ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

IJIREEICE INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 10, October 2015

NFC Hardware Device Based Access Control System using Information Hiding

Snehal Muke[1], Shubhangi Shinde[2], Chetana Mistry[3], Prof. Prashant B. Jawalkar[4]

Student, Computer, JSPM's BSIOTR, Pune, India[1, 2, 3]

Asst. Prof. JSPM's BSIOTR, Wagholi, Pune[4]

Abstract: In the fields of data security, access control is the selective restriction of access to a place or other resource. Digital Security access control systems are designed to avoid unauthorized entry. It will control one door in a single room or many arrivals in an entire building. This is truly the best way to limit or control access to certain areas and know who has been where and when. It is introduced as an alternative system to the most common access control system using physical keys, mechanical locks, digital keypads, digital access cards, biometric access control to increase the level of ease to access a statement. However, an intruder is able to gain access to the premise if he possesses the access card or the physical keys. We propose an access control system that utilizes near field communication (NFC) device information hiding technique using stegenography to overwhelmed the disadvantage mentioned previously on the existing systems.

Keyword: Access control system, NFC smartphone/device, near field communication, information hiding, authentication, stego-photo.

I. INTRODUCTION

Nowadays, the number of building break-in cases increases and this problem is increasingly severe from time to time. An access control system serves as a necessity prevention to reduce the number of building break-in and at the same time, provide a safer alternative in security perspective. An access control system is simply defined as any technique used to control passage into or out of any area or any entry, such as residential area, office and others. The evolution of science and technology creates a new generation of the access control system, known as digital access control system.

Digital access control system allows users to access a area digitally using an access card. The term 'digitally 'gradually eliminates the need of using physical keys. In other words, the access card is stored with the user's access passcode and in order to gain access to the premise, he simply taps his access card in front of a reader. The access passcode within the access card is then transmitted to an access control system for verification. If the access passcode in the access card matches with the access passcode stored in the control system, the door will be unlocked and the user can gain access to his premise. However, the access card is not bound to the user. Once the access card is lost, anyone who is in the possession of the card could easily enter the premise illegally.

In this paper, we propose an access control system based on the concept of two-factor authentication [1], a security process that provides two means of identification: one of which is typically something that the user has, and the other is typically something that the user wants to be memorize or know. The proposed system uses the concept of Near field communication (NFC) and stegnography to overcome the disadvantage exhibited by the access control system using the access card. NFC is defined as a short range wireless communication protocol that is primarily intended to be used on smartphone/device. It operates based on Radio Frequency Identification (RFID) technology [3], and it is a contactless system that uses radio frequency (RF) waves to transfer or accept data over a short distance from a tag, typically several centimeters away [3]. In recent years, NFC smartphone/devices start to appear to fulfill the proximity communication requirements, such that the arrival of contactless NFC technology makes life easier [4]. For example, NFC smartphone/devices replace the role of electronic cards like access card or credit card. With NFC, all these cards are stored within smartphone/devices and the data is transmitted by touching to another devices or transaction is made by touching to the payment device.

Together with NFC smartphone/device, the proposed access control system uses stego-photo that is generated from the information hiding technique. Information hiding [5] refers to the process of embedding important or secret information into a cover object, such as image, audio, video or text to generate a stego-object such that the existence of the information in the stego-object is not visible to the human eyes. In this paper,

Information hiding refers to the process of embedding an access passcode into a user's photo to generate a stego-photo. In section II, we describe four existing access control systems. We then describe the proposed access

DOI 10.17148/IJIREEICE.2015.31016

control system in section III. System implementation and results are given in section IV, and section V determines this paper.

II. SYSTEM COMPONENTS AND WORKFLOW

A. The following subsections describe four different existing access control systems [6-10] that are being implemented.

1. Authorised entries using Physical Keys and Mechanical Locks

The most common type of access control system utilizes physical keys and mechanical locks. In this system, physical keys play an important role as users simply lock or unlock the door with a physical key. Despite the manufacturing cost of the system that is relatively inexpensive and the simplicity of the system, it still possesses some limitations. Firstly, it is inconvenient to carry a bunch of keys around. For instance, if a user owns several units of premises, he has to carry several bunches of keys around. Secondly, users may sometimes carelessly leave the physical keys at home or forget to take along the keys when nobody is at home. There is no alternative way to gain access to the premise unless the user has spare keys. Thirdly, physical keys may get lost or stolen easily. Anyone who is in the possession of the physical keys is able to gain access to the premise as physical keys are not able to recognize the legitimate user. In order to make the system more secure, digital keypad is utilized as described in the following subsection.

2. Access Control System using Digital Keypad

The evolution of science and technology creates a new generation of the access control system known as a digital access control system. Users gain access to the premise by just entering numeric password on the keypad. Thus, the level of convenience increases tremendously as compared with the system that utilizes physical keys as users do not need to carrylarger and heavier bunch of keys around. However, this system possesses weakness in the security perspective. A potential drawback of using keypad system is that it is more susceptible to shoulder surfing attack [6]. In shoulder surfing attack, a spy from a distance might observe or record the overall process of the user keying the numeric password.

3. Access Control System using Digital Access Cards

Access card is another approach that allows users to access their premise using an access card. Likewise to the keypad system, the convenience has been enhanced significantly in digital system as the smaller and lighter access card is far more convenient to carry around compared with the larger and heavier bunch of keys. Unfortunately, the probability to lose the smaller and lighter access card is higher than physical keys. The emergence of the access card allows proximity of contactless mechanism to be developed [7]. For instance, a physical contact between the key and door lock and effort in entering password in keypad system are required in order to access the premise. In the case of access card, users have to wave the access card in front of the door reader. The access passcode within the access card is then transmitted to an access control system for verification. The door will only be unlocked if the access passcode is matched with the access passcode stored in the control system. However, users are not bounded to the access card. Once the access card is lost, anyone who is in the possession of the card could easily enter the premise illegally.

4. Biometric Access Control System

Biometric access control system uses physical part of the user, such as fingerprint and iris as a method of authentication. The biometric systems basically implement the same working principle where unique user's finger is utilized to identify and verify the correct user in the fingerprintaccess control system [8]. For example, an authorized user hashis fingerprint physically scanned to the fingerprintreader. The physical characteristic of his fingerprinthas to be recognized by the reader before access is granted. One of the benefits of the biometric system is that itensures user's identification with something that cannot be lost or duplicated. No doubt, the level of convenience is enhanced significantly and this system is far more reliable than the previous systems in terms of speed and accuracy. Nevertheless, this system suffers a drawback in term of hygiene. There is a high possibility that the fingerprint reader does not recognize the user if there is a scar on the user's finger. Besides that, dirt on the fingerprint reader or iris's camera may cause the systems to be malfunctioned. Moreover, cost is another limitation in the biometric system as access control system using physical keys, keypad and access card are normally cheaper than biometric system. In the next section, we propose an access control system that is convenient and secure.

B. System Workflow

In the Proposed System the Computer acts as a registration server where all the users availing this facility needs to register here. On successful registration the Server generates a unique passocde and encodes the passcode in the user photo. The newly created photo which called as a stego photo is downloaded on the users smart phone/device. The User is also issued with a NFC Tag which he/she has to use when access to the door. During the Door access the User first taps the NFC Tag on

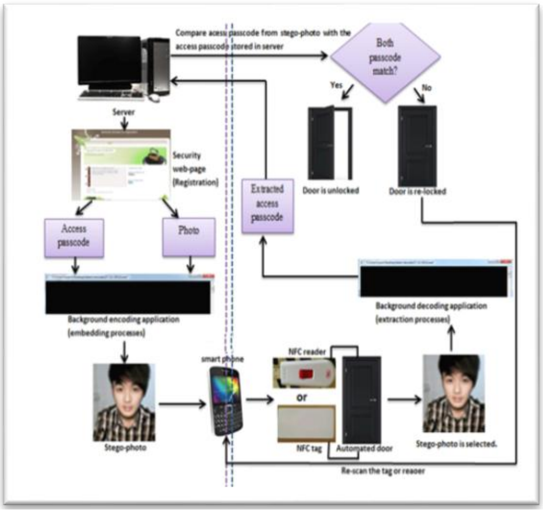
Compare acess passcode from stego-photo with the access passcode stored in server
Both passcode match?
Yes
No
Server
Security web-page (Registration)
Door is unlocked
Door is re-locked
Extracted access passcode
Access passcode
Photo
Background encoding application (embedding processes)
Background decoding application (extraction processes)
NFC reader
smart phone
or
Stego-photo
NFC tag
Automated door
Stego-photo is selected.
Re-scan the tag or reaoer

Fig1. System Workflow

DOI 10.17148/IJIREEICE.2015.31016

the NFC Reader which is connected to the Door System. The Reader send the TAG ID to the Door Computer. The Door computer accordingly sends it the Server for validation. The Server validates the TAG ID and acknowledges the Door computer to select the stego-photo from the user smart phone/device. On stego-photo selection the photo is send to the Door Computer where the software extracts the hidden data using LSB technique. After extraction the data is further send to the server for validation. On Validation of the data the server sends acknowledgement to the door computer software and accordingly directs the door to open if validated else denies and alarm the security.

1. Least Significant Bit (LSB) Insertion

As a proof of concept, least significant bit (LSB) insertion [5] is used as an information hiding method. LSB insertion takes a binary representation of the hidden message and overwrites the LSB of each byte within a cover-photo with the message's bit one by one. This cover-photo uses 24- bit color and is normally represented in the form of pixels. There is an approximately l.7 million of colors (224) forming a palette for a 24-bit image and each pixel is denoted by threebytes in terms of Red, Green, and Blue (RGB). The operation of LSB insertion is relatively simple and it can be well understood by showing an example of embedding a letter 'A' into a 24-bit image. The letter 'A' has an American Standard Code for Information Interchange (ASCII) number of 65 and 01000001 in binary. Each pixel is denoted by three bytes in RGB, and therefore three consecutive pixels arerequired to embed the letter 'A' into the 24-bit image. Since three pixels consist of a total of nine bytes, an extra byte isleftover.

2. Encoding and Decoding Processes

In general, the encoding and decoding processes involve the embedding and extraction processes respectively Encoding process is executed when the background application detects the existence of the access passcode and the user's photo. The program starts with the opening of a cover photo and a stego-photo files (stego-photo is an empty file). Then, the cover photo pixels are read and displayed in binary representation. Next, the text file with the access passcode is opened for reading.The access passcode is then embedded into LSB of each byte within cover photo. The program then writes the modified bytes of pixels into stego-photo. The remaining unmodified bytes are read and written into stegophoto.

A stego-photo is thus generated. On the other hand, decoding process is executed when the background application detects the existence of the stegophoto sent back to the server.

Fig. 3 shows the flowchart of the decoding process. The program starts when a stego-photo received from the NFC smartphone/device is opened. The stego-photo pixels are then read and displayed in binary representation. The LSB of each byte of stego-photo is retrieved and each 8-bit is grouped and converted into an ASCII character to obtain access passcode. The extracted access passcode is then compared with the one in the server for verification. The door is unlocked if both passcode match, and remained locked if both do not match.

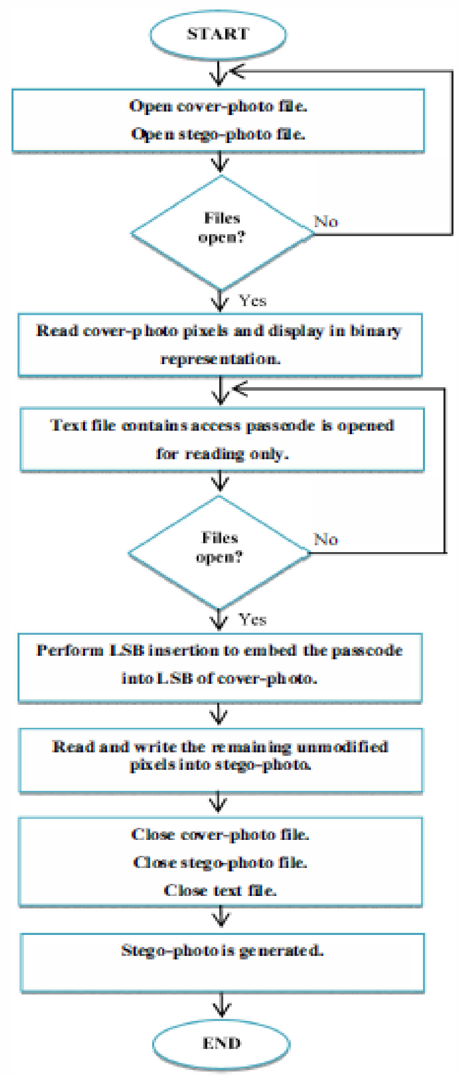
START
Open cover-photo file.
Open stego-photo file.
Files open?
No
Yes
Read cover-photo pixels and display in binary representation.
Text file contains access passcode is opened for reading only.
Files open?
No
Yes
Perform LSB insertion to embed the passcode into LSB of cover-photo.
Read and write the remaining unmodified pixels into stego-photo.
Close cover-photo file.
Close stego-photo file.
Close text file.
Stego-photo is generated.
END

Fig2. Flowchart of encoding process

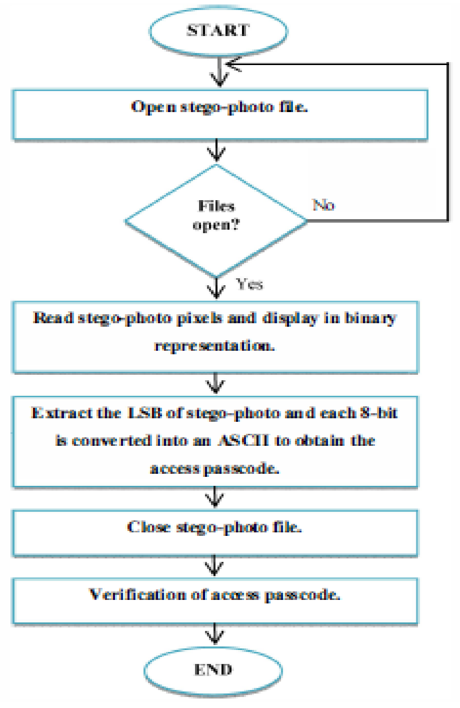
START
Open stego-photo file.
Files open?
No
Yes
Read stego-photo pixels and display in binary representation.
Extract the LSB of stego-photo and each 8-bit is converted into an ASCII to obtain the access passcode.
Close stego-photo file.
Verification of access passcode.
END

Fig3. Flowchart of decoding process

III. APPLICATIONS

NFC fall under three different categories upon its usage in different fields.
1- Service initiation category
2- 2- Peer-to-Peer category
3- 3- Payment and Ticketing category

1. Service initiation:-
In this scenario functioning of NFC is the same as of RFID. NFC device reads some data from a tag and uses this information in several different ways. In this case tag serves as transponder, it could be a turned off cell phone. NFC device can read the data even if the cell phone is powered off. Example of such scenario can be the advertisement or information poster.

2. Peer-to-Peer:-
In this application direct link between two devices is set up to transfer data. Amount of data may not be too large. If user wants to transfer large amount of data, Wi-Fi or Bluetooth connection can be set up, but that is invisible to user.

3. Payment and Ticketing:-
In this scenario cell phone is used as electronic wallet. Nowadays we are using cards only for payments. But with NFC equipped device multiple functions could be collected under the same platform. Virtual money can be loaded in the cell phone that can be used to pay travelling tickets or parking fees.

IV. CONCLUSION

In this paper, we have proposed an access control system based on the concept of two-factor authentication [1]. The proposed system utilizes NFC smartphone/device (i.e. something that the user has) and stego-photo (i.e. something that the user knows) to overcome the disadvantage exhibited by the access control system using the access card. This system has been introduced as a trade off balance between security and convenience. If the level of security increases, the level of convenience decreases and vice versa. This is true as a secure system typically is a complex system and requires complex algorithms which will eventually sacrifice the convenience. An insecure system, on the other hand, performs simple algorithm, thus convenience is dominant.

REFERENCES

[1] F. Aloul, S. Zahidi, and W. El-Hajj, "Two Factor Authentication Using Mobile Phones," in IEEE/ACS International Conference on Computer Systems and Applications, vol. 6, pp. 641-644, May 2009.
[2] AA Hussein, and AA Mohammad, "Near Field Communication (NFC)," International Journal of Computer Science and Network Security, vol. 12(2), pp. 93-100, Feb. 2012.
[3] J. Christian, J. Scharinger, and Gerald, "NFC Devices: Security and Privacy," in Proc. of the 2008 Third International Conference on Availability, Reliability and Security, pp. 642-647,2008.
[4] C.H. Dubin, "Get Smart About Access Control," International Journal of Electronics Applications, vol. 2,p p. 112-115, Oct. 2011..
[5] S. Narayana, and G. Prasad, 'Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions," International Journal of Signal and Image Processing, vol. 1(2), pp. 60-73, Dec. 2010.
[6] A Kumar, and K.M. Pooja, "Steganography-A Data hiding Technique," International Journal of Computer Applications, vol. 9, pp. 1-5, Nov. 2010.
[7] V. K. Sharma, and V. Shrivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection," Journal of Theoretical and Applied Information Technology, vol. 36(1), pp. 1-8, Feb. 2012.
[8] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric Authentication: A Review," International Journal of Science and Technology, pp. 13-16, Sept. 2009.
[9] H. Zhao, and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme ", Scalable Software Systems Laboratory Department of Computer Science Oklahoma State University, Stillwater, USA.
[10] M. Lourde, and D. Khosla, "Fingerprint Identification in Biometric Security Systems," International Journal of Computer and Electrical Engineering, pp. 852-853, Oct. 2010.