Contents

NFC Smartphone Based Access Control System Using Information Hiding

Peng-Loon Teh, Huo-Chong Ling, SoonNyean Cheong

1 Abstract

In the paper, they proposed a digital access control system by using near field communication (NFC) smartphone to unlock the door and replace the access card. They mentioned that if the system uses the access card or physical key as key to access the premise, then everyone who has the key can gain the access which is an insecure system. So, they provided an information hiding technique to overcome the problem by using stego-photo. System will generate the passcode and embedded it into the users photo which will become the stego-photo. The NFC reader will receive the stego-photo sent by smartphone, if the passcode inside the stego-photo is not match with the passcode inside the database, a light emitting diode (LED) will be turned on to alert the unauthorized users.

2 Problem Solved

If the access card access password matches the password stored in the access control system, the door will unlock, and the user has access to his premises. Once the access card is lost, anyone who is in the possession of the card could easily enter the premise illegally.

3 Claimed Contributions

The system prevented unauthorized people who get the key (smartphone) will not be able to access to the premise. Access control system using access card will not prevent this problem.

4 Related work

A. *Access Control System using Physical Keys and Mechanical Locks*
In this system, as users can easily by using physical key to lock or unlock the door.

B. *Access Control System using Digital Keypad*
In this system, as users can pressing numeric password to get access the door.

C. *Access Control System Using Digital Access Cards*
In this system, as users can using the access card to get access the door.

D. *Biometric Access Control System*
In this system, as users can uses physical part to get access the promise. For example, fingerprint or authentication. [2]

5 Methodology

The user need to register an account first through the security web-page. The user submits an access passcode and uploads a photo to the web-page to generate the stego photo. [4] The system will translate the passcode to American Standard Code for Information Interchange(ASCII) number and use the Least Significant Bit(LSB) insertion [1] to embed the translated passcode into the photo. The stego photo is generated and user can download it to the smartphone by scanning the Quick Response(QR) code. The user tags his smartphone on the NFC reader [3] of the door. A link will sent to the smartphone to initial a program to let user to send the stego photo to the reader. If the passcode decoded from stego photo is same as the passcode inside the server, the door will be unlocked. However, it is not matched, a light emitting diode(LED) will be turned on to alert the unauthorized user.

6 Conclusions

In this paper, they used NFC and hiding information technique, stego photo to enhance the access control system to solve the problem of unauthorized people can access to the premise with the access card. The enhanced system is more secure, but it is more inconvenient.

7 What did you learn ? And possible extention/Future work

For further work, we can implement the near field communication (NFC) and stego photo to replace the touch n go card. This will improve the security level of the touch n go card and it will become an evolution of the e-wallet.

References

[1] Information hiding techniques for steganography and digital watermarking. 2000.

[2] A. Batool and A. Tariq. Computerized system for fingerprint identification for biometric security. pages 102–106, Dec 2011.

[3] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger. Nfc devices: Security and privacy. pages 642–647, March 2008.

[4] Huanyu Zhao and Xiaolin Li. S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. 2:467–472, May 2007.