Behavioral Keys in Cryptography and Security Systems

Marek R. Ogiela[1(✉)] and Lidia Ogiela[2]

[1] Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering, AGH University of Science and Technology, 30 Mickiewicza Ave., 30-059 Krakow, Poland
mogiela@agh.edu.pl

[2] Cryptography and Cognitive Informatics Research Group, AGH University of Science and Technology, 30 Mickiewicza Ave., 30-059 Krakow, Poland
logiela@agh.edu.pl

Abstract. In this paper will be presented new ways of using some behavioral features and habits for security purposes and cryptography. In particular several different solutions will be described, which present possible application of selected behavioral patterns, characteristic for particular users. Such behavioral patterns can be extracted thanks to the application of new generation cognitive vision systems. Obtained personal feature, can be next use for security reasons, as well as in cognitive cryptographic protocols.

1 Introduction

In modern cryptographic technologies and security protocols an important role may play application of some, very specific and individual human characteristics, including behavioral features. In many situations we need to use some protocols, which should be oriented on particular user or be assigned to user of communication protocol. To create such human oriented cryptographic procedures we can use specific or very unique personal features, including behavioral patterns. Of course involving personal features into security procedures should allow providing required security level, and be connected with particular user. In this paper will be described selected approaches, based on application of personal and behavioral patterns, in creation of such security protocols. Extraction or registration some specific behavioral features are usually very difficult, but application of cognitive vision systems allow us to evaluate some common behavioral patterns, like hand or finger movements, specific human body motions or unusual personal gesture. Having such specific behavioral patterns or personal gestures, we can find many interesting application in creation protocols for securing strategic or classified data, guarantee secure transmission, remote services management or application in the Cloud environment and many others [1–3]. Everything shows that in near future such technologies may play important role in ambient cities, pervasive computing and IoT [4–6].

The main goal of this paper will be presentation of possible application of personal and behavioral features for security purposes and cryptographic protocols. Presented solutions will be based on evaluation of behavioral feature vectors, which next can be

L. Barolli et al. (eds.), *Advances in Intelligent Networking and Collaborative Systems,*
Lecture Notes on Data Engineering and Communications Technologies 8,
DOI 10.1007/978-3-319-65636-6_26

involved into the encryption process [6, 7]. Such solutions are very promising for development of modern security technologies based on vision systems, which can monitor personal habits, movement characteristics or other human motion actions. Such new procedures may allow extending existing cryptographic methodologies towards a new branch of cognitive cryptography [8, 9].

2 Acquisition of Behavioral Patterns

For security application it is possible to use different motion and behavioral patterns. From our point of view, the most interesting is acquisition of nonstandard personal features in the form of behavioral patterns, which may be applicable for security purposes. Conducted research showed that for such purposes are very useful cognitive vision systems [5, 10].

In general cognitive systems try to imitate the mental functions and thinking processes, and are based on one of the known model of human visual perception, named knowledge based perception [4, 11]. In this model cognitive resonance processes are performed, which allow to understand observed situation or patterns, and allow evaluating the semantic meaning. Using cognitive information systems we tried to show some new opportunities in application of personal and behavioral features in new security protocols and cryptographic procedures. Such features may be used in creation of strong encryption keys or creation of a special kind i.e. personalized behavioral lock. It is worth underline that creation of such cryptographic solutions is inspired by biological models and finally allows to create a new branch called cognitive cryptography defined in [7, 12]. This new computational paradigm combines techniques, which are using to guarantee data confidentiality, with some personal or behavioral information describing particular user and extracted using cognitive information systems. Such compilation of security approaches with cognitive processes may be very promising for future development of security solutions.

Acquisition of personal features or behavioral characteristics can be performed with application of cognitive vision systems in connection with other motion sensor devices like Leap Motion technologies, Kinect or MoCap devices.

We can consider following different behavioral patterns, which can be used for security application:

- Simple finger or palm movements. For registration of such simple patterns we can use Leap Motion or Kinect devices. Personal feature vector may be next created using cognitive vision systems, which allow extracting informative parameters registered by these recording devices.
- More complex motion patterns performed using hands or other human body parts may be analyses by advanced motion capture devices connected with cognitive vision systems.
- The most complex patterns (specific exercises, sport techniques) may be analyzed using dedicated recording equipment with cognitive features.

Presented methodology allows analyzing different types of behavioral patterns, and create personal feature vector, which next may be used in creation personalized security solutions. Among the most important areas of application of behavioral features for security purposes we can consider:

- Visual cryptography and secret sharing protocols.
- Personally oriented information management procedures.
- Fuzzy vault and steganography which depend on personal feature [2].

3 Hand Gesture Features for Security Applications

For security applications we can consider different specific behavioral patterns, also these connected with gesture or movement activities.

Application of motion sensors or Kinect devices, which allow trace and register finger or palm movements, allow also to extract some specific motion features and use them for security purposes. The simplest solution is using hand or single finger movements or gesture for personal authentication procedures, during which we can extract very specific personal features, which next may be used as behavioral lock or authentication keys. Finger motion analysis seems to be one of the most natural and simplest, so it may be focused on tracing a fingertip positions changes during making particular gesture. Analysis of simple gestures has many advantages like noninvasive data acquisition, possibility of analysis of different gesture types like user determined, fixed movement patterns, or natural gesture. It allows considering also the motion dynamics and acceleration of performed gesture, and may be performed in real-time.

In real security applications we should consider only enough complex gesture or movements, which will be sufficient for obtaining the distinctive features for particular user, which are not similar to other persons. To register such complex patterns we can analyze movements performed using one or more fingertips or, if necessary, for using the palms or hands.

To register unique personal gesture features we can use any motion sensor (Kinect, MoCap etc.), which is able to register hand position changes during the time. As a result we can create a personal motion feature vector, which contain very unique parameters describing performed gesture like direction, velocity and acceleration.

In conducted research we have implemented such procedures, which involve cognitive systems for hand and finger analysis. In the first stage of such analysis it is necessary to create a learning set, which contain particular number of well-defined motion patterns. The second stage allows classifying a new pattern by comparing it with elements stored in learning set. Such comparison is made by calculation any similarity measure between new registered motion pattern and elements stored in learning set. Base on a feature vector and classification function, it is possible to determine the type of hand or finger movement, but also it is possible to use such feature vector as a specific behavioral key or in other security applications like personalized encryption key generation, multi secret steganography, fuzzy vault etc. The security of such behavioral keys is strongly depended on complexity of analyzed movements, so for stronger cryptographic solutions should be considered more complex or very specific gestures.

4 Complex Movements for Security Applications

Beside simple behavioral features describing hand or finger movements it is also possible to consider more complex individual movements performed while walking, dancing or practicing sport. In general analysis of such movements is more difficult and should be connected with registration of motion sequences, but in some special cases it may also be done towards extraction of personal feature vector for security application. The reason is very simple, and connected with different abilities of performing very complex movement by different persons, which are strongly dependent on personal habits, physical conditions, age, and skills. For example persons acknowledgeable with infrequent dances can perform it in his personal manner, and such performance allows evaluating some specific personal features, which may be next used for security purposed.

In the same way we can consider some sport and gym activities and extract specific features from recording presenting very high sport skills or techniques e.g. acrobatics, martial arts etc. (Fig. 1).

Fig. 1. Extraction of personal features from sport and acrobatic techniques.

Analysis of several sport activities towards evaluating very specific motion feature can be done in the same way as in [12]. Having such specific motion features we can use them for security purposes in the same manner as described previously with connection to finger and palm gestures.

5 Conclusions

In this paper we have presented different possibilities of using personal features and unique characteristics for security application and cryptography. Personal information extracted from motion sequences and representing behavioral features may be used in security protocols dedicated for information sharing, fuzzy vaults and multi-secret steganography. Besides traditional simple finger and palm movements, for security application we can consider more complex gesture patterns representing personal behavioral

features. Extraction of personal or behavioral characteristics is possible thanks to the application of cognitive information systems, which allow evaluate unique parameters from nonstandard personal patterns or specific human body movements. Application of such specific and unique parameters proved that personal features and cognitive systems can be used in development of advanced cryptography procedures for strong key generation, secret management, visual cryptography, and creation of behavioral lock.

Acknowledgments. This work has been supported by the AGH University of Science and Technology research Grant No 11.11.120.329.

References

1. Cox, I.J., Miller, M.L., Bloom, J., Fridrich, J., Kalker, J.: Digital Watermarking and Steganography. Morgan Kaufmann Publishers, Burlington (2008)
2. Jin, Z., Teoh, A.B.J., Goi, B.-M., Tay, Y.-H.: Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recogn. **56**, 50–62 (2016)
3. Ogiela, L.: Computational intelligence in cognitive healthcare information systems. Stud. Comput. Intell. **309**, 347–369 (2010)
4. Ogiela, L.: Cognitive informatics in image semantics description, identification and automatic pattern understanding. Neurocomputing **122**, 58–69 (2013)
5. Ogiela, L., Ogiela, M.R.: Beginnings of cognitive science. In: Advances in Cognitive Information Systems. Cognitive Systems Monographs, vol. 17, pp. 1–18 (2012)
6. Ogiela, L., Ogiela, M.R.: Data mining and semantic inference in cognitive systems. In: Xhafa, F., Barolli, L., Palmieri, F., et al. (eds.) 2014 International Conference on Intelligent Networking and Collaborative Systems (IEEE INCoS 2014), Salerno, Italy, pp. 257–261, 10–12 September 2014
7. Ogiela, L., Ogiela, M.R.: Management information systems. In: Park, J., Pan, Y., Chao, H.C., Yi, G. (eds.) Ubiquitous Computing Application and Wireless Sensor. LNEE, vol. 331, pp. 449–456. Springer, Dordrecht (2015)
8. Ogiela, M.R., Ogiela, U.: Linguistic approach to cryptographic data sharing. In: FGCN 2008 – The 2nd International Conference on Future Generation Communication and Networking, Hainan Island, China, vol. 1, pp. 377–380, 13–15 December 2008
9. Ogiela, M.R., Ogiela, U.: Security of linguistic threshold schemes in multimedia systems. Stud. Comput. Intell. **226**, 13–20 (2009)
10. Ogiela, M.R., Ogiela, U.: Shadow generation protocol in linguistic threshold schemes. In: Ślęzak, D., Kim, T., Fang, W.C., Arnett, K.P. (eds.) Security Technology. CCIS, vol. 58, pp. 35–42. Springer, Heidelberg (2009)
11. Ogiela, M.R., Ogiela, U.: Grammar encoding in DNA-like secret sharing infrastructure. In: Kim, T.-h., Adeli, H. (eds.) ACN/AST/ISA/UCMA -2010. LNCS, vol. 6059, pp. 175–182. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13577-4_15
12. Ogiela, M.R., Ogiela, U.: Secure Information Management Using Linguistic Threshold Approach. Advanced Information and Knowledge Processing. Springer, London (2014)