Voice Password Based Biometrical Cryptosystem

L.K. Babenko
Department of Security in Data Processing Technologies
Taganrog State University of Radioengineering
Taganrog, Russia
e-mail: blk@fib.tsure.ru

E.P. Tumoian
Department of Security in Data Processing Technologies
Taganrog State University of Radioengineering
Taganrog, Russia
e-mail: tumoyan@fib.tsure.ru

V.A. Gronin
Department of Security in Data Processing Technologies
Taganrog State University of Radioengineering
Taganrog, Russia
e-mail: blk@fib.tsure.ru

Abstract[1]

In this work we are researching some aspects of biometrical cryptosystem - cryptographic key generation based on human biometric features. We also offer a method of biometric key generation by voice password. According to the author's experiments, obtained estimations allow us to consider the proposed method to be secure enough for most practical applications.

1. Introduction

The problem of secure cryptographic key storage has not been solved yet. Indeed the size of cryptographic keys varies from 64 to 2048 bits, which is impossible for a user to remember. Many methods of secure storage and operative use have been offered, however none of them are satisfactory. We shall review them in detail. Key access management should be implemented with password authentication. Password protection is a reliable authentication mechanism and has many advantages such as simplicity, low authentication time, and absence of probabilistic authentication failures [1]. However these advantages are counterbalanced by user mistakes: users often use "weak" password such as words or letter sequences, which are used frequently by the others or are connected with user personal data. Therefore, in spite of the technical reliability and efficiency of password technique, password authentication cannot be considered absolutely secure.

The most effective solution for this problem is the use of human biological or behavioural features such as retina, fingerprints, voice, signature dynamics and other personal characteristics. Such methods were called biometric authentication. Its advantage is the use of parameters, which cannot be forgotten, lost or stolen. However this technology has its disadvantages. In major cases it demands significant computational resources and provides probabilistic solution [1]. The structure of a typical biometric system is shown on Figure 1. The system receives authenticated biometrics parameters, processes them and makes a "YES/NO" decision, which can be used by other security-related procedures such as network authentication, encryption, and digital signature. It is obvious that such system gives the intruder an opportunity to perform unauthorized activities including forging of stored biometric data, falsification of transmitted parameters, breaking of biometrics authentication procedures, decision falsification etc.

Due to the listed vulnerabilities of biometric authentication procedures, systems with increased security of biometric storage and increased security of biometric authentication procedures are used.

The development of biometric cryptographic systems, which use biometric-based procedures of generation, storage, and authentication, is one of the insufficiently investigated areas of secured biometrics. In prospective this approach could allow to store, distribute and use keys in unsafe environment. One of the possible methods of solving this problem is discussed in this paper. The approach is based on the use of artificial neural networks, trained to transform biometric parameters into keys irreversibly. Biometric parameters submitted by a legal user cause the neural network to recover his private key; contrariwise, submission of any other biometric

[1] *Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the CSIT copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Institute for Contemporary Education JMSUICE. To copy otherwise, or to republish, requires a fee and/or special permission from the JMSUICE.*

Proceedings of the 8th International Workshop on Computer Science and Information Technologies CSIT'2006
Karlsruhe, Germany, 2006

parameters leads to generation of a random bit set. We research theoretic aspects of this approach, share our ideas on the security of this approach, and give results of some experiments.

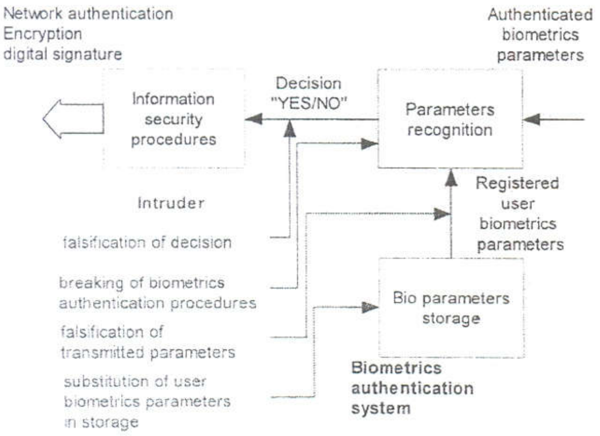

Network authentication
Encryption
digital signature
Authenticated biometrics parameters
Information security procedures
Decision "YES/NO"
Parameters recognition
Registered user biometrics parameters
Intruder
falsification of decision
breaking of biometrics authentication procedures
falsification of transmitted parameters
substitution of user biometrics parameters in storage
Bio parameters storage
Biometrics authentication system

Figure 1. Common Vulnerabilities of Biometrics Authentication Systems

2. Related Works

Now biometric cryptography is one of the newest areas in information security. First works in this area were published in 1998. One of them is the publication by C. Soutar, D. Roberge et al. [2]. The authors have offered an algorithm of cryptographic key generation based on fingerprints based on a digital filter and error-correction codes application. However, authors could not prove the safety of the developed method and have not given experimental estimations of false reject and false accept errors.

In 1998 and 1999 G. I. Davida et al. [3,4] offered an algorithm of cryptographic key generation based on retina binary representation (IrisCode). Authors claim, that the representation of IrisCode contains over 90 % conterminous bits for one user and less than 60 % for various users that allows to authenticate users with low FAR and FRR. Some retina scans are used in the method. Error-correction codes (adjusting up to 10 % of biometric parameter variability) are applied to the scans. The method has shown high speed and proved security, however independent researches have shown, that IrisCode can vary for as much as 30 % for various representations of a single retina which influences ERR negatively.

In 1999 F. Monrose et al. [5] offered an algorithm for keyboard password reinforcement by adding typing dynamics characteristics and creating so-called "hardened password". Error-correction codes and the table of instructions for key restoration are also used. This scheme is rather fast, however at standard password lengths (6 - 15 symbols) it adds biometric components up to 15 bits long, that increases password privacy only slightly. In 2001 F. Monrose offered update of this scheme for cryptographic key generation based on voice password. The modified method allows to generate biometric keys up to 60 bits long. The suggested method was implemented for Compaq IPAQ handheld computer. Now this scheme is considered the most practical one, since it has been confirmed by experimental results. Other researchers, for example P. Tuyls et al. [6], A. Juels and M. Wattenberg [7], T.C. Clancy et al. also use methods of key generation with error correction.

The use of artificial neural networks for cryptographic key generation allows to get some advantages, which are inaccessible in filtration and error-correction methods. The main advantages of this approach are: the applicability of a single method to various biometric data (certainly with specific signal processing algorithms), high complexity of the analysis (rules of transformation of biometric parameters into keys contained in a large number of neural network weights), and also the use of well researched pattern recognition theory.

3. Theoretical Background

Originally artificial neural networks were offered as a model of human brain. Artificial neuron, developed by McCulloch and Pitts [8, 9], was considered a model for biological neural networks. Many neural architectures were developed and investigated, some of which differ greatly from their original biological prototypes and which are actually the implementation of mathematic methods of approximation, classification and control. At present one of the neural architectures, feedforward networks, is the most well researched one and has a solid theoretic background and effective training methods [10]. These ideas were very important for our work; that is why we will discuss only feedforward networks.

Artificial neural networks are schemes, which implement multivariable function, matching a set of inputs to a set of outputs $X \rightarrow Y$ by given examples. In this case a neural network consists of inputs $X = \{x_i\}, i = 1..N,$ two layers of artificial neurons, connected with weighted links,

$$W^h = \{w^h{}_{ji}\}, W^o = \{w^o{}_{kj}\}, j = 1..J, k = 1..K$$

and outputs $Y = \{y_k\}$.

In analytical form the functions implemented by the neural networks are represented as:

hidden layer function

$$p^h{}_j = \sum_{i=1}^{N} w^h{}_{ji} \cdot x_i + b_j, \quad j = 1..J \quad ,$$
$$z_j = g(p^h{}_j)$$

output layer function

$$p^{o}{}_{k} = \sum_{j=1}^{J} w^{o}{}_{kj} \cdot z_{j} + c_{k}, \quad k = 1..K$$

$$y_{k} = g(p^{o}{}_{k})$$

In these formulas g(.) are transfer functions of the scheme providing non-linear transfer. There were many transfer offered and researched, e.g. threshold, saturated linear transfer, sigmoid, and arctangent function. Adaptable parameters of neural networks are: $W^{h} = \{w^{h}{}_{ji}\}, W^{o} = \{w^{o}{}_{kj}\}$ - neural network weights, b_{j}, c_{k} - biases.

A neural network works correctly only if its parameters W^{h}, W^{h} are selected correctly. There are many training algorithms, some of which are very effective ones for training particular types of neural networks, e.g. backpropagation training is suitable for multiplayer neural networks with differentiable transfer functions.

One of the principal questions connected with training and using of feedforward neural networks is the question of what kinds of mapping $X \to Y$ can be modeled by the neural network. Many publications are devoted to the research of this question [11]. It is determined that in case of using non-linear transfer functions, feedforward networks can approximate any continuous mapping $X \to Y$ given enough hidden layer neurons.

A set of theorems is proven on approximation of continuous multivariable functions by a set of continuous functions of single-variable. The proof of this fact is given in many publications. For instance in [12] and other works, a proof is given that a neural network containing two layers of adaptive parameters can approximate any continuous input-to-output mapping with pre-selected accuracy given enough hidden layer neurons and suitable training.

4. Method Description

In order to be cryptographically safe, the method must meet the following conditions (partly taken from [16, 17]):

Condition 1. Transformation of biometric parameters into a cryptographic key should succeed with false positive rate low enough to reconstruct the key effectively. The false accept probability should be low so that linear search could not reconstruct a cryptographic key. False negative rate should provide comfortable work: number of consecutive retrieval attempts should not exceed 3-5 in worst case.

Condition 2. Transformation of biometric parameters into a cryptographic key should be done directly without an intermediate yes/no decision-making and without keeping a cryptographic key in the system explicitly.

Condition 3. An intruder should not be able to compute a cryptographic key with a fast algorithm using a biometric template from the database. Besides that we state the following condition: an intruder should not be able to compute correct values of biometric parameters with a fast algorithms even if he knows a correct cryptographic key.

Condition 4. Retained cryptographic key must be replaceable. Besides that we state the following strict condition: biometric parameters should also be replaceable.

One of the most difficult requirements is the requirement of low computational complexity. Taking into account the cryptographic context of our problem, the most acceptable form of this requirement is: computational complexity should be comparable with the complexity of finding the same key with other methods.

Soft condition - computational complexity must match the time of the fastest method of cryptanalysis; determination of such time is valid only in context of a certain cipher, in this case we can use some average time values.

Hard condition - computational complexity must match the time of exhaustive search of stored cryptographic key.

The method, which satisfies these conditions, is a special case of a biometric recognition system. It consists of independent procedures: user cryptographic key enrollment and cryptographic key release.

Figure 2 shows cryptographic key enrollment and release schemes. This scheme resembles the standard scheme of biometric authentication, however biometric template creation aims at its saving. Similarly, instead of user recognition, key release and check is performed. Among many existing biometric identifiers it is necessary to exclude those which are not used with interactive user recognition and are not well researched (DNA, body odour, earprint, palm thermogram, etc) [1]. The other identifiers can be used with the proposed method, however it is necessary to consider such characteristics as identifier uniqueness, password variability, and biometric identifier variability.

1. Uniqueness: it is obvious that any biometric identifier is unique enough to identify a person, but it should provide reliable storage of the cryptographic key, which demands higher level of uniqueness (see Condition 1).
2. Key replaceability: matches one of the stated requirements for biometric system, we should assume that any biometric feature will potentially provide key replaceability with the respective key enrollment method (see Condition
3. Biometric identifier replaceability is the possibility to change one biometric pattern to another for a chosen

biometric identifier (see Condition 3). For instance, when a voice password is compromised, it can be changed with another one without changing the system. In case this opportunity is not provided, when a user biometric pattern is compromised (e.g. his palmprint), his authenticity is compromised as well. A set of publication discusses the possibility of "identity theft" in digital society.

Rule 1.1. Only replaceable biometric features, such as voice password, password keystroke dynamics, password handwrite dynamics are secure. Also we shall consider the application of fingerprint password namely the replaceable password, based on fingerprints. This work is devoted to the use of voice password; many publications demonstrate successful use of voice features for authentication as well as for key generation. Besides that, this type of biometric pattern is considered one of the most hygienic and natural ones.

Biometric features. The choice of transformation of biometric identifiers into digital parameters is very important. Wrong choice of transformation can lead to the decrease of feature variability for different users and can decrease recognition rate. In fact, the uniqueness itself, which is often the main criterion of quality, hardly influences false positive and false negative rates deeply. These rates depend on dispersion properties of selected parameters. Here we state the following obvious requirements to biometric parameters.

The more similar are biometric patterns, the closer should be their biometric parameters, i.e. $\mathit{If}\ D(X_i, X_j) \to 0,\quad \mathit{then}\ d(x_i, x_j) \to 0$, where X_i, X_j are any two biometric patterns, $x_i = F(X_i), x_j = F(X_j)$ are respective biometric parameters, *D is a certain similarity measure, d is a similarity measure in parameter space.*

The less similar are the biometric patterns, the more distant should be their biometric parameters in parameter space, i.e. $\mathit{If}\ D(X_i, X_j) \to \infty,\quad \mathit{then}\ d(x_i, x_j) \to \infty$, where X_i, X_j are any two biometric patterns, $x_i = F(X_i), x_j = F(X_j)$ are respective biometric parameters, D is a certain subjective similarity measure, d is a similarity measure in parameter space.

Often it is necessary to reduce dimensions of biometric parameters in comparison with a source biometric pattern; this requirement is often fair because otherwise decision-making algorithm becomes slow and complex.

The idea of subjective similarity is rather complex and often controversial; even experts' opinions about similarity of various biometric patterns can differ greatly.

Thus similarity condition should be weakened in the following way.

Rule 2.1. If $X_i, X_j \in \Lambda, Y_k \notin \Lambda$ and $x_i = F(X_i), x_j = F(X_j),\ y_k = F(Y_k)$, then $d(x_i, x_j) < d(x_i, y_k)\ \forall i, j, k$, where Λ is a set of biometric features of a single user. That is the distance between any two biometric feature vectors of one user should be less than the distance to any biometric feature vector, which do not belong to this user.

Besides that there are following considerations regarding cryptographic strength of this method.

Rule 2.2. The number of parameters must be low enough to provide effectiveness of decision rules; increased number of parameters leads to additional noise in data and obstructs correct work of decision-making rule, however the number of parameters must be big enough to prevent brute-force attacks in parameters space.

Besides that, when biometric parameters are chosen, many factors should be taken into account, e.g. complexity of parameter computation, expert estimations.

Commonly used speech parameters were estimated according to the stated criteria. These are Fourier-calculated cepstrum, Lpc-calculated cepstrum, Fourier coefficients, Reflection coefficients.

The estimations showed that the use of lpc-calculated cepstrum is optimal. The number of coefficients is chosen in the range of 25-35 according to the analysis of variance, each coefficient is represented by 4-byte floating point value.

Artificial neural network is the most important element, which characterizes security and accuracy of the proposed method. The neural network can operate in two modes: training mode (for key saving), and recognition mode (for key releasing).

During training the neural network learns to match user's biometric parameters ($F_1, F_2, ..., F_N$) and his private key (PPK). As we already mentioned in section 1, the functioning of the neural network is completely determined by its weights W and biases b_j, c_k. The main objective of training is to tune weights W to minimize the difference between target vector (desired output) and actual output vector. The training is performed until training error E_t reaches desired minimal value (threshold P_t). After training, neural weights are saved; then they are loaded again to restore neural network functionality. The procedures of training and releasing are shown on Figure 4. Whenever user biometric parameters are enrolled, they are submitted to the neural network ($F_i \subset \Lambda$), where Λ is the set of enrolled users' parameters; the network generates his personal private key (PPK). If illegal user parameters are submitted, i.e. $G_j \not\subset \Lambda$, a random bit set (RBS) is generated by the network, depending on its weights.

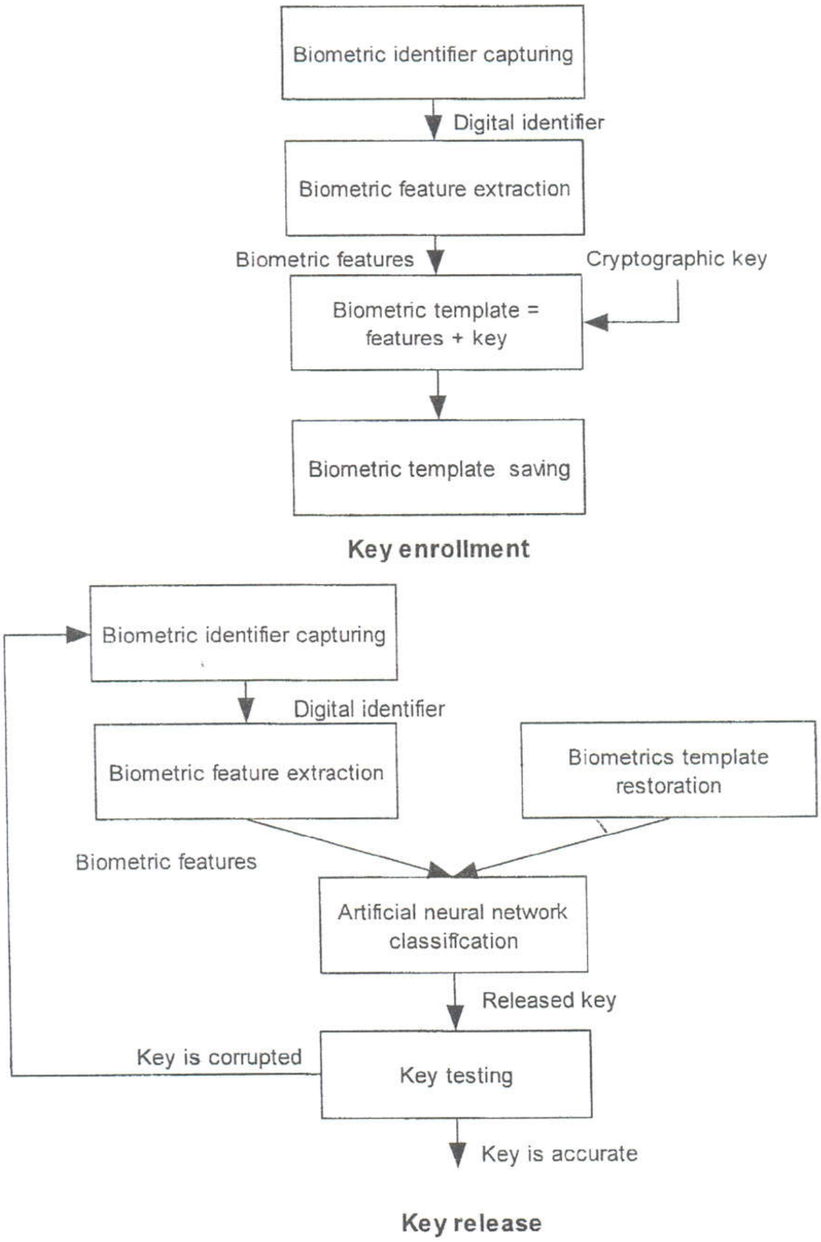

Biometric identifier capturing
Digital identifier
Biometric feature extraction
Biometric features
Cryptographic key
Biometric template = features + key
Biometric template saving
Key enrollment
Biometric identifier capturing
Digital identifier
Biometric feature extraction
Biometrics template restoration
Biometric features
Artificial neural network classification
Released key
Key is corrupted
Key testing
Key is accurate
Key release

Figure 2. Key Enrollment and Release Schemes

The principal question is whether the network can work this way. A neural network with two hidden layers can approximate any continuous mapping with pre-selected precision provided enough neurons. However the stated mapping is not continuous because it is determined with the following rule:

$$f(x)=\begin{cases}PPK, x\in\Lambda\\ RBS_i, x\notin\Lambda\end{cases}. \qquad (1)$$

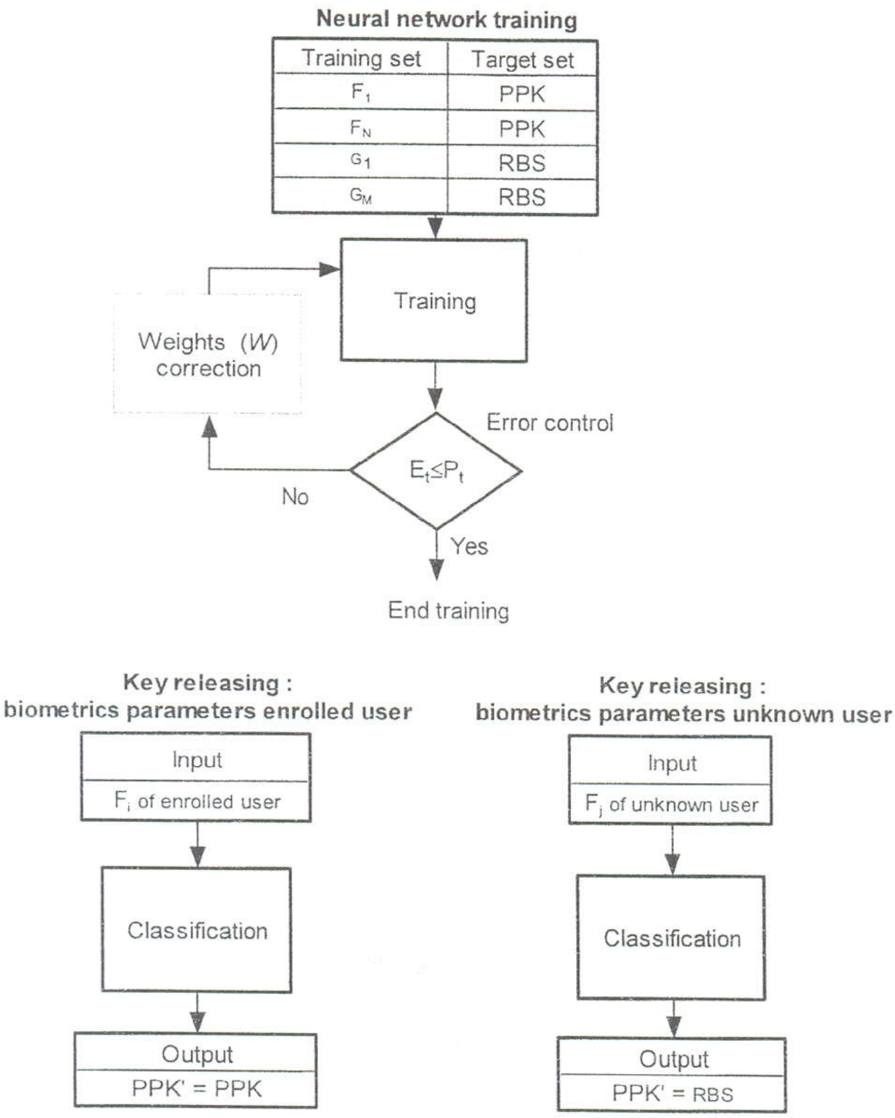
That is a certain area of biometric parameters must be mapped by the neural network into one bit set.

The second rule in (1) implies the fact that each point of the feature space is mapped into a random point from the key space, which doesn't meet condition of continuousness. Taking this into account we expect that this mapping is transformable to piecewise-continuous mapping such as

$$f(x)=\begin{cases}PPK, x\in\Lambda\\ RBS_i, x\in K_i\end{cases}. \qquad (2)$$

Such weakening of previously stated condition is not principal because:

- transformation of biometric features into cryptographic key is kept unchanged;
- transformation of areas K_i into random areas does not give an intruder any information about secret key.



Training set	Target set
F_1	PPK
F_N	PPK
G_1	RBS
G_M	RBS

Figure 3. Network Training and Key Releasing

Thus a neural network allows to approximate required mapping with necessary precision, determined by hidden layer neurons quantity and training algorithm.

As it was shown above, in order to train a feedforward neural network a backpropagation-based algorithm is needed. We chose resilient backpropagation as one of the most effective training algorithms. The condition of training termination is either falling of mean square error below a chosen threshold or a number of training epochs becomes higher than a chosen limit.

According to condition 1 the method should provide releasing of the correct cryptographic key only; otherwise collisions with encryption and decryption are unavoidable. A key checking method was developed to solve this problem.

On enrollment phase:

64-bit random number P is generated. P is encrypted with PPK key, the result is hashed. Any strong algorithms of encryption and hashing can be used, e.g. they could be AES and SHA:

$$P \xrightarrow[Encrypt(PPK)]{} E \xrightarrow[Hash]{} H,$$

$$P \xrightarrow[AES(PPK)]{} E \xrightarrow[SHA-1]{} H$$

P and H are encrypted with PPK key, in order to receive E_{full} it must be stored in the database with neural network

$$[P\ H] \xrightarrow[Encrypt(PPK)]{} E_{full}$$

$$[P\ H] \xrightarrow[AES(PPK)]{} E_{full}$$

On release phase:

PPK' key is released. E_{full} is decrypted using PPK' key. P' and H' are extracted, i.e.

$$E_{full} \xrightarrow[decrypt(PPK')]{} [P'\ H']$$

$$E_{full} \xrightarrow[AES(PPK')]{} [P'\ H']$$

P' is encrypted with PPK' key, the result is hashed to H''.

$$P' \xrightarrow[Encrypt(PPK')]{} E'' \xrightarrow[Hash]{} H''$$

$$P' \xrightarrow[AES(PPK')]{} E'' \xrightarrow[SHA-1]{} H''$$

If $H' = H''$, the key is $PPK' = PPK$

Key generation. The method does not require a fixed PPK- generation algorithm. Keys are generated by the respective cryptographic algorithms; they should be strong enough for chosen encryption algorithm. These methods are researched well and are not discussed in this paper.

5. Experiments

According to the described method, the software system model of transformation of voice password parameters into a cryptographic key was developed. 20 speakers of various age without appreciable deviations in an articulation participated in experiments. Voice samples are recorded in conditions of ordinary office sound environment. For extraction of informative features the voice signal is segmented using Hamming windows approximately 20 – 400 ms each (200 - 400 samples) with 50% overlap. 25 to 35 cepstral coefficient are calculated in each window. 32-bit random cryptographic key is used as PPK. Random 32-bit sets are used as RBS. The obtained training set is used for training of the three-layer feedforward neural network. Resilient backpropagation was used for training [18].

During experiments were estimated such parameters as probability of wrong key restoration at correct voice parameters (false rejection rate), correct key restoration at wrong voice parameters (false acceptance rate) and memory size needed for key restoration, memory size for neural network parameters. The total number of experiments was over 10^6. The results are shown on Table 1 and Table 2.

Table 1[2]

Layer size	FAR	FRR	Training time, sec.	Testing time, sec.
80	0.0035	0.35	250	1.5
120	0.0012	0.20	350	2.25
150	0.0025	0.20	400	3.0

The neural network with 120 hidden neurons demonstrates the best results. Detailed results are shown in Table 2.

Table 2

False acceptance rate	False reject rate (ones)	False reject rate (double)	False reject rate (trip.)
0.00125	0.2	0.1	0.04

We can see that the average value of FAR is 0.00125; the average value of FRR is 0.2, the probability of two sequential rejections is 0.1; and the probability of three sequential rejections is 0.04. Memory requirements to store neural network parameters are less than 40 KB. Authentication evaluation time is 0.22 sec.

As we mentioned above the experiments were carried out with 32-bit cryptographic keys. This key length is not used in practice, so a quadruple replication scheme was developed to store 128-bit keys. The scheme has a set of peculiarities compared with the basic scheme. During key enrollment each neural network trains to match voice password parameters and one of the 32-bit parts of 128-bit key. It is important to note that training sets for each neural network are created so that they could guarantee mutual statistical independence of FAR and FRR for each network. During key release each network releases one part of the cryptographic key. Experiments displayed the following results: average value of FAR $= 2 \cdot 10^{-13}$, average value of FRR is approximately 0.20. Storage memory size of four neural networks parameters is less than 160 KB. 128-bit key restoring time = 0.9 sec.

6. Conclusion

The proposed method has a lot of advantages compared to traditional biometric authentication methods including the fact that it doesn't allow an intruder to attack the system as shown on Figure 1. The development of the proposed method and its characteristics are given in our publications. Advantages of the developed method allow to use it to provide biometric access control for unprotected devices, such as PDA, smartphones, remote biometric access devices, secure biometric authentication off-card matching.

Acknowledgments

This work was supported by grants from the Russian Foundation for Basic Research (grant # 06-07-89010-a).

References

1. Anil J. Kain, Bolle Ruud and Pankanti Sharath "BIOMETRIC: Personal identification in networked society". Kluwer Academic Publichers, 1999.

[2] PC Intel Celeron 1.7 GHz, 128 MB RAM, 2000 SP3, Dhrystone = 3500 MIPS, Whetstone = 900 MFLOPS

2. Soutar C., Roberge D., Stojanov S.A., Gilroy R. and Kumar Vijaya B.V.K. "Biometric encryption using image processing". In: *Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques II*, Vol. 3314, 1998, pp. 178-188.

3. Davida G.I., Frankel Y. and Matt B.J. "On enabling secure applications through off-line biometric identification". In: *Proc. of Symp. Privacy and Security IEEE*, 1998, pp. 148-157.

4. Davida G.I., Frankel Y., Matt B.J. and Peralta R. "On the relation of error correction and cryptography to an offline biometric based identification scheme". In: *Proc. of Workshop Coding and Cryptography (WCC'99)*, 1999, pp. 129-138.

5. Monrose F., Reiter M.K. and Wetzel S. "Password hardening based on keystroke dynamics". In: *Proc. of 6th ACM Conf. Computer and Communications Security*, 1999, pp. 73-82.

6. Verbitskiy E., Tuyls P., Denteneer D. and Linnartz J.P. "Reliable biometric authentication with privacy protection". In: *SPIE Biometric Technology for Human Identification Conference*, Orlando, FL, USA, 2004.

7. Juels A. and Wattenberg M., "A fuzzy commitment scheme". In: *Proc. 6th ACM Conf. Computer and Communications Security*, G. Tsudik, Ed., 1999, pp. 28–36.

8. McCulloch W.S., Pitts W.A. "A logical calculus of the ideas immanent in nervous activity". *Bull. Math. Biophys*, 1943; 5: 115-133.

9. Pitts W.A., McCulloch W.S. "How we know universals: The perception of auditory and visual forms". *Bull. Math. Biophys*, 1947; 9: 127.

10. Haykin S. "Neural Networks: A Comprehensive Foundation. Prentice Hall", 2nd edition. Upper Saddle River, New Jersey, 1999.

11. Poggio T. and Girosi F. "Networks and the best approximation property". *Biological Cybernetics*, 1990; 63: 169-176.

12. Hornik K., Stinchcombe M. and White H. "Universal approximation of an unknown mapping and its derivatives using multilayer feedforward networks". *Neural Networks*, 1990; 3: 551-560.

13. Stone M.H. "Applications of the Theory of Boolean Rings to General Topology". *Transactions of the American Mathematical Society*, 1943; 41(3): 375-481.

14. Stone M.H. "The Generalized Weierstrass Approximation Theorem". *Mathematics Magazine*, 1948; 21(4): 167-184 and 21(5): 237-254.

15. Gorban A.N. "The generalized Stone-Weierstrass approximation theorem and approximation of continuous functions of several variables by an arbitrary non-linear function of one variable, linear functions and their superpositions". *Advances in Modelling and Analysis*, Vol. 35, 1999; 1: 7-13.

16. Uludag U., Pankanti S., Prabhakar S., Jain A.K. "Biometric Cryptosystems: issues and challenges". In: *Proc. of the IEEE*, Vol. 92, 2004, pp. 948-960.

17. Monrose F., Reiter M.K., Qi Li, Wetzel S. "Cryptographic Key Generation from Voice". In: *Proc. of IEEE Symposium on Security and Privacy*, 2001. www.cs.jhu.edu/~fabian/papers/oakland.pdf.

18. Riedmiller M. and Braun H. "A direct adaptive method for faster backpropagation learning: The RPROP algorithm". In: *Proc. of the IEEE International Conference on Neural Networks*, 1993.

19. Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D. and Whiting D. "Improved Cryptanalysis of Rijndael Seventh Fast Software Encryption Workshop". Springer-Verlag, 2000. http://www.schneier.com/paper-rijndael.html.