Mathematical Problems of Computer Science 38, 56–58, 2012.

Information-Theoretic Approach to Biometric Identification Problem

Mariam E. Haroutunian, Lilit A. Ter-Vardanyan

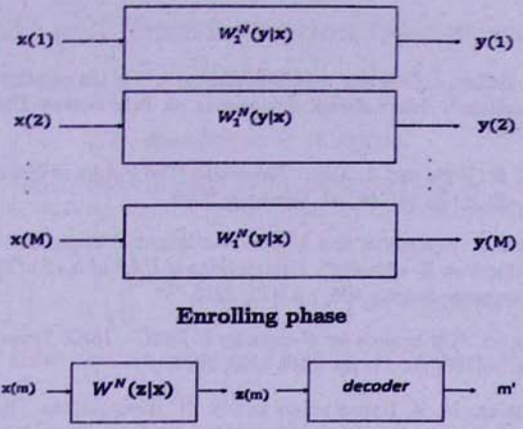
Institute for Informatics and Automation Problems of the National Academy
of Sciences of the Republic of Armenia
armar@ipia.sci.am, lilit@sci.am

Nowadays people live in the era of large-scale computer networks connecting hug numbers of electronic devices. These devices execute applications that use networks for e changing information. Sometimes the information that is transmitted within these network and stored by the devices is sensitive to misuse. Moreover, the networks and devices cann always be trusted. Also illegal copying of copyrighted content, illegal use of e-payment sy tems, and identity theft can be foreseen. Traditional systems for access control, which a based on the possession of secret knowledge (password, secret key, etc.). Moreover, passwor can often be guessed, since tend to use passwords which are easy to remember.

Biometrics is the technology that is used to uniquely identify a specific human being. I is primarily used to provide security for personal or business assets. A biometrics syste must first store a person's biometric data. Then, when someone tries to access a personal c business system, the stored biometric data is compared to the data of the person currentl accessing the system. If the data matches up, the person can have access to the protecte information.

Biometric systems offer a solution to most of the problems mentioned above. They coul either substituted for traditional systems or used to reinforce them. Biometric systems a based on physical or behavioral characteristics of human beings, like faces, fingerprints, voic irises. The results of the measurement of these characteristics are called biometric data. Bi metric data have the advantage that potentially they are unique identifiers of human bein A biometrics system must first store a person's biometric data. Then, when someone tries t access a personal or business system, the stored biometric data is compared to the data of th person currently accessing the system. If the data matches up, the person can have access t the protected information. The attractive property of uniqueness, that holds for biometric also results in its major weakness. Unlike passwords, biometric information, if compromise once, cannot be canceled and easily replaced by other biometric information, since peopl only have limited resources of biometric data. Requirements for biometric systems shoul include secure storage and secure communication of biometric data in the applications whe they are used.

The problem of biometric identification is transferred to information-theoretical mod by Willems et al [1]. The model of a biometric system is shown in Figure 1.



Enrolling phase

Identification phase

Figure. 1. Model of biometric identification system

Biometrical identification in general involves two phases. In an enrollment phase all individuals are observed and for each individual a record is added to a database. This record contains enrollment-data, i.e. a noisy version of the biometrical data corresponding to the individual. In the identification phase an unknown individual is observed again. The resulting identification-data, another noisy version of the biometrical data of the unknown individual, is compared to (all) the enrollment-data in the database and the system has to come up with an estimate of the individual. Essential in this procedure is that both in the enrollment-phase and in the identification-phase noisy versions of the biometrical data are obtained. The actual biometrical data of each individual remain unknown.

Willems et al [1] investigated the fundamental properties of biometric identification system. It has been shown that it is not possible to identify reliably more persons than capacity which is an inherent characteristic of any identification system. They derived the capacity of such system.

We investigate the exponentially high reliability criterion in biometric identification systems. In other words we introduce a new performance concept of biometric identification E-capacity, which takes into account a stronger requirement on identification fault events with extremely small probability (2^{-NE} instead of ε). In terms of practical applications an exponential decrease in error probability (namely, in unwanted identification faults) is more desirable. We investigate the E-capacity function, which is the generalization of the capacity, as it tends to capacity, when E tends to 0. Upper and the lower bounds for identification E-capacity for maximal and average error probabilities are constructed in [3]. When $E \to 0$ we derive upper and lower bounds of the channel capacity, which coincide with the capacity obtained in [1]. When $E \to 0$ we derive the lower and upper bounds of the channel capacity, which coincide with the capacity obtained in [1].

A similar result is obtained for the biometric identification system with random parameter, which is more realistic for applications.

References

[1] F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, "On the capacity of a biometrical identification system", *International Symposium on Information Theory*, Yokohama, Japan, p. 82, 2003.

[2] S. Pankanti, R. M. Bolle and A. Jain, "Biometrics-The Future of Identification", *IEEE Computer*, vol. 33, no. 2, pp. 46 49, February, 2002.

[3] M. Haroutunian, A. Muradyan and L. Ter- Vardanyan, "Upper and lower bounds of biometric identification E- capacity", *Transactions of IIAP of NAS of RA, Mathematical Problems of Computer Science*,v36, pp.1-10, 2012.

[4] E. A. Haroutunian, "On bounds for *E*-capacity of DMC", *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4210-4220, 2007.

[5] E. A. Haroutunian, M. E. Haroutunian and A. N. Harutyunyan, "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, no 2-3, pp. 97-263, 2008.

[6] M. E. Haroutunian, "Estimates of *E*-capacity and capacity regions for multiple-access channel with random parameter", *Lecture Notes in Computer Science*, vol. 4123, Springer Verlag, pp. 196-217, 2006.

[7] M. E. Haroutunian, S. A. Tonoyan, "Random coding bound of information hiding *E*-capacity", *Proc. of IEEE International Symposium on Information Theory*, p. 536, USA, Chicago, 2004.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[9] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.