Biometric Dynamic Personality Authentication in Open Information Space

Akhmetov B.S., Ivanov A.I., Kartbaev T.S., Malygin A.U., Mukapil K.
Kazakh National Technical University named after K.I.Satpayev
E-mail kartbaev_t@mail.ru, kartbaev_t@kaznu.kz

Abstract
The protection methods of personal data in open information spaces with the using of biometric identity authentication technology. An analysis of biometric methods using static biometrics person. Celebrated their potential danger due to the threat of loss of base biometric templates. For the protection of personal data is proposed to use dynamic biometric characteristics of the person, which are well suited for remote user authentication. These parameters are sensitive to the current psychophysical state of man, and at the same time can be changed by the will of man. Especially given the dynamic neural network biometric identity authentication on the example of the biometric characteristics such as signature, handwriting keyboard, voice.

1. Introduction
One of the most common methods of protecting personal information in an open information space is the electronic digital signature (EDS). It ensures authentication and integrity of electronic documents created electronically by the government, businesses and citizens. Of fundamental importance is the fact that the storage key digital signature algorithm are good exhaust problems [1-3].

The classical scheme of digital signature is shown in Figure 1.

![Figure 1. The classic pattern of use of digital signature](image)

However, a normal user cannot provide reliable storage of his/her own personal key to your computer or the safe and its use only in a trusted computing environment. All of it is dangerous to provoke an attack on a citizen. In this regard, the Government must provide the citizen with the means of safe storage of private keys and digital signature algorithm trusted computing environment for their application in the face of certification authorities that provide services to support public key certificates citizens. However, citizens do not want to officially register your public key to verify the signature of legally significant. The problem is that along with the registration of a public key citizen inevitably gets an extra risk of compromise of its private key digital signature algorithm. Anyone who has stolen the private key man is able to generate on its behalf EDS any electronic document [4].

2. Static biometric technology
One of the most appropriate ways to solve this problem is to link the code to the user's biometrics. Biometrics as a scientific and technical direction is being actively developed [5-10]. Its main task was to create devices and programs that could very likely recognize his master, and with even higher probability to recognize intruders trying to masquerade as legitimate users.

The basic idea of such tools is to use static person's biometric data, which are given to man by birth and cannot be changed by them [11-15]. These include the identification of: a drawing iris pattern leather fingertips (on the pattern of papillary lines), the parameters of two-and three-dimensional geometry of the hand, two-and three-dimensional geometry of the human face, drawing blood vessels: the fundus of the eyeball, the back side of the hand, the geometry of the ears, the electrocardiogram of the heart, body odor, DNA analysis, ion spectrum traces of sweat. On the basis of these data formed the biometric template, which is signed by electronic signature and shall be published (stored) in the system of biometric identification certifying centers [4].

This gives rise to the so-called threat of a "mark of an animal" [5]. Biometric template pattern of your fingerprint or your iris will get not only a map of your biometric data, but also to the corresponding centralized database. This may be a corporate biometric database, where it can accumulate approximately 1000 times more sensitive biometric information of the people working in the corporation and actively interacting with the corporation from the side. The
largest volume of sensitive biometric information can be stored in the state of biometric databases. Shoot people of their biometrics and place it in a large database is extremely dangerous.

To eliminate the threat of compromised biometric templates to create new biometric technology, which on one hand can reliably (Highly reliable) to authenticate a person by his biometrics, and on the other hand make biometrics a person is not available for observation and understanding. One of the ways to reach the goal of partial confidentiality and anonymity of biometric data is to use neural networks large and extra-large size [16-18].

Figure 2 shows a block diagram of a classic means of organizing a highly reliable biometric authentication.

Figure 2. Typical block diagram of the organization means a highly reliable biometric authentication

A positive aspect of neural network solutions is that disappeared biometric template has been stored previously in explicit form. Instead, it appears neural transmitter biometric code (blocks 3 and 4). In fact, this table is a neural network connection of neurons and synaptic connections table (weights) trained to recognize "Insider" neural network. Mystery of biometrics is provided by the fact that the tables relations trained neural network, and the tables of weights to calculate the donor biometrics (find a person based on biometric images) is technically very difficult. Privacy biometrics, placed in the container, the neural network is provided at a level comparable to the confidentiality provided by encryption.

3. Dynamic biometric technology

A man cannot force his will to edit a picture of your finger print or geometric parameters parts of his body. Once human fingerprint patterns compromised they cannot be used to effectively protect the biometric information. In this respect, the static biometrics will always remain weak.

3.1. Identification of the person on the specifics of the dynamics of handwriting

One of the most difficult (informative) is a biometric image of the person obtained by the analysis of the dynamics of the handwritten word-play password. Obviously, the compromise of the dynamics play written word, password-man is not a catastrophe for its information security. If the biometric image is compromised, it must be replaced immediately to the other, the image is not compromised, the other written word-password. In contrast, only 10 different patterns of fingerprints handwritten passwords, reproduced handwriting even one person can be many.

The reason for the unique dynamics of the handwriting of each of us is the huge complexity of the human hand. Five fingers on the hand are at the joint 3, each of the joints is a ball-joint, i.e. the first crude approximation fingers are $5 \times 3 \times 3 = 45$ degrees of freedom. For our three-dimensional space is a huge redundancy in 42 additional control variables. When the number of degrees of freedom equal to the dimension of the problem, neither of which redundancy can be no question. In this case, the individual handwriting cannot be, every handwriting is determined by the geometry of the actuator and the optimality conditions of its application.

If the number of degrees of freedom of the actuator (hand) is much higher than the dimension of the problem, then be sure there is a personality of handwriting solution. Each of us once had to seek out their own solution of the problem of the dynamic play of handwritten letters by his own hand. Possible dynamic solutions to reproduce the same letter there is a huge amount of very high order mechanism play - hands. Each of us while learning the letter had to find and memorize its decision, which further shapes our individual style.

Remembering found solutions of dynamic problems on a subconscious level, on their daily decision making is very accurate and very fast. If a person plays a handwritten signature or password, without hesitation, that this action is wasted little time. This situation is illustrated in Figure 3, where the given dynamics play an autograph "Insider" and the dynamics of the bypass autograph "Strangers".

While the instrument is sharply reduced in the moments of human use of his eyes and a high level of intelligence. The processing of visual images - this is a very time-consuming operation. We are able to move faster than seeing. This built on a lot of tricks, but move faster than to see possible only if included only subconscious. Magicians are forced to work for years juggling cards and moving them into the sleeve.
Not only our eyes are the cause of slowing our actions. Another reason is the interference with the waste to the level of the subconscious program slows a higher level of intelligence. If all of a sudden "centipede" reflects, to which foot to start walking, then there is quite palpable silence. This situation is well monitored and displayed in Figure 4.

With regard to the dynamics of reproduction of the signature we stop seeing the pen for the duration of the slower of the universal consciousness. When the unconscious (subconscious) play written word-user password "Insider" is fast and stable, it is this mode and use all means authenticate the identity of the dynamics of handwriting. There are a number of approaches [1, 2, 19, 20] to the construction of the calculation procedures controlled by biometric handwriting and a decision on it. One approach to solve the problem can be built on the calculation of the Fourier coefficients and the iterative learning of a single neuron with a large number of inputs. Obviously, instead of expansion dynamics oscillation pen Fourier series may be used any more for different expansion of the orthogonal basis functions (Walsh Haar wavelet decomposition [21, 22]). Decision rules can be different - from classical decision by maximum likelihood Bayes [23] to neural network solutions with single and multiple neurons [20].

The most important fundamental difference between all of biometric authentication manuscript handwriting is the only one - whether the secret biometric handwriting image is used. If the conditions for the secrecy of biometric handwritten word-password are provided, then the remedy of biometric authentication can be classified as highly reliable. If this condition is not fulfilled, then we can speak only of the residual resistance of the compromised biometric image. Residual resistance compromised biometric image can not be high, after some training attacker will always be able to overcome the protection of biometric open manner. If handwritten biometric image is known to all (as protection is used autograph person), then the user "Insider" will be different from the attacker's "Stranger" only by the number of attempts undertaken by them in the public domain. Usually by "Insider" permitted the use from 2 to 5 access attempts in the same session of biometric authentication. Prepared for the implementation of the attack an attacker to access the system should be from 20 to 50 attempts. Identify the series of repeated failures and broken authentication sessions can be achieved only with the use of special tools to collect and analyse biometric audit [20].

Author names and affiliations are to be centered beneath the title and printed in Times 12-point, non-boldface type. Multiple authors may be shown in a two- or three-column format, with their affiliations italicized and centered below their respective names. Include e-mail addresses if possible. Author information should be followed by two 12-point blank lines.

3.2. The dynamics of keyboard handwriting

One of the complicated tasks, routinely solved by many people, is a fast text input from the computer keyboard. Usually a quick keyboard input can be achieved through the use of all fingers of both hands, with each person has their own unique handwriting keyboard. It should be emphasized that the unique personal handwriting is produced in the solution of a similar problem in Morse code transmission, which was used previously for the identification telegraph in his handwriting.

Traditionally, the restriction of access to information is for passwords. However, if the password is to increase and make it easy to remember [24], it becomes possible to observe the correct password for the user typing characteristic handwriting. For example, the password, use the following phrase: "Password - this is a way to protect the information." When you enter a passphrase, such biometric system records the time you press each key, and the time interval between pressing the button once and releasing the previous key. Graph of the relationship of time intervals and release, for the word "Password" is shown in Figure 5.
regard, meaningful passphrases can be long enough characters as opposed to meaningful phrases. In this remembers the bad meaningless combinations of meaning of a meaningful text. [24] The common man passphrase appropriate use of the word with the contain from 21 to 42 keystrokes. In the synthesis of a passphrase should be memorable and length of biometric identification passphrase. Practice shows that the passphrase should be memorable and

Figure 5. Timing diagram of typing the word "Пароль"

Note that during testing keyboard dialed handwriting passphrase must have a sufficient length and at the same time, they must be well remembered people. To achieve a good memory long enough passphrase must use meaningful lyrics. In the case where the text of the passphrase is obtained by extracting a random word from a dictionary, allowed the introduction of the phrase prepositions, changing endings of words, their mortality and declines in accordance with the rules of the language user.

From the above figure, the keystrokes are times t1, t2, t3, ..., tn different and, respectively, the values of these parameters can be used to identify the characteristics of the individual user's handwriting keyboard. Furthermore, can be used as controlled variables, the intervals between adjacent touch keys τ1, τ2, τ3, ..., τN-1. Controlled parameters tc and tk essentially depend on how many fingers are used in the user specific combinations of the various movements of the fingers and the characteristic movements of the hands when typing. In particular, if the force users to work with one finger of one hand, the keyboard writing style is almost completely loses its identity. In this case, the time of keystrokes to different people no longer reflect their individuality. The intervals between keystrokes are proportional to the distance between the keys, and the overlap of adjacent keys presses becomes impossible (parameter tk is always greater than zero). On the other hand, with increasing skills with the keyboard and with the transition to a blind set of all fingers of both hands, significantly increasing individuality keyboard handwriting of any of the users.

A very important feature of this technology is the length of biometric identification passphrase. Practice shows that the passphrase should be memorable and contain from 21 to 42 keystrokes. In the synthesis of a passphrase appropriate use of the word with the meaning of a meaningful text. [24] The common man remembers the bad meaningless combinations of characters as opposed to meaningful phrases. In this regard, meaningful passphrases can be long enough resistance such password can always be measured in space Hamming codes. Unlike classic passwords, typing a long passphrase allowed errors in one or two characters, which is somewhat impairs resistance to static passphrase selection, but it greatly reduces the chance of errors of the first kind. Adjustment of the small number of errors in the password phrase is usually code detection and correction of errors or using neural network equalizer [25, 26]. Biometric standard passphrase receive calculating expectations and variances of monitored parameters. In the calculations it is extremely important exception to the training sample of abnormal emissions [27]. Good results are obtained by using fuzzy sets [28] to reduce the uncertainty of the original data. Perhaps the most challenging for the technology of biometric identification is the issue of the presence of the user is an individual handwriting keyboard. In [29] are special computational procedures to answer this question and to measure the degree of stability and identity of a particular person's handwriting keyboard.

3.3. Biometric authentication is the person on the speaker's voice

One of the fundamental differences between people from the higher animals is the presence of the people first, allowing transfer from one person to large amounts of information. Hear it and try to talk the person starts almost from his birth, but articulate (understandable to others) the child's speech is only after two or three years. That is, two or three years, each of us has gone out to learn how to manage our vocal cords, reproducing the sounds of speech intelligible to others. The vocal apparatus of each of us is very complex (complex of any of the artificial musical instruments), having mastered them one day, we keep for life their individual speech patterns.

Human speech consists of sounds, which in its formalization can be identified with letters and, accordingly, speaking person can be represented in the form of hand-written or printed text. Representation of human speech in the form of text leads to a complete loss of speech biometrics. After recording a speech to the paper it is impossible to recover the speaker's voice characteristics. To formalize the Russian language uses the Cyrillic alphabet. The letters of the Cyrillic alphabet, as well as the sounds of speech are divided into three groups: a sizzling, tone deaf, ringing tones. Figure 6 displayed a sound wave pressure oscillations air, forming a word consisting of four coordinated (tone) sounds and a hissing sound.
Figure 6. Example of dividing the word on the tones numbered 1, 2, 4, 5, consisting of periodic oscillations of the sound pressure and the occasional hissing sound number 3

All tones to have a strong periodic (tonal) component and each period of their oscillations similar to the neighboring periods, hissing sounds, on the contrary, random and have no repeating units. For periodic (tone) sounds can be calculated their period. During the speech pitch period of the sound changes from one tone to another sound. As a result, the passphrase can build the variation of the pitch period. An example of the curve of variation of pitch passphrase is shown in Figure 7. For each individual curve of variation of the pitch period is unique and can be used for biometric authentication identity.

Figure 7. Graph of variation of the pitch period in the password phrase announcer voice-1

Figure 8 shows the curves of variation of the pitch period of two speakers, uttering the same phrase. It can be seen that the curves of the variation of the pitch to the same speaker similar. For two different speakers pitch variation curves differ in shape, moreover, they differ even by a constant component (in the average value of the pitch period).

The average value of the pitch period of human speech is related to the geometry of his voice pipes (larynx). Typically children and women pitch period is approximately two times shorter than men. Variations in the distribution of the average period of the fundamental tone, typical of men and women are displayed in Figure 9.

The speech coding is often used frequency approach. This is due to the fact that the speech sounds have different frequency content. You can classify the sounds of speech of one person over the frequency spectrum, which accounts for most of the energy sound. Figure 10 shows the representation of sounds corresponding to the various letters of the alphabet in the time and frequency domains.

Figure 8. Charts curves of variation of the pitch period like for one person and are substantially different for different people, even for the same phrase

Figure 9. A graph of the variations in the value of the pitch period for the same phrase uttered by male and female voices

The figure shows that the widest range of frequencies has a tonal sound “a”, a much more narrow range of tones to be owned by others. To estimate the width of the spectrum of tonal sounds, you can use the modules summing the amplitudes increasing frequency. Typically, the upper value calculation sound frequency effected on the basis of 80% of the sound energy
threshold. Figure 10 shows that for a sound "and" 80% of the energy is in the frequency range from 0 to 90 counts of frequency. The main energy spectrum of sound "o" is in the range from 0 to 60 counts of frequency. For audio, the "e" bulk of the energy is concentrated in the range from 0 to 30 counts frequency.

Figure 10. Display the letter-sounds ("a", "e", "o"), spoken by one person in the time and frequency domain.

Evaluate the width of the frequency spectrum of the sound cannot display it in the frequency domain. It's enough to count the number of vibrations of sound pressure per one pitch period. It can be seen that the sound of "a" is about 4 variations of sound pressure per one pitch period. The greater the number of vibrations, falling on the pitch period, the wider spectral band sound. There is an inverse relationship between the number of vibrations of sound pressure falling on the pitch period and the width of the frequency spectrum of the sound.

It should be emphasized that the frequency ordering (classification) sounds only works well when it is applied to the speech of one person. For voice, one person is characterized by a much higher order of sounds in comparison with the variety of sounds of different people. Each of us, there are several varieties of pronunciation of a sound that is quite simple ordered. If you try to compare the different sounds of the same person, they are substantially different. You can see this on maps sounds Figure 11, which displays options "a" sound in a few words spoken by one person and different people.

Figure 11. The similarity of sounds "a", spoken by one person (left side of the poster) in comparison with the same sound "a" spoken by different people.

The figure shows that the sounds of "a" different words spoken by one person alike. The same sound of "a", uttered by different people, is quite different in form sound waves. It is this fact that underlies the voice biometrics. The sound wave, which is formed by one person in one and the same word has almost the same shape, and the shape of the waves in the pronunciation of the same sound of one word different people are different.

Modern coding theory sounds treats periodic oscillations as a sound wave vibration response of a human vocal tract system for periodic impacts, the next with the same period T0, with different amplitude effects. This situation is displayed in Figure 12.
If the volume of the audio tone increases, the amplitude of the periodic impulse excitation effects should increase. The opposite is true, with a continuous decrease in the amplitude of the audio tone is a smooth decrease in the amplitude of excitation pulses. The above model is convenient because it separates the model of the sounds on a linear oscillating unit and some kind of generator excitation pulses, following a pitch period. One embodiment of the receiving system is a system of oscillating links of band pass filters 16, a block diagram is shown in Figure 13.

![Figure 13. Block diagram of preprocessing band pass vocoder sound](image)

Virtually all vocoders band pass power measurement performed on the outputs of comb band-pass filters 16, and periodically transmits these data to the digital communication channel. At the receiving end of the band vocoder restores audio data received on its intensity in different spectral frequencies. If the user utters some passphrase consisting of 6 consecutive sounds (the word "garden" in the figure), we obtain for each of the 16 parameters of frequency sound intensity. Total will have a vector of 96 biometric parameters corresponding to the average intensity of each sound in 16 channels to 6 letters (sounds).

The practice of voice identification of people showed that the spectral composition of the passphrase depends strongly on the passphrase itself, and the individual characteristics of the speaker's voice. If you try to build for each of the 16 channels analysed the distribution of the parameters "Stranger", we will get close to a normal distribution. The distribution of the values of the i-th biometric is also close to normal. The typical ratio of distributions "Insider" and "Strangers" for the i-th bioparametra shown in Figure 14.

![Figure 14. Typical ratio distributions "Insider" and "Strangers"](image)

It can be seen that for biometrics "Insider" standard deviation is approximately one and a half - two times less than the standard deviation of all the images of "Strangers." If we use a few examples of the image of "Insider", we can reliably find the values for each monitored biometric. This allows us to build on each of the monitored parameters primitive sampler is described by the following terms of conversion:

\[
\begin{align*}
\text{y}(\xi_i) &= 0 \quad \text{if} \quad \xi_i < \min(v_i); \\
\text{y}(\xi_i) &= 1 \quad \text{if} \quad \min(v_i) \leq \xi_i \leq \max(v_i); \\
\text{y}(\xi_i) &= 0 \quad \text{if} \quad \xi_i > \max(v_i). \\
\end{align*}
\]

With regard to the situation displayed in Figure 14, i-th digit of the 96 bit output code will give the state "1" for images of "Insider." For all biometric images "Strangers" in the i-digit output code with a probability of 0.7 would appear the state "1" and with a probability of 0.3 would appear the state "0". That is, the probability of error of the second kind (false recognition of the "Stranger" as 'his') for the i-th digit is 0.7. Analysing only one biometric parameter cannot identify with high confidence the image of "Insider". However, if we analyze the 96 monitored biometric parameters, we, with a probability close to unity, we can recognize the image of "Insider" and with a sufficiently high probability of detecting an image of "Stranger" by the code having at least one discharge status of '0'.

It should be noted that all the machines operating by the above procedure should have a biometric template as the conditions (1), comprising write explicitly the nonlinear transformation. With this pattern, we can always restore stored in the machine biometric image. The only escape from the compromised biometric image of "Insider" is the physical protection of the biometric template. A block diagram of the organization of the elementary converters biometrics code is not able to ensure the confidentiality of biometric image of "Insider" is shown in Figure 15.

If a means of biometric identification (authentication) holds the hardware and biometric templates are pre-loaded into it, then it is safe. If this means of biometric identification (authentication) is satisfied, either programmatically or by its working conditions need to load new biometric patterns, such a facility cannot be considered reliable because they do not provide privacy protection of biometric templates.

Analysing the program, you can always find a biometric template to distort it in the correct way, or make a fake biometric image of "Insider" in the well-known biometric template. Protect the biometric template cannot be encrypted because the cipher text with the biometric template cannot work. Before each use of the biometric template, you have to decipher.

Band pass vocoder sounds work from the late 50s of the last century and have been implemented by means of analogue equipment. The transition to digital technology has allowed creating digital oscillatory units in the form of a recursive digital filter, the structure of which is shown in Figure 16.

Typically, such filters have from 10 to 12 weight coefficients ai, which are calculated by linear predictors audio coding [30]. In systems of biometric identity authentication by voice linear prediction coefficients ai (coefficients of linear digital filters with the vibrational impulse response function) is usually regarded as the voice biometrics pipe member which does not depend on the amplitude of the reproduced sound tone. That is, as the basis for pre-processing voice biometric systems may be used not only quite primitive baseband vocoder, but also any other more sophisticated speech processing procedures used by modern vocoders.

The modern theory of biometric identity authentication by voice tones to consider speech as the main carriers of information about a person's personality. It is believed that the noise-like sounds [31, 32] are not substantially individual and it cannot reliably identify (authenticate) the identity of the person.

Examples of sound waves hissing sounds are shown in Figure 17. From this it can be seen that each of the sibilance has burst of energy in some part of the high-frequency spectrum. It is these injection energy of sound waves and reproduce existing audio vocoders.

It is quite obvious is the fact that the existing vocoders have the ability to change the density of the human voice compression due to changes in the number of transmitted through communication channels parameters. When using a large number of parameters passed to a person's speech is digitized streams from 64 kilobits / sec (for the simplest of vocoders) to 4.8 Kbit / s (for the linear prediction vocoders), and to provide high quality voice biometrics (speaker recognizable to those who hear.) If you reduce the number of transmission channels for the parameters, then it remains legible person (of course, what people say), but loses its biometric features. A so-called "robot voice effects."
The balance between legibility and recognizable announcer in modern vocoders skewed toward intelligibility. To control the speech, a special standard [33]. It turns out that each of the more than 100 existing vocoders distorts the voice biometrics speaker at their (speaker recognition or transfer of its biometrics is not standardized.) That is, each of biometric identity authentication by voice should be oriented only to a specific vocoder. Using a different vocoder in place of the result, the user is "Insider" is no longer recognizable.

4. Conclusion
The currently used classical biometric authentication technologies in open information systems based on the use of static biometric person potentially dangerous because of the threat of loss of the base of biometric templates. Once the biometric data of the person compromised they cannot be used to effectively protect information. In this respect, the static biometrics will always remain weak.

A potentially more powerful is dynamic biometric characteristics of the person, such as a signature, keyboard handwriting, voice. In its pure form, they have limited use because of their low resistance to attacks of selection; however, they are well suited remote user identification.

5. References
[26] The patent RU 2355307, the application number 2007118896/09 (020584) authors Ivanov A.I., Funtikova D.A. “The method of identity authentication on the image of the fingerprint and device for its implementation”, the priority of 21.05.2007, published on 20.05.2009, Bull. #14.
[33] GOST 50840-95 "Voice over paths of communication. Methods for assessing the quality, legibility and recognition.”