Multimed Tools Appl
DOI 10.1007/s11042-013-1780-6

An image-based key agreement protocol using the morphing technique

Qian Mao · Chin-Chen Chang · Lein Harn · Shih-Chang Chang

Abstract Most traditional key agreement protocols are based on data exchange. In this paper, a novel key agreement protocol based on image exchange is proposed. In this protocol, the communication entities who want to establish a session key are pre-assigned a secret image by the registration center (RC) initially. In real-time communication, using this image as the source image, along with another image of her/his choosing as the target image, the entity creates a morphed image and transmits it to the other communication entity. At the receiver side, the entity de-morphs the received image using the same source image and recovers the target image. However, the recovered image is not completely the same as the original image because some pixels have been lost during the morphing process. Therefore, the relationship between the original image and the morphed image needs to be analyzed and the lost pixels are located accurately. By removing the lost pixels from the self-generated original image and the recovered image of the other entity, both communication entities can obtain the same information that can be used as the secret session key. This approach using the exchanged morphed

Q. Mao
School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, No. 516, Jungong Rd., Yangpu, Shanghai 200093, People's Republic of China
e-mail: maoqiansh@gmail.com

Q. Mao · C.-C. Chang
Department of Computer Science and Information Engineering, Asia University, No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan

C.-C. Chang (✉)
Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
e-mail: alan3c@gmail.com

L. Harn
Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64110, USA
e-mail: harnl@umkc.edu

S.-C. Chang
Department of Computer Science and Information Engineering, National Chung Cheng University, 160 San-Hsing, Ming-Hsiung, Chiayi 621, Taiwan
e-mail: chang.coby@gmail.com

Published online: 28 November 2013