

# IMPROVING EFFICIENCY OF ACCESS TO INFORMATION WITH THE USE OF IDENTIFICATION LOGIC-TIME FUNCTION

Natalia V. SACHANIUK-KAVETS'KA, Olena P. PROZOR, Maya B. KOVALCHUK

<sup>1</sup>Vinnitsia National Technical University, 95, Khmelnytsky Hwy, 21021, Vinnitsia, Ukraine

**Abstract.** The possibility of increasing the effectiveness of access protection to information with the use of a special identification logic-time function is considered. Using of such a function for passive and biometric identification of subjects is suggested. The rules of constructing the keys of an asymmetric cryptographic algorithm are formulated on the basis of the identification logic-time function.

**Keywords:** identification logic-time function,  $\Delta$ -sampling, polynomial, key, password.

## 1. INTRODUCTION

The rapid development of information technology has led to an increase in the relative importance of certain aspects of public life, in particular any information. Information has some value (it may be sold), it is not localized in space and can easily be distributed. Information exists in various forms: it can be stored on computers, transmitted by computer networks, printed or recorded on paper, as well as sounded in conversations. The use of computer systems and networks for solving various business tasks, strategic development, implementation of various communications between enterprises and their partners, clients, and managing institutions in the on-line regime made it possible not to limit information flows and information processes to the boundaries of an individual enterprise. Information and information systems, networks in which enterprises, organizations, institutions operate, are their extremely important resources [1]. On the one hand, the availability, integrity and confidentiality of information can be of particular importance for the competitiveness and reputation of the organization, its profitability, compliance of management decisions with the legal norms of Ukrainian legislation and international legal requirements. On the other hand, the increased dependence of organizations on information, communication systems and services makes them more vulnerable to violations of the security regime.

Taking into consideration the questions of security, all kinds of information need reliable protection. However, access control is an effective method of comprehensive protection of information that regulates the use of information system resources and includes such an important element as user identification. Recently, more and more attention is being drawn to biometrics, as one of the newest information technologies, which uses the unique characteristics of identification and verification objects. Therefore, the issue of protection of access to information resources is relevant.

## 2. OVERVIEW OF PROBLEMS AND PROBLEM STATEMENT OF CREATING INFORMATION SECURITIES IN ACCESS CONTROL SYSTEMS, USING THE UNIQUE CHARACTERISTICS OF OBJECTS

With the advent and development of information technologies, the problem of information security, related to the preservation of the information confidentiality that is processed and stored in computer systems, became urgent [2]. Managing and delimiting of access to information resources is one of the important aspects of information security. Methods and systems of information security based on access control perform such functions as: user authentication; identification and authentication of the user according to the account data; admission to certain conditions of work in accordance with the regulations.

There are three most common types of subject identification [3].

1) Password identification. The main advantage of the password identification is the simplicity of implementation with the use of a password-login twain. The main disadvantage of such identification is the dependence of its reliability on users, i.e. on their chosen passwords (so-called human factor).

2) Hardware identification, using keys, tokens or cards, which are in the exclusive use of identification subjects. The main advantage of such identification is its rather high reliability. However, the high cost of such devices, the likelihood of their theft in registered users, as well as the possibility of duplication reduces the curiosity to hardware identification.

3) Biometric identification [4], using the unique properties and features of a person, which are of two classes:  
 - static, which are based on the physiological unique characteristics of objects (fingerprint, face thermogram, palm, retinal, DNA, location of veins on the front side of the palm, etc.) that are practically unchanged with the lapse of time;  
 - dynamic, which are based on the behavioural characteristics of subjects, that is built on features characteristic of subconscious movements in the process of reproduction of any action (by handwriting, by keyboard, by voice, etc.). The main advantage of biometric technologies is the highest reliability, and the main disadvantage is the cost of the equipment.

In the context of modern information technologies of information security, biometrics is an applied branch of knowledge that uses unique human features to create automated access systems.

All of these approaches to protecting access to information are fairly easy to implement in the logical-time environment, turning all the necessary parameters into logic-time functions (LTF) [5], which are of three functionally complete classes, closed with respect to Boolean operations, a special operation of unequal subtraction and differentiation. For example, an elementary LTF of the first class, this takes a constant value between two zeros:

$$f(t, t_1, T_1) = \begin{cases} t - t_1, & \text{if } t_1 < t \leq t_1 + T_1 \\ 0, & \text{if } t_1 + T_1 < t \leq t_1 \end{cases}, \quad (1)$$

where  $t$  – the current value of the time parameter,  $t_1$  – the time coordinate,  $T_1$  – the length of the interval of existence.

LTFs are considered on a time interval  $[t_k, t_{k+1}]$  sampled by means of  $\Delta$ -interval ( $\Delta$ -sampling) of time (minimum time interval, length  $\Delta_i$ ,  $\Delta_i = t_{i+1} - (t_i + T_i)$ ) between two time coordinates of the LTF. The operation of the unequal subtraction ( $|k|$ ), which is based on  $\Delta$ -sampling, is defined as follows:

$$f_1(t, t_{11}, T_{11}, a_1) |k| f_2(t, t_{21}, T_{21}, a_2) = \left\{ (t - (t_1 + i\Delta_i)) \cdot |a_{i1} - a_{i2}|, t_1 = \min(t_{11}, t_{21}) \right\}, \quad (2)$$

where  $t_{11}, t_{21}$  – time coordinates of variables,

$T_{11}$  and  $T_{21}$  – the duration of the existence segments of the first and second functions,

$a_1$  and  $a_2$  – the corresponding amplitudes,

$i$  – number of  $\Delta$ -intervals in the selected interval of time,

$\Delta_i$  – duration of  $\Delta$ -interval

$a_{i1}, a_{i2}$  – the corresponding amplitudes on  $i$ -th  $\Delta$ -interval.

The result of this operation will be the LTF, which can be called unequal difference. In the future, for simplicity of presentation of the material, LTF will be marked  $f_i(t)$ .

The purpose of this article is to develop possible options for improving the effectiveness of protecting access to information using the identification logic-time function.

### 3. BASIC CONCEPT

The main advantage of the password protection system is its simplicity and habitualness. Passwords have long been embedded in systems and services. With the correct use passwords can provide acceptable level of security of access to information resources for many enterprises. However, the reliability of such passwords can be greatly enhanced if you use not a customary set of letters and characters, but some of the image that is converted into an ID into logic-time function [6]. In work [5] software was developed (**LTF Model**), which allows to select edges of arbitrary images using the traditional mathematical operation of differentiation in the form of a special logic-temporal function. The general view of the dialog box of this program is shown in Fig. 1.

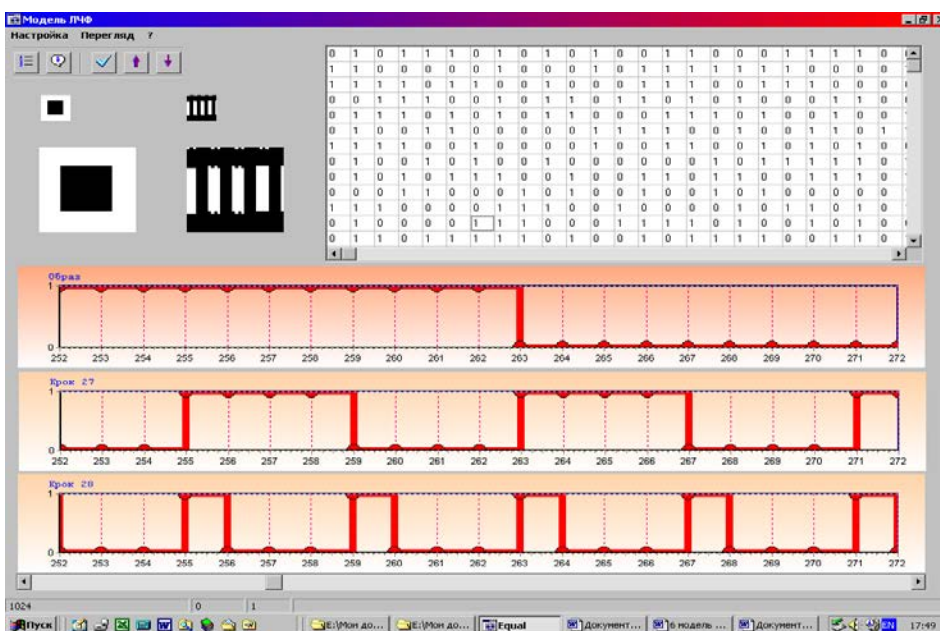



Fig. 1 – General view of the **Model LTF** program window

The window has a title bar with the name of the program, the menu bar and the toolbar row.

The menu bar contains two items: **Setup**, **View**, which are used to control the program. The toolbar contains the most frequently used buttons. First of all:

- **Mark**  – displays the values of the graph (Fig. 2);

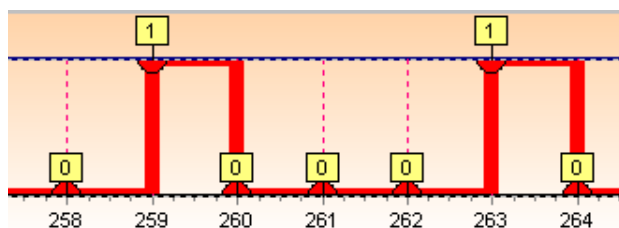





Fig. 2 – Schedule with labels

- **Number of iteration**  – allows you to go to the necessary step iteration;

- **Up**  – transition to the previous iteration step;
- **Down**  – move to the next iteration step;

We also have three right-click context menus: image menu, table menu and graphics. The last menu copies the desired graph to the clipboard for later use in other applications.

The context menu of the image allows you to insert an image from a \*.bmp file with a colour number of no more than 256 and a size of 32x32 pixels. The image file must be located in the same directory as the program itself. The file must be pre-prepared by **Paint**.

Let us have some LTF of  $k$ -fold logic  $f(t, t_1, \dots, t_m, T_1, \dots, T_m, a_1, \dots, a_m)$ ,

where  $t_1, \dots, t_m$  - time coordinates,

$T_1, \dots, T_m$  – the corresponding segments of existence,

$a_1, \dots, a_m$  – amplitudes that correspond to these segments of existence.

Then the derivative of the specified function is defined as follows:

$$f'(t, t_1, \dots, t_m, T_1, \dots, T_m, a_1, \dots, a_m) = \begin{cases} (t - (t_k + i\Delta_i)) |a_{k,i+1} - a_{k,i}|, & \text{where } i - \text{sequence number} \\ \Delta - \text{sampling}, & i = 0, \frac{T_k}{\Delta_i} + 1, k = \overline{1, m} \\ 0, & \text{if } (t \leq t_1) \wedge (t_k + T_k + \Delta_i < t \leq t_{k+1}) \wedge \\ & \wedge (t > t_m + T_m + \Delta_i), k = \overline{1, m} \end{cases} \quad (3)$$

Note that in the case of binary logic, formula (3) is somewhat simplified, since the amplitudes can take a zero or a single value.

The derivative of an arbitrary LTF can be represented graphically (Fig. 3).

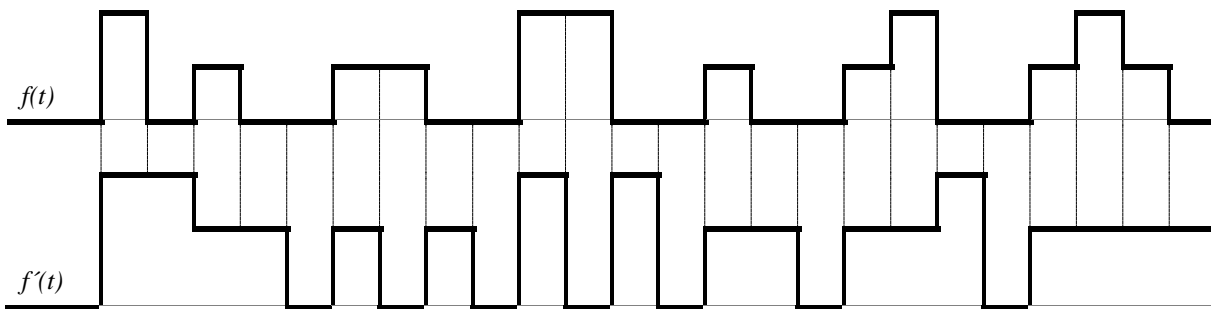


Fig. 3 – An option for graphical finding of the derivative of a random LTF of three-valued logic

If necessary, you can enhance the selected image edge by re-differentiating the identification function. As a user password, you can use any image known to him only. Moreover, this image can be black-and-white (binary LTF of the first and second classes), and colour (LTF of  $k$ -valued logic of the first-third class). Such a password in the form of a logic-time function can be used for a long time, since it is almost impossible to reproduce the image by the function-contour. What is more, there is a possibility of mathematical study of the speed of changing such a password.

User account is a set of identifier and its password. As an identifier, you can use a special identification logic-time function, which is unequal to the difference in the LTF of the biometric characteristics of the subject, ranked in importance. This feature is unique to this user and can include both static and dynamic features and properties, and virtually prevents its use by malicious users. The subject is identified by comparing the obtained identification with the reference samples of the

knowledge base. In the case of incomplete identification, the expansion of the knowledge base is carried out by recording the result of comparison in memory as a new sample and determining the closest to the reference sample obtained.

Since biometric systems can operate in two modes: verification, the task of which is to verify the correspondence of the measured biometric characteristic with the recorded template of the declared individual; and the identification at which the biometric characteristic is measured, which will be compared with the database of previously recorded templates of all "known" objects, this considerably extends the possibilities of using an identification LTF.

It should be noted that in some cases the password system can perform a number of additional functions, in particular the generation and distribution of short-term (session) cryptographic keys. An important aspect of the stability of the password system is the way of storing passwords in the accounts database: in the open form; in the form of a compression (hashing); encrypted by some key. Of greatest interest are the second and third ways. For greater reliability of password retention, it is suggested not to store the identification LTF itself, but the corresponding polynomial [7], that is, the encryption of passwords. For example, a second-class LTF containing two segments of existence that does not intersect each other (Fig. 4) corresponds to a polynomial:  $P_6(t) = t^2 + t^3 + t^6$ , but a monotonically growing LTF, depicted in Fig. 5, corresponds to the polynomial:  $P_2(t) = t + 2t^2$ .

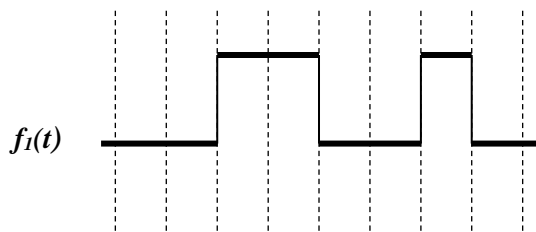


Fig. 4 – Possible variant of LTF with two segments of existence

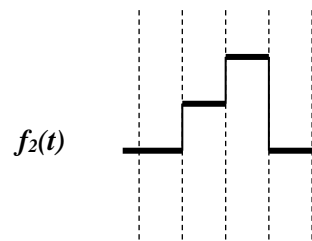


Fig. 5 – Possible variant of growing LTF

When encrypting passwords, special importance is given to how to generate and store an encryption key and decrypt the database of accounts. Asymmetric cryptosystems in which encryption and decryption are performed using various keys are considered the most promising data protection systems today. Such systems require much more time to calculate, but they do not create difficulties when distributing keys. It can be stated that precisely asymmetric algorithms are used to encrypt information. To better conceal information and protect it from modification, forgery or distortion, you can use asymmetric algorithms that allow you to encrypt user data in different modes.

1. Using the secret key of the sender. Then, anyone who has the public key can decrypt the transmitted message.
2. Encrypting using the public key of the recipient, then only the owner of the secret key that is paired to the open one can decrypt such a message and gain access to the information.
3. Using the secret key of the sender and the public key of the recipient of the transmitted message. Then only the right user can access the necessary information resources.

Since there are no two people with the same biometric characteristics, it is advisable to use them for the construction of the cryptosystem. Moreover, it is possible to use several characteristics, ranked according to importance, in the identification LTF. The comparative characteristics of the most commonly used biometric systems are given in Table 1.

From a security point of view, a false admission error is more significant than a false failure, which affects only the user's ease of system use. It should be detailed that the hand geometry includes: palm parameters, vein pattern, palm shape. And the face geometry includes 2D and 3D models and thermo grams.

Since the derivative of the LTF is used for the derivation of signs, which highlights the image edges, then when constructing a LTF key, taking into account the likelihood of unauthorized admission, it is advisable to use the following 5 characteristics (from best to worst): iris, retina, fingerprint, placement of veins in the palm, 3D model of the face.

Table 1 – Comparative characteristics of biometric systems.

№	Model	Biometric method	Probability of false failure	Probability of false admission
1	Eyedentify ICAM	retina	0,0001	0,4
2	Iriscan	iris	0,0008	0,0007
3	FingerScan	fingerprint	0,0001	1,0
4	BioMet	hand geometry	0,1	0,1
5	Vocord (2D)	face geometry	0,01	0,2
6	Hitachi VeinID	vein pattern	0,0008	0,01

Moreover, the sender's key can contain its biometric characteristics, and the key for decoding the message and access to the information – the characteristics of the recipient.

When constructing keys of cryptographic algorithms using biometric characteristics, it is necessary to observe such rules.

1. For each biometric characterization of the subject of access, we construct the LTF  $f(t_1, \dots, t_m, T_1, \dots, T_m, a_1, \dots, a_m)$ , where  $t_1, \dots, t_m$  – time coordinates;

$T_1, \dots, T_m$  – the corresponding segments of existence;

$a_1, \dots, a_m$  – amplitudes that correspond to the given segments of existence;

using the differentiation [5, 6]. Note that the best characteristic is the amplitude  $a = 5$  (iris of the eye), and the worst –  $a = 1$ .

2. We obtain the LTF-key as the result of unequal subtraction of the functions obtained in the previous paragraph.

3. We write the LTF-key in the form of a polynomial, where the coefficient near the corresponding degree of the variable  $t$  equals the value of the corresponding amplitude  $a_i$ . Note that this key can be applied not only as a polynomial, but also as n amplitude matrix of dimension  $1 \times m$ .

An important characteristic that determines the choice of the required biometric system is its bandwidth. Under the bandwidth we understand such number of people requiring authentication, in which the work of the system with a given error rate of error access will be stable over a period of time. For example, let  $N$  persons pass through the biometric access system within an hour. If we consider 2 system errors within an hour as allowable, then the bandwidth can be calculated by the formula:

$$N \approx \sqrt{\frac{2}{FAR}} \quad (4)$$

where  $FAR$  – the error of the false admission, which occurs in the case when the subject was identified incorrectly, that is, he did not match the standard.

It should be noted that the passwords and keys based on the identification of the LTF can be transmitted over the network in an open form or without the direct transmission of password information ("zero-disclosure"), since they have high cryptographic stability.

The "zero-disclosure" authentication schemes provide an opportunity for one of the couple of subjects to prove the truth of a certain statement to another, without informing him any information about the content of the statement itself. For example, the first individual can convince other that he knows a certain access password to information resource, without

actually transmitting any information about the password itself. That excludes the possibility of stealing a password by a violator.

#### 4. SUMMARIES

Based on the analysis of threats to information security and existing methods for the identification and authentication of users of information systems, it can be stated that password protection today is one of the most common ways of protecting access to information, both in individual computers and networks, and in networks of world-wide scale. The reliability of passwords can be greatly improved if you use a certain image, converted to a logic-time function. As an identifier of the accessor to information resources you can use a special identification logic-time function, which is an unequal difference between the user's biometric LTFs, ranked by importance.

The uniqueness of keys with biometric characteristics based on identifying LTFs is the impossibility of recovering and reading messages by unauthorized users, quick response to attacks, and sufficiently short encryption and decryption time. Moreover, an intruder user cannot give himself up for the subscriber. Using such keys reduces the possibility of confidentiality violation to a minimum. Keys with biometric characteristics based on identifying LTFs can be used to confirm authorship and have easy procedure of exchange and simple mathematical research, since they are presented as polynomials. It can be stated that it is easy to manage such keys in a large network.

**Authors:** *Ph.D., Associate Professor, Associate Professor of Higher Mathematics Department Natalia Sachaniuk-Kavets'ka, Vinnytsia National Technical University, Khmelnytsky Hwy, 95, 21021 Vinnitsa, Ukraine, E-mail: [skn1901@gmail.com](mailto:skn1901@gmail.com), Ph.D., Associate Professor of Higher Mathematics Department Olena Prozor, Vinnytsia National Technical University, Khmelnytsky Hwy, 95, 21021 Vinnitsa, Ukraine, E-mail: [el.przr@gmail.com](mailto:el.przr@gmail.com), Ph.D., Associate Professor, Associate Professor of Higher Mathematics Department Maya Kovalchuk, Vinnytsia National Technical University, Khmelnytsky Hwy, 95, 21021 Vinnitsa, Ukraine, E-mail: [maya.kovalchuk@gmail.com](mailto:maya.kovalchuk@gmail.com).*

#### REFERENCES

- [1] Smyt S. Tsyfrovaya obrabotka signalov. Praktycheskoe rukovodstvo dlya inzhenerov i nauchnykh rabotnikov; per. s angl. A.YU. Lynovych, S.V. Vytyazev, Y.S. Husynskoho. Moskva: Dodéka XXI, 2012. 720 p.
- [2] Rusyn B.P., Varets'kyi YA.YU. Biometrychna autentyfikatsiya ta kryptohrafichnyy zakhyst. L'viv: Kolo, 2010. 287 p.
- [3] Akhramovych V. M. Identyfikatsiya y autentyfikatsiya, keruvannya dostupom // *Suchas. zakhyst informatsiyi*. 2016. №4. P. 47-51.
- [4] Hnidets' T. YA. Biometriya: syl'ni ta slabki storony // *Naukovyy visnyk L'vivskoho derzhavnoho universytetu vnutrishnikh sprav*. 2014. №2. P. 273–282.
- [5] Sachaniuk-Kavets'ka N.V., Kozhemiako V.P. Elementy oko-protsesornoyi obrobky zobrazhen' u lohiko-chasovomu seredovyshchi. Monohrafiya. Universum-Vinnytsya, 2004. 135 p.
- [6] Sachaniuk-Kavets'ka N.V. Vyznachennya chutlyvosti identyfikatsiyanoi funktsiyi do zminy vkhidnykh kharakterystyk obrobky zobrazhen' dlya rozpoznavannya sub'yektiv u systemakh zakhystu informatsiyi. // *Reyestratsiya, zberihannya i obrobka danykh*. 2017. T. 19. № 1.p. 55–64.
- [7] N. Sachaniuk-Kavets'ka, V. Kozhemiako, W. Wojcik, D. Kassymkhanova, A. Kalizhnova The use polynomials as a possible variant analytical processing on logic-time functions// *Optical Fibers and Their Applications 2015 Proceedings of SPIE*. Volume 9816. Lublin, Poland, 98161S-1 to 98161S-2.