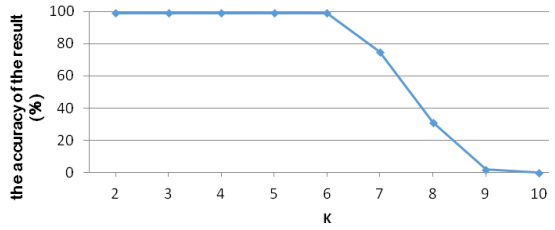

Fig.3. The key information accuracy dependency received from the system work on the number of segments

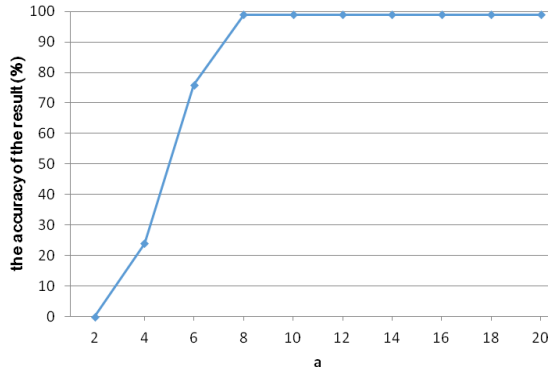

Fig.4. The key information accuracy dependency received from the system work on the deviation value

The key information created by the TFinger system to generate cryptographic keys and passwords through fingerprints must be safe to confront the possible attacks. And the possible attacks are dependent on the algorithm created by key information and the value of the parameters, which this algorithm uses [2]. Since key information is generated from some data (from fingerprint and input data) [3], the reliability and security of the generated keys and passwords depend on the security of this data. Three different attacks have been observed to assess the stability of the system:

- attack with unique segments,
- direct brute force attack,
- interval brute force attack.

Now let's study these attacks. The first is the attack with unique segments. Let us remind you that the unique segments of that image were separated from the fingerprint image [2], and the distance between which is calculated based on their configuration, which, after certain processing, are used in the process of key information creation [3]. Let's study the case when the brute force manages to break the TFinger system database and get specific segments from the user's fingerprint. In that case, the hacker should find out the configuration between the received segments. As there is no information stored in it, the brute force will only have to try all the possible variants.

All the possible positions of one segment on the picture can be calculated by formula (1):

$$m = (N - M + 1)^2, \quad (1)$$

where m - Á is the number of possible positions per segment, N - the size of one side of the image (as the image is square), M - is the size of one side of the segment. The second segment may be found in all positions except the position of the first segment. Therefore, the number of all possible positions will be $m - 1$, the third one will be $m - 2$ and so on. Consider, taking into account the total number of the configuration of K segments, n can be calculated by the formula (2):

$$n = (N - M + 1)^2 \cdot ((N - M + 1)^2 - 1) \cdot \ldots \cdot ((N - M + 1)^2 - (K - 1)). \quad (2)$$

As in the TFinger system $K = 6$, $M = 16$ [1], and as an experimental value of image size $N = 192$, result is $n \approx 10^{27}$. The number obtained shows how many variants should be observed by the brute force, with the help of exhaustive brute force, to find out the precise configuration of the segments.

The next attack, the direct brute force attack shows how many possible variants can the distances between the unique segments be distributed in the digital range. Let`s study what the distance of the two segments in the range of natural numbers is. Since the segments cannot be found in the same position, it is obvious that the minimum value will be 1. To calculate the maximum value, let's study Fig. 5.

The two farthest parts are the sections on both ends of the diagonal. Therefore, the maximum distance between the two segments will be the distance between them. According to Pythagoras' theorem for the equal rectangular triangle [4], the given distance L_{max} can be calculated by the formula (3):

$$L_{max} = \sqrt{2 \cdot (N - M)^2} \quad (3)$$

Consequently $L_{max} = [248.902] = 249$: which means that the distances between the segments are in $L \in [1,249]$ interval.

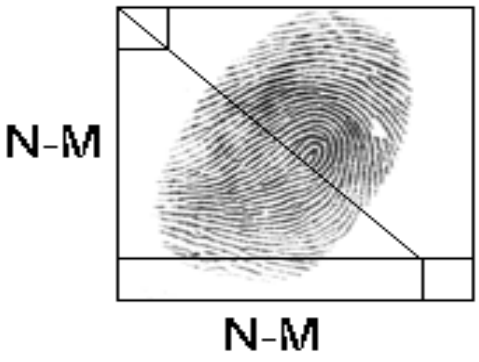

Fig. 5. The maximum distance between the segments

It turns out that 15 distances between the segments (*in the case of* $K = 6$- $C_L = 15$) [2] are in the stated range. Let's consider how many of these 15 numbers can be

distributed in the stated range. The number of q variations can be calculated by the following combination (4) [5]:

$$q = \left(\widetilde{\begin{matrix} L_{max} \\ C_L \end{matrix}}\right). \quad (4)$$

By simplifying the combination, we will get:

$$q = \left(\widetilde{\begin{matrix} L_{max} \\ C_L \end{matrix}}\right) = \left(\begin{matrix} L_{max} + C_L - 1 \\ C_L \end{matrix}\right) =$$
$$= \frac{(L_{max} + C_L - 1)!}{C_L!\,(L_{max} + C_L - 1 - C_L)!} =$$
$$= \frac{(L_{max} + C_L - 1)!}{C_L!\,(L_{max} - 1)!}$$

As $L_{max} = 249$, $C_L = 15$, $q \approx 10^{25}$: The number obtained indicates how many options the brute force, using exhaustive brute force, should consider to find out the real distributions $L \in [1{,}249]$ in the range $C_L = 15$.

The next attack is the interval brute force attack, the question is, how many variants there are between the distances of unique segments to get the statistical data. Using $a = 8$ shift size [1], statistical data are obtained from these distances. Now let's calculate p-the number of every possible variant of the data obtained of L distances. Since this method returns the same data from a specific number within the interval, you can assign that interval as a single point. The number of these ranges will be equal to the number of L distances C_L: In this case, the digital interval will turn from 1 to L', where: $L' = [\frac{L_{max}}{a}] = [31.125] = 31$: Consequently p-can be calculated (5) by the formula:

$$p = \left(\widetilde{\begin{matrix} L' \\ C_L \end{matrix}}\right). \quad (5)$$

Simplifying the given combination, we will get:

$$p = \left(\widetilde{\begin{matrix} L' \\ C_L \end{matrix}}\right) = \left(\begin{matrix} L' + C_L - 1 \\ C_L \end{matrix}\right) =$$
$$= \frac{(L' + C_L - 1)!}{C_L!\,(L' + C_L - 1 - C_L)!} =$$
$$= \frac{(L' + C_L - 1)!}{C_L!\,(L' - 1)!}$$

As $L' = 31$, $C_L = 15$, $p \approx 3 \cdot 10^{11}$, that is, the number of all the possible versions of the fingerprint data. But, as the user also enters additional data during the generation of key information, and the final data, on the basis of which the key information is created, are generated from the combination of fingerprints and input data, practically it becomes impossible for the brute force to get the right key information.

Now let's compare the TFinger system with the system working on other biometric technologies. The most popular systems (ATRx Secure PunchIn, BioDesk), working on the fingerprints have been tested and compared with the TFinger results. It should be noted that the main characteristics of the stability and security of the sensitivity systems are the values of the rejection error (RE) and permission error (PE).

The comparison showed that the RE value of the TFinger system was about 2.5 times more than the value of the comparable RE systems, which in no way affects the security of the system, but causes slight inconvenience to the user, and the value of PE, in the result of experiments, has been approximately 10 times smaller than that of the comparable systems, which directly increases the system security.

2. CONCLUSION

The TFinger system work is divided into two stages, the working hours of which are different. The first is the user registration phase, which is slower, and the second - the key information creation phase - faster. Since the registration phase is made for each user only once, it is permissible that the duration of the work at that stage is great 10…15 seconds. And the duration of the second phase is considerably smaller and range between 0.01…0.09 seconds. The results of comparison are given in Table.

Table *Comparison of the results of biometric systems*

	ATRx Secure PunchIn	BioDesk	TFinger
Rejection Error (RR) (ՄՍ)	0.1%	0.6%	1.5%
Permission Error (PE)	0.01%	0.01%	0.001%
Operating time	< 2 sec.	< 1 sec.	10 – 15 sec. < 1 sec.
Fingerprint image saving	Yes	Yes	No

Thus, the number of versions observed during the attack by brute force has been given.

- The number of possible variants of the segments' configuration to each other $n \approx 10^{27}$,
- $C_L L$ in the range [1, L_{max}], the number of possible variants of distribution ` $q \approx 10^{25}$,
- L the number of possible variants for receiving static data from the distances is $p \approx 3 \cdot 10^{11}$:

REFERENCES

[1] Տ. Անդրեասյան "Կենսաչափողական տվյալների վրա հիմնված բանալիային տեղեկատվության ստեղծման համակարգ", *Доклады международной научно-практической конференции по вопросам безопасности информационных систем*, pp. 37-42, 2011.

[2] Տ. Անդրեասյան "Բանալիային տեղեկատվության գեներացում մատնահետքի հիման վրա՝ առանց էտալոնի պահպանման", *ՀՊՃՀ Լրաբեր, գիտակա ևև մեթոդական հոդվածների ժողովածու - Երևան, Հայաստան*, pp. 253-256, 2010.

[3] V. Markarov, T. Andreasyan "An Approach to Key and Password Generation Based on Specific User Data", *Applications of Information theory, Coding and Security, Workshop (WAITS2010)*, pp. 47-50, 2010.

[4] H. Jacobs "Geometry: Seeing, Doing, Understanding - W H Freeman & Co", 2004.

[5] И. Ерош "Дискретная математика. Комбинаторика", 2001.