Comparison of Biometric and Linguistic Secret Sharing Protocols

Lidia Ogiela, Marek R. Ogiela, Urszula Ogiela
AGH University of Science and Technology
Cryptography and Cognitive Informatics Research Group
30 Mickiewicza Ave., 30-059 Krakow, Poland
logiela@agh.edu.pl, mogiela@agh.edu.pl, ogiela@agh.edu.pl

Abstract. In this paper will be presented comparison and security features of biometric and linguistic threshold schemes. Additionally efficiency evaluation for such protocols will be done. Possible application of presented algorithms will be described with future directions in the area of strategic information management, and security for cloud applications.

1 Introduction

For division of strategic data cryptographic threshold protocols were proposed. The first sharing methods were proposed in late seventies, but till now it have been proposed many complex, efficient, and secure algorithm. All such techniques define two different classes i.e. secret sharing techniques and secret splitting. Data sharing algorithms were presented manly in [1], [2], [3], and the main idea of such methods is to secure information by split them between particular groups of participants. All secret splitting methods allow to generate a particular number of secret parts (called shadows), than distribute them among participant of protocol. But to restore the original information it is necessary to compile all the secret parts. In secret sharing approaches shadow generation is very similar, but to restore the original information it is enough to compile a less number of secret parts. Secret sharing is more universal and allows to restore the previous information also in case of losing any secret parts.

For similar tasks we propose two new types of threshold procedures called biometric threshold schemes and linguistic threshold schemes. These algorithms allow involving some personal information into the encryption process [4], [5], [6], [7]. In following section will be presented these procedures with theirs features evaluation and comparison.

L. Barolli et al. (eds.), *Advances on Broad-Band Wireless Computing, Communication and Applications*, Lecture Notes on Data Engineering and Communications Technologies 2, DOI 10.1007/978-3-319-49106-6_49

2 An Idea of Linguistic Threshold Schemes

The first proposed technique for information sharing is linguistic threshold procedure [1]. The main idea of such methods lays in using mathematical linguistic formalisms for representation of shared data and encoding procedure. In this technique it is necessary to define special type of formal grammars which enable encoding bit sequences with different length. It only depends on the defined formal grammar as well as some features, which may be additionally encoded in one of generated secret parts. The way of information encoding using linguistic procedures is more general encoding scheme use in DNA cryptography [8], [9]. However in classic DNA cryptography can use only four nitrogen bases, to encode particular bits of information or two bits block in particular nitrogen bonds.

In linguistic threshold schemes it is possible to create more general encoding structure, which allows encoding in one step, more than two bits of information e.g. 5, 6 or more.

3 Information Division Using Biometric Threshold Schemes

Second approach is connected with using some personal features in sharing protocol. Such technique is called biometric threshold schemes and was proposed by authors in [9]. In biometric threshold schemes each shadow is generated using biometric features. In biometric threshold schemes is possible to use the single biometric feature or several different patterns [10], [11]. The most popular biometric patterns appropriate for this purpose are:

- fingerprint patterns,
- handwriting features,
- retina patterns,
- facial features,
- hand vein layouts,
- voice parameters.

Sometimes we can also consider different non-standard personal features obtained from different sources like medical records, personal habits or behavioral feature [12], [13].

The biometric data encryption is realized in two separated steps. The first one, is after splitting the information, and contains indexing procedure for each shadow by biometric features. The second one, is realized while combining the strategic information.

Such techniques allow to perform secure data sharing processes, because each participant gives only shadow marked by his or her personal features. It isn't possible to give shadow to non-trusted participants.

4 Comparison of Linguistic and Biometric Sharing Protocols

Both described classes of proposed threshold procedures i.e. linguistic threshold procedures and biometric threshold protocols are not only very interesting from scientific point of view, but also extend features of classic threshold procedure. Biometric and linguistic threshold procedures are extensions for classic threshold procedure, and remain all security features, which characterize classic protocols. Both of them have also some important additional features, which are not present in classic threshold algorithms. Among such additional features in linguistic threshold procedures we can find:

1. Application of formal grammars and languages to split strategic information.
2. Possibility to encode block of information with different bit length.
3. Polynomial complexity which depends on applied formal grammar.
4. Possible application for strategic data sharing in different management structures like layered as well as hierarchical structure [14], [15].
5. Possibility to generate personalized shadows, which determine the way of information encoding.
6. Application in secure information management tasks for different structures.
7. Possibility to generate different number of secret parts considering personal accessing grant to original information.

Most important additional features in biometric threshold procedures are following:

1 Possibilities of creating personalized shadows. Such shadows allow not only restoring original information but also determining the owner of secret part [16].
2 Applicability with cognitive information systems at the stage of personal feature extraction [17], [18].
3 Standard and non-standard biometrics may be use in shadow generation.
4 Unlimited number of shadows can be generated.

Mentioned features, make these systems very universal with many possibilities of different application.

5 Conclusions

Described in this paper sharing protocols have many important features, which make them applicable in personalized cryptography or secure information management tasks. These protocols seem to be very efficient and secure because security features are guaranteed by basic threshold procedure, which may be use in the whole sharing protocol. Additionally both of these procedures have some special properties, which extend its functionality.

In biometric threshold procedures it is possible to use some personal characteristics, which finally allow creating personalizes parts of divided information. Such feature allows determining who is the owner of secret part, what also prevent the information leakage, when such protocol may be violated.

In linguistic threshold schemes it is possible to divide information in different manners considering the numbers of trusted persons and also theirs accessing grants to restore original information. Both of these protocols may be applied in general secret sharing application, but also in professional strategic data sharing and management, and trusted communication infrastructures [19]. They may also be applied in secured data distribution in the cloud environment, and information or services management in ubiquitous computing or ambient world.

Acknowledgments. This work has been supported by the National Science Centre, Republic of Poland, under project number DEC-2013/09/B/HS4/00501.

References

1. Ogiela, M.R., Ogiela, U.: Linguistic Approach to Cryptographic Data Sharing, FGCN 2008 – The 2nd International Conference on Future Generation Communication and Networking, December 13-15, 2008, Hainan Island, China, 1 (2008) 377–380
2. Ogiela, M.R., Ogiela, U.: Grammar Encoding in DNA-Like Secret Sharing Infrastructure. 2nd International Conference on Advanced Science and Technology (AST), Miyazaki, Japan, Jun 23-25, 2010. LNCS 6059, (2010) 175-182
3. Ogiela, M.R., Ogiela, U.: Shadow Generation Protocol in Linguistic Threshold Schemes. in: D. Slezak, T.H. Kim., W.C. Tang et all., Security Technology, Communications in Computer and Information Science 58 (2009) 35-42
4. Ogiela, L., Ogiela, M.R.: Cognitive systems for intelligent business information management in cognitive economy. International Journal of Information Management, 34 (2014) 751-760
5. Shi, J., Lam, K-Y.: VitaCode: Electrocardiogram Representation for Biometric Cryptography in Body Area Networks. 1st International Conference on Ubiquitous and Future Networks, Hong Kong, China, Jun 07-09 (2009) 112-115
6. Kumar, A., Kumar, A.: Adaptive management of multimodal biometrics fusion using ant colony optimization. Information Fusion 32 (2016) 49–63
7. Shi, J., Lam, K-Y.: VitaCode: Electrocardiogram Representation for Biometric Cryptography in Body Area Networks. 1st International Conference on Ubiquitous and Future Networks, Hong Kong, China, Jun 07-09 (2009) 112-115
8. Ogiela, L.: Semantic analysis and biological modelling in selected classes of cognitive information systems. Mathematical and Computer Modelling, 58 (2013) 1405-1414
9. Ogiela, L., Ogiela, M.R.: Cognitive systems and bio-inspired computing in homeland security. Journal of Network and Computer Applications, 38 (2014) 34-42
10. Bajwa, G., Dantu, R.: Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Computers & Security 62 (2016) 95-113
11. Hani, M.K., Marsono, M.N., Bakhteri, R.: Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. Future Generation Comp. Syst. (2013) 800–810
12. Hachaj, T., Ogiela, M.R.: CAD system for automatic analysis of CT perfusion maps. Opto-Electronic Review, 19 (2011) 95-103
13. Nandakumar, A.K.J.K., Pankanti, S.: Fingerprint-based fuzzy vault: Implementation and performance. In: IEEE Transactions on Information Forensics and Security. 2 (2007) 744–757
14. Ogiela, L.: Towards cognitive economy. Soft Computing 18 (2014) 1675-1683
15. Ogiela, L., Ogiela, M.R.: Management Information Systems. in: J.J. Park, Y. Pan, H.C. Chao, et all., 2nd FTRA International Conference on Ubiquitous Computing Application

and Wireless Sensor Network (UCAWSN), South Korea, 07-10 July 2014, Ubiquitous Computing Application and Wireless Sensor, Lecture Notes in Electrical Engineering 331 (2015) 449-456

16.Ogiela, L.: Cognitive informatics in image semantics description, identification and automatic pattern understanding. Neurocomputing 122 (2013) 58-69

17.Ogiela, L.: Cognitive Computational Intelligence in Medical Pattern Semantic Understanding. in: M. Guo, L. Zhao, L. Wang (Eds.), Fourth International Conference on Natural Computation, ICNC 2008, Jinan, Shandong, China, 18-20 October, 2008, 245-247

18.Ogiela, L.: Computational Intelligence in Cognitive Healthcare Information Systems. in: I. Bichindaritz, S. Vaidya, A. Jain et all., Computational Intelligence in Healthcare 4: Advanced Methodologies, Studies in Computational Intelligence 309 (2010) 347-369

19.Ogiela, L.: Data management in cognitive financial systems. International Journal of Information Management 33 (2013) 263-270