International Journal of Internet, Broadcasting and Communication Vol.12 No.2 1-7 (2020)
http://dx.doi.org/10.7236/IJIBC.2020.12.2.1

IJIBC 20-2-1

Building Control Box Attached Monitor based Color Grid Recognition Methods for User Access Authentication

Sung Hoon Yoon*,**, Kil Soo Lee**, Jae Sang Cha***, Timur Khudaybergenov****,
Min Soo Kim****, Deok Gun Woo*****, Jeong Uk Kim†******

** Ph.D Candidate, Department of Energy grid, Graduate School, Sangmyung University, Seoul, Korea*
E-mail: sh_yoon@nate.com
*** KOGEN Co., Ltd, Korea*
**** VTASK Co., Ltd, Korea*
***** PhD Course, Graduate School of NID Fusion, Seoul National Univ. of Sci. & Tech., Korea*
****** IoT Convergence Research Technology Lab, Seoul National Univ. of Sci. & Tech., Korea*
******* Professor, Department of Electrical Engineering, Sangmyung University, Seoul, Korea*
E-mail: jukim@smu.ac.kr † Corresponding Author

Abstract

The secure access the lighting, Heating, ventilation, and air conditioning (HVAC), fire safety, and security control boxes of building facilities is the primary objective of future smart buildings. This paper proposes an authorized user access to the electrical, lighting, fire safety, and security control boxes in the smart building, by using color grid coded optical camera communication (OCC) with face recognition Technologies. The existing CCTV subsystem can be used as the face recognition security subsystem for the proposed approach. At the same time a smart device attached camera can used as an OCC receiver of color grid code for user access authentication data sent by the control boxes to proceed authorization. This proposed approach allows increasing an authorization control reliability and highly secured authentication on accessing building facility infrastructure. The result of color grid code sequence received by the unauthorized person and his face identification allows getting good results in security and gaining effectiveness of accessing building facility infrastructure. The proposed concept uses the encoded user access authentication information through control box monitor and the smart device application which detect and decode the color grid coded informations combinations and then send user through the smart building network to building management system for authentication verification in combination with the facial features that gives a high protection level. The proposed concept is implemented on testbed model and experiment results verified for the secured user authentication in real-time.

Keywords: *Color Grid, Face Recognition, Control System Box, Access Control System, Smart Building*

1. Introduction

Manuscript Received: February. 2, 2020 / Revised: February. 10, 2020 / Accepted: February. 14, 2020
Corresponding Author: jukim@smu.ac.kr
Tel: +82-2-781-7602, Fax: +82-2-781-7602
Department of Electrical Engineering, Sangmyung University, Seoul, Korea

A smart building managing and control system is a super-system of interconnected the lighting, Heating, ventilation, and air conditioning (HVAC), fire safety, and security building facility system. The access security is the major issues to focus on accessing interconnected building facility control in the future smart buildings development trend. An authorized user access to the smart building control box systems must be well organized for building facility energy management and security. There are many research related to the network security, and software solutions security for the smart buildings and smart cities [1, 2, 3] are studied and analyse in details. The secure physical access to the building facility control boxes is also very important to issue to consider for smart buildings. Nowadays, most of the building facility uses the access control based on radio-frequency identification (RFID), near-field communication (NFC), bluetooth, Wi-Fi and all these radio frequency (RF) based access control subject to easy security breaches.

In modern data communications standards are providing an opportunity to use light bulbs or a monitor and displays as a data transmitting elements and receive the data using camera that is called optical camera communication (OCC). The optical wireless communication (OWC) standard allows to use a color grid coded data to be transmitted on light illumination devices. The OCC technology allows to enable the communication between the cameras inbuilt the device, like a smart device with any light illumination devices like light-emitting diode (LED), color display based element of building facility infrastructure [4, 5].

In that way, this approach uses of building infrastructure without adding any additional components in the building facility infrastructure and use of light things based access control technology is a perfect to be used in a smart building. This paper proposes the color grid code for user authentication using OCC combined with face recognition technologies to improve access authentication security level. The following sections describes the proposed building facility proposed building facility control box access authentication method, authentication procedure and authentication algorithm , experiment results and analysis, and conclusion in section 2, section 3, section 4, and section 5 respectively.

2. Proposed Building Facility Control Box Access Authentication Approach

The proposed building facility control access authentication uses the hybrid authentication approach by integrating OCC using color grid code for user access authentication with facial biometric authentication method. In this approach the biometric authentication provides based on face recognition with timestamps. The main objective of face recognition systems is to first identify the user is related to building facility management member or not by their facial informations captured by a CCTV camera. The face recognition systems built-in on central management system establish the presence of an authorized person rather than just checking whether a valid identification (ID) or key is being used or whether the user knows the secret personal identification numbers (PIN) or passwords. The face recognition system directly compares the facial features of the users and finding matching ID record in the database [6, 7]. For an example, SecurID is a timestamps technology based on the use of hardware keys and time synchronization. The user authentication works based on the generation of random numbers at specific time intervals.

A unique secret key is stored only in the central access control system server and in the hardware device of the user, in this proposed approach use the smart devices. When the objective user requests control box access, the user is prompted to enter a PIN code, as well as a randomly generated number displayed at that moment in encoded on the display monitor and transmit the user access authentication informations as color grid code. The color grid coded user access authentication algorithm works based on the principles of the OCC. The smart device based OCC color grid code recognition is shown in Figure 1.

The OCC access control algorithm working by the principles of image mapping and color determination according on color grid code position. First of all visual frame which captured from the camera is analyzed to find a region of interest (RoI).The RoI used to transmit the color grid code is a rectangular or square region on the control box connected monitor which is linearly gridded on defined equal spaced areas. After capturing visual frames and the RoI of the visual frame is detected using computer vision algorithm. Then the color value of the center pixels of each grid cell from the RoI is estimated using the color matching principles. From the detected color pattern the transmitted code binary sequence estimated for user access ID verification.

The access control system server application compares the entered PIN code, the objective user secret key and face recognition record from the database, and generates a random number based on the parameters of the secret key from the database and the current time. Then the identity of the generated number and the number entered by the user is verified [8] and provide the authentication status to the accessing user.

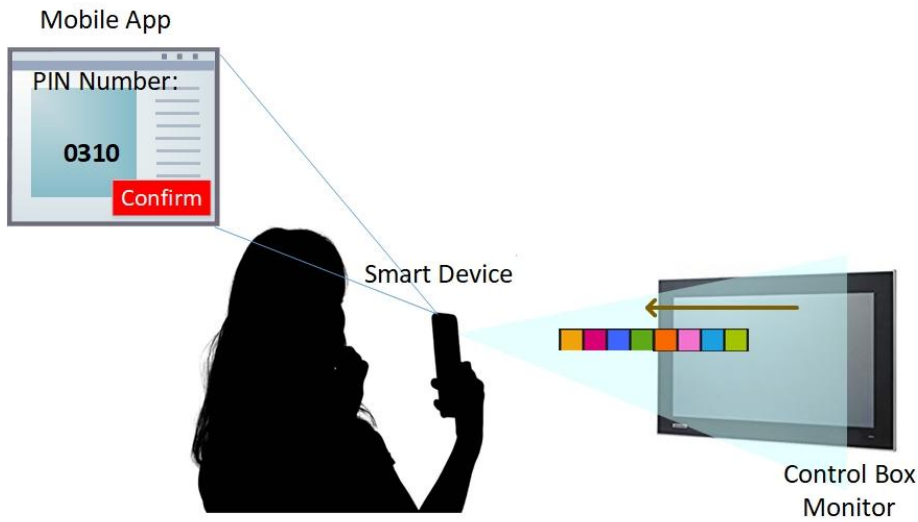


Figure 1. Building Control Box attached Monitor based on Color Grid Recognition Methods

3. Building Facility Control Box User Access Authentication Algorithm

The access control system (ACS) is a complex of hardware and software solutions based on logic of analyses of rights and rules for the registered subscribers to access particular system or region. The ACS rules and access permissions are exactly determined in access control lists (ACL) of users based on their roles and responsibility defined by the building facility administrator. According to ACL, the building facility administrators are allowing different levels of the access to the facility installed control boxes. The use case diagram of the user authentication procedure is shown in Figure 2.

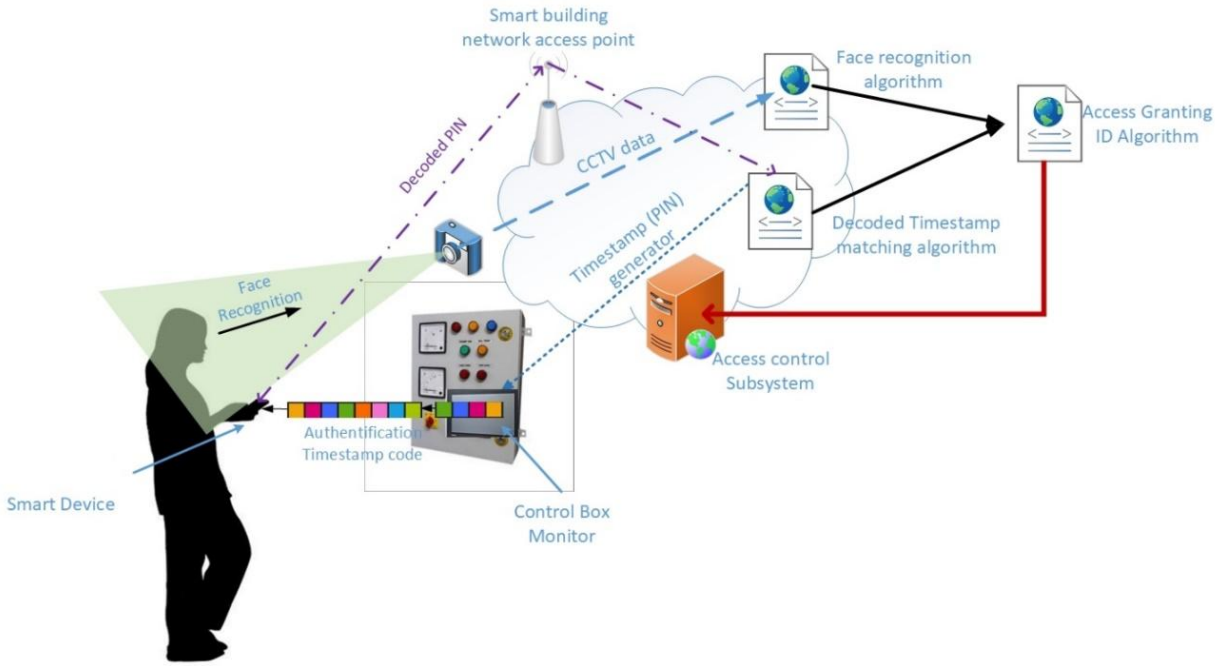


Figure 2. Control Box Access Authentication Block Diagram

The authorization requesting the user getting an authentication code from the monitors attached in building facility control box, in which the user wants to get an access control to use for planned activities. The decoded authorization information from user's smart devices transmitted to the smart building connected cloud based building facility management system to be processed by matching algorithm to recognize the access permitted user device identity (ID).

In parallel, the CCTV camera captures the access requesting user image, which is connected to the smart building network surveillance system and send the image to process in the face recognition [9, 10, 11] system. The user face ID must match in ACL record stored in ACS database, and then determine the access level of the requested user.

If face recognition ID recognition procedure is successful, then the ACS server system proceed an algorithm of user access matching with Face ID and user device ID. And then the ACS server gives the authentication to access the facility installed control box if Face ID and user device ID identification processes are successful.

In this proposed system, the authentication procedure based on the access control subsystem, which is physically a server based remote access architecture model. The ACS Server works with the facility management members user ID records database, which is keeping the user ID records for every registered facility management member and codes to generate timestamp PIN codes based on the access time. Figure 3 illustrates the control box access authentication algorithm processing intercommunication state diagram.

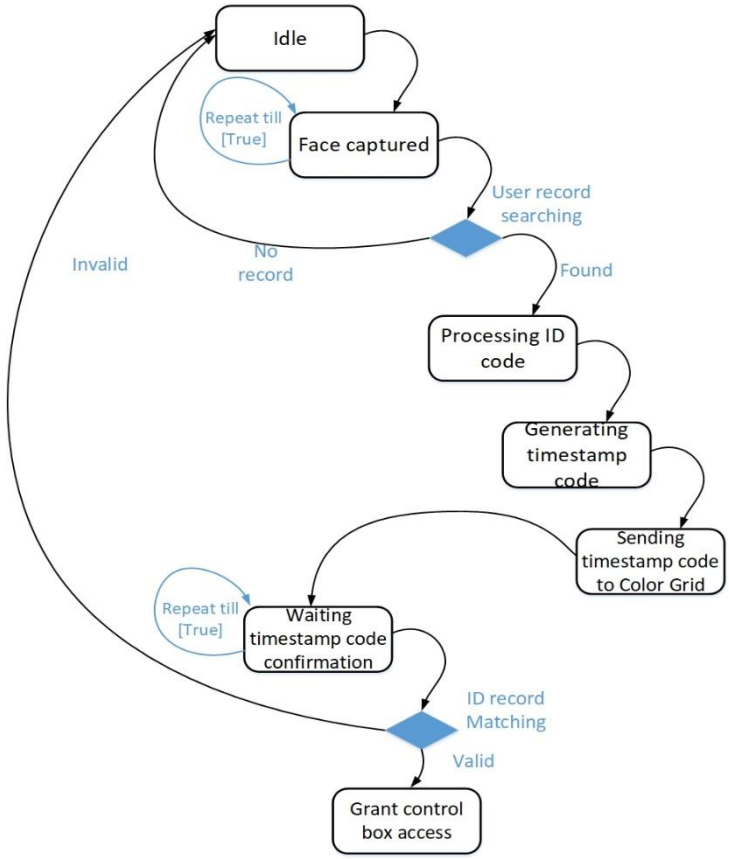


Figure 3. State Diagram of Control Box Access Authentication

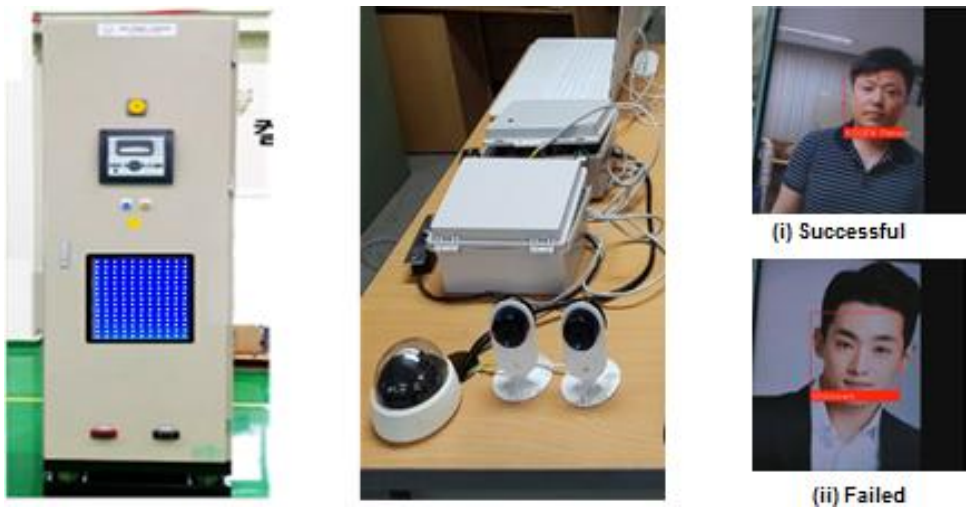
In this proposed control box access authentication algorithm, the CCTV cameras are capturing facial informations of the user who want to get a control box access authentication while system is idle mode. Once the user face ID is recognized then the process of searching of a matching code in the database record is started [6, 7] in the ACS server. The user access specific timestamp PIN code generated and transmitted through the control panel attached monitor using color grid modulation. This user access specific code be decoded only by current user using building facility provided smart devices in which the same user specific code is pre-installed with authentication application. The smart device user authentication client application reads color code from control box connected monitor and decode the timestamp PIN transmitted from control box, and sending back this timestamp PIN to the server for authentication verification.

This proposed algorithm allows to ensure the particular facility management user, in particular time is using registered smart devices with assigned personal identity code. This dual identification code based authentication is working on the fact that knowing the timestamp PIN exact before access and have a key which is matching to his personal ID record. Thus providing a much more reliable level of user authentication compared to reusable passwords. The proposed ACS solution is novel solution that automatically changes the password every fixed time period, regulated by security politics. This proposed double level identification process allows to avoid illegal user access and possible detect identification devices from thefts or misplaced by access users.

4. Experimental Result and Analysis

To evaluate the proposed building facility control box attached monitor based color grid code recognition

for user access authentication, the control box monitor panel is designed using Arduino Mega open-source hardware platform with ESP8266 Wi-Fi controller and Xiaomi 1080P HD CCTV camera installed in the building facility. The building facility control box attached monitor model is shown in Figure 4(a) and the building facility CCTV camera infrastructure is shown Figure 4(b). The controller box and CCTV system connected to ACS server using Wi-Fi. The smart device based custom android demon application developed for user authentication process. The windows framework based deep neural network library (DNNL) used for face recognition in ACS server system. The ACS server designed on Intel i5 core based windows platform.



(a) Control Box with Monitor (b) CCTV Camera (c) Authentication Status

Figure 4. Experimental Results

The OpenCV based computer vision algorithm on smart device application used to recognition color grid code and decode the authentication information. The average time to recognize the color code is 270 milliseconds and windows based ACS server takes 420 milliseconds to recognize the registered users face to authenticate. In overall, the proposed solution take 780 milliseconds to authenticate the access to control box. The proposed solution control box authentication result is shown in Figure 4(c). This proposed system implementation, the color grid data transmission and face recognition allows to organize safe and convenient access control to the control box installed in the building facility. The suggested multi-level authorization for user access gives good results in security and gaining effectiveness of control box protection.

5. Conclusion

This paper presented the color grid code based OCC and face recognition based control box author authentication method that allows to organize safe and convenient access control system solution for the building facility. The presented proposed solution uses the multi-level verification of authorization for requested user to access facility installed HVAC, fire safety, network and security devices and that allows to provide higher security and effective control box protection. This novel VLC based authentication with face recognition techniques is a one of the best way increasing security level and timely response in smart building facility to avoid illegal user access to essential infrastructure management systems.

Acknowledgement

This work (Grants No. S2613746) was supported by project for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups in 2018.

References

[1] H.A. Boyes, "Cyber security of intelligent buildings: a review," 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, January 2013. DOI: 10.1049/cp.2013.1698

[2] M. Mylrea, "Cyber Security and Optimization in Smart Autonomous Buildings," AAAI Spring Symposium Series, 2015. DOI: 10.1007/978-3-319-59719-5_12

[3] Z. Pan, S. Hariri, Y. Al-Nashif, "Anomaly based intrusion detection for building automation and control networks," IEEE/ACS 11th International Conference on, IEEE, 72–77, 2014. DOI: 10.1109/AICCSA.2014.7073181

[4] Jaesang Cha, Vinayagam Mariappan, Sukyoung Han, Minwoo Lee, "Smartphone Color-Code based Gate Security Control," International Journal of Advanced Smart Convergence Vol.5, No. 3, pp.66-71, 2016. DOI: 10.7236/IJASC.2016.5.3.66

[5] Jaesang Cha, Minwoo Lee, Vinayagam Mariappan, "VTASC – Light based Flexible Multi-Dimensional Modulation Technique for OWC," IEEE COMSOC MMTC Communications – Frontiers, Vol.13, No.2, pp.39-43, 2018.

[6] R. Jafri, H. R. Arabnia, "A Survey of Face Recognition Techniques," Journal of Information Processing Systems, Vol.5, No.2, June 2009. DOI: 10.3745/JIPS.2009.5.2.041

[7] D.N. Parmar, B.B. Mehta, "Face Recognition Methods & Applications," International Journal of Computer Applications in Technology, Vol.4, No.1, pp.84-86, 2014.

[8] RSA SecurID Suite, 2019 Available, Online: https://www.rsa.com/en-us/products/rsa-securid-suite

[9] R. Ranjan, S. Sankaranarayanan, C. D. Castillo, and R. Chellappa, "An all-in-one convolutional neural network for face analysis," In Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG), 2017. DOI: 10.1109/FG.2017.137

[10] R. Ranjan, V. M. Patel, and R. Chellappa, "A deep pyramid deformable part model for face detection," In Proceedings of the 7th International Conference on IEEE in Biometrics Theory, Applications and Systems (BTAS), pp.1-8, 2015. DOI: 10.1109/BTAS.2015.7358755

[11] R. Ranjan, A. Bansal, J. Zheng, H. Xu, J. Gleason, B. Lu, A. Nanduri, et al., "A Fast and Accurate System for Face Detection, Identification, and Verification," Journal of latex class files, Vol.14, No.8, 2015. DOI: 10.1109/TBIOM.2019.2908436