New User Authentication Based on Optical Spectrum and Its Realization of Embedded Systems

Chia-Fu Su, Jui-Chieh Kao, Chin-Shiu Shieh, Jui-Fang Chang, and Mong-Fong Horng

***Abstract*—User authentication (UA) is the first and significant step for users before accessing information services. The most popular and typical approach to UA is based on username/password to identify and authenticate users. The traditional approach is neither convenient and nor reliable. In this paper, a new approach based on optical spectrum is proposed. The authentication code is generated according to optical spectrum to make password secure. Besides, the generated code is renewed after the code has been authenticated. Such a one-time password effectively protects systems from the malicious copy and skimming attacks. A numeric analysis illustrate that the proposed approach have lower crack probability than iris and fingerprint authentication. The proposed UA is realized on an Arduino Nano Board to verify the feasibility. The results illustrate the UA proposed by this study. Have potential to surpass the existing user authentication technology at security. And it is reliable, low-cost and feasible system design.**

***Index Terms*—Embedded system, one-time password, optical color coding, user authentication.**

I. Introduction

According to the statistics report from the world-renowned market research company, IDTechEx in 2015, the global RFID product market reached 10.1 billion USD and is estimated to 13.2 billion USD in 2020. Obviously, demand for intelligent user authentication technology will keep growing with smart life in future. As known, intelligent user authentication technology gradually replaces the traditional password-based technology. Optical-based authentication has attracted lots of researcher to discover the way through the optical color coding and light transmission to realize user authentication. The proposed methodology is named as Optical Color Coding for User Authentication (OCCUA). OCCUA combines optical color coding technology, One-time-password (OTP) [1]-[3] and embedded systems realize a new identity recognition technology for more creativity, safety and convenience.

The rest of this paper is organized as follows. In Section II, the related literatures are reviewed to present an overview of technical analysis. In Section III, the application scenario, system architecture and operations are presented. The realization of the proposed OCCUA and numeric analysis are introduced in Section IV. We conclude this work in Section V.

II. Literature Discussion and Technical Analysis

A. User Authentication Technology

Fang Jing-Li has proposed [4], user authentication is an important part of information security. Bakar and Z. Zhang [5], [6] also proposed that user authentication allow users or systems that require access to prove their identities. Authentication requires supporting information to make sure that the information provided by users is in compliance with validation specifications. The methodology of user authentication is based on one of the following three elements: (1) What you know: refers to the things users know, such as the user account/password and the user pre-set questions. This is the most common deployed in almost all information systems. (2) What you have: means that the user owns and is unique as a voucher or the mobile phone number such as the ID number. (3) What you are: intended to verify the user inherent biological characteristics, such as fingerprints, iris, sound and palm lines. These methods are with various costs and security levels.

B. CIE 1931 Color Space

The CIE color space is an international color standard proposed by the International Commission on Illumination in 1931 [7]. Fig. 1 illustrates the CIE color space. The outer curved boundary is called the spectral locus [8], with wavelengths presented in nanometers. The spectral locus includes all the light wavelengths in this study. The spectrum consists of continuous light, belongs to the analogy system. So it cannot be accessed by digital systems. Based on this factor, this study converts the color of light into RGB color model through CIE coordinates. The benefit of converting to RGB color model is to provide coding possibilities for embedded systems.

C. One-Time Password Technology

All the user authentication technologies have the problem of certificate outflow. The reason of certificate outflow may be lost or stolen. If the user authentication system does not delete the outflow credential permissions, that will be at risk of being compromised. Importing one-time password technologies can improve this issue. Because the password is not fixed, it will be changed at ever authentication success. Even hackers use phishing or keyboard skimming to steal

Manuscript received May 19, 2018; revised August 17, 2018. This work was supported in part by the National Science Council, Taiwan (ROC), for financial support under the grants MOST 105-2221-E-151-034-MY2 and MOST 107-2622-8-151-001-TE2.

Chia-Fu Su, Jui-Chieh Kao, Chin-Shiu Shieh, and Mong-Fong Horng are with the Department of Electronic Engineering, National Kaohsiung University Science and Technology, Kaohsiung 80778, Taiwan (e-mail: sufu1122@gmail.com, 1102105204@gm.kuas.edu.tw, csshieh@ieee.org, mfhorng@ieee.org).

Jui-Fang Chang is with the Department of International Business, National Kaohsiung University Science and Technology, Kaohsiung 80778, Taiwan (e-mail: rose@kuas.edu.tw).

DOI: 10.7763/IJCTE.2018.V10.1213

information. Nor will it be used for the next authentication [9].

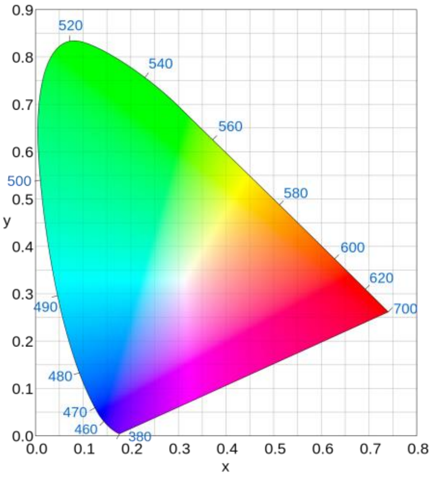

Fig. 1. CIE color space.

III. An Optical Color Coding for User Authentication

A. Application Scenarios

The application scenario of the proposed approach is illustrated in Fig. 2. When user intends to authenticate with his credentials, a color code is generated from CIE color space by user key to transmit to the lock for authentication. The light bulb and the cylinder in the figure represent OCCUA's optical communication transmitter module and receiver module. The certificate and user authentication in this system named Palette key and Palette Lock. Each Palette Key and Palette Lock has its own ID. The purpose is to distinguish each other by ID. Palette Key and Palette Lock also have the memory of ID. As a result, multiple palette keys can be integrated as illustrated in Fig. 2. User only needs a Palette Key can be authenticated multiple Palette Locks. This will effectively enhance the user convenience.

Fig. 3 illustrates the OCCUA communication process. The first step is that Palette Key and Palette Lock will exchange IDs to confirm both sides have the identity record. The above step is to exclude other strange Palette Keys. The second step is to send a password from Palette Key to Palette Lock for authentication. Finally, when the authentication is successful, Palette Lock will feedback a new password to Palette Key to complete communication process.

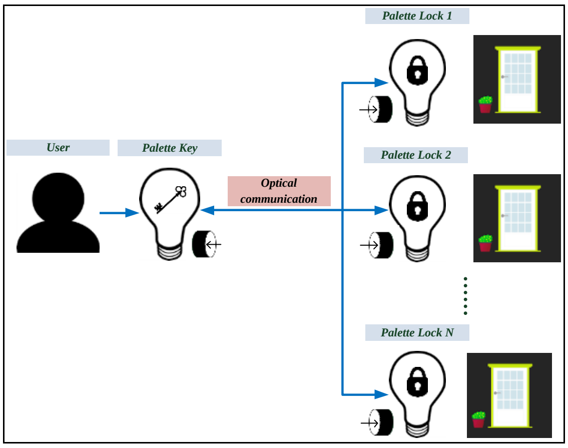

Fig. 2. Application scenarios.

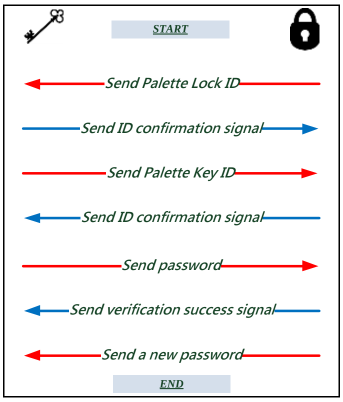
START
Send Palette Lock ID
Send ID confirmation signal
Send Palette Key ID
Send ID confirmation signal
Send password
Send verification success signal
Send a new password
END

Fig. 3. Communication process of OCCUA.

B. System Architecture

Fig. 4 is the system architecture of this study. The system architecture of Palette Key and Palette Lock are composed of the main controller, optical communication transmitter module (OCTM), optical communication receiver module (OCRM), memory module and power module. The content of their work is illustrated as follows. First of all, the main controller is responsible for the entire system operation, including the read/write operation of all modules, memory, coding, decoding and logic control. OCTM is responsible for sending the light code. OCRM is to convert the received optical signals into authentication data. Memory module stores key/lock ID and password information. The power module, responsible for the supply of electricity to ensure that all hardware has enough energy to operate.

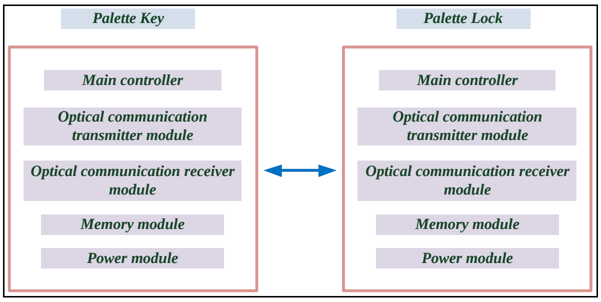
Palette Key
Main controller
Optical communication transmitter module
Optical communication receiver module
Memory module
Power module
Palette Lock
Main controller
Optical communication transmitter module
Optical communication receiver module
Memory module
Power module

Fig. 4. System architecture.

C. Operations of OCCUA

This paragraph will be divided into two parts, Palette Key process and Palette Lock process, to illustrate the systematic operation of this study. Fig. 5 illustrates the operations of Palette Key in six steps. Step 1 is to place the Palette Key in the data exchange area by the user. Palette Key is ready to start the following communication procedures. Step 2, Palette Key will receive the ID from Palette Lock. And follow the step 3, Palette Key will search memory for the corresponding ID. If the ID has not been found, it means that both parties are un-paired devices. System will end the authentication. Conversely, if the ID is found, it means that the devices are paired with each other. System will continue the next step. Palette Key will send own ID to Palette Lock in step 4. Step 5, Palette Key will in accordance with Palette Lock ID to find the corresponding password in memory and send it to Palette Lock. Finally, Palette Key will receive the new password from Palette Lock to ensure the password is synchronized.

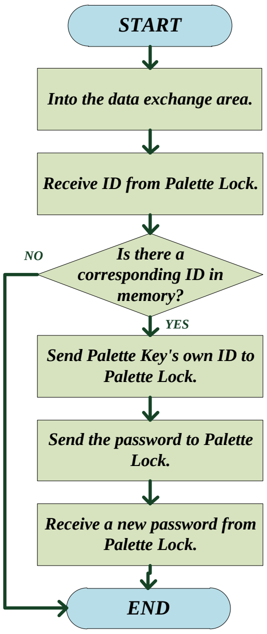
START
Into the data exchange area.
Receive ID from Palette Lock.
Is there a corresponding ID in memory?
NO
YES
Send Palette Key's own ID to Palette Lock.
Send the password to Palette Lock.
Receive a new password from Palette Lock.
END

Fig. 5. Operation of palette key.

The following paragraphs describe the operation of Palette Lock. As illustrated in Fig. 6, there are nine steps in the operation process. Step 1 is Palette Lock detects the palette key into the data exchange area. Palette Lock will ready to start the following communication procedures. Steps 2 and 3 are procedures for exchanging ID by both devices. Step 4 is based on the ID to confirm whether the two sides are paired devices. If the Palette Key ID cannot found in Palette Lock's memory. It means both are un-paired devices and authentication will end. Conversely, if ID is found, it represent that both are paired device. In step 5, Palette Lock will receive the password from the Palette Key to authenticate. If the password is wrong, it means the authentication fails. On the contrary, if the password is correct, the user authentication is successful. Palette Lock will generate a new set of passwords in steps 7 and 8, which will then be sent to the Palette Key to synchronize the password. Finally, system according to the application to perform the actions such as opening the door.

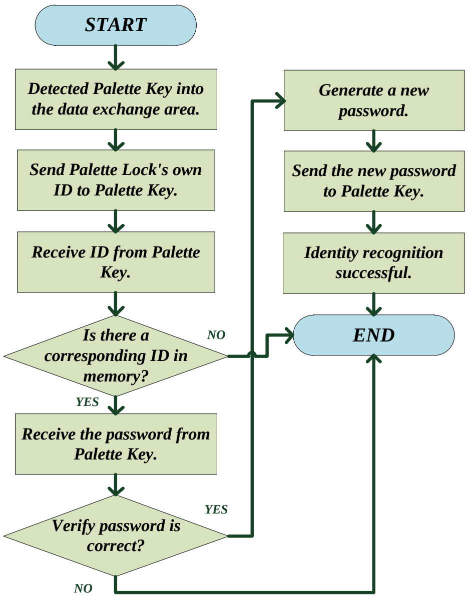
START
Detected Palette Key into the data exchange area.
Send Palette Lock's own ID to Palette Key.
Receive ID from Palette Key.
Is there a corresponding ID in memory?
NO
YES
Receive the password from Palette Key.
Verify password is correct?
YES
NO
Generate a new password.
Send the new password to Palette Key.
Identity recognition successful.
END

Fig. 6. Operation of palette lock.

IV. Analysis and Comparison of Experimental Results

A. Experimental Analysis

The results of experiments in this study demonstrated that OCCUA is applicable in practical applications. Fig. 7 is the photo of the Palette Key. The main controller is developed on Arduino Nano. Its advantages are small size and meet the hardware needs. In addition, we use a RGB LED as optical communication transmitter module. It meets our needs with the ability to transmit light of different colors. And we use the TCS3414CS color sensor as the optical communication receiver module. It can finish the task of optical communication receiving and decoding.

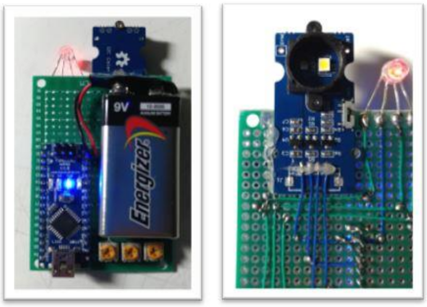

Fig. 7. Palette key actual picture.

A prototype of Palette Key and Palette Lock is illustrated in Fig. 8. The optical communication transmitters and optical communication receivers of both devices will cross-correspond, to achieve the purpose of optical communications. A user authentication system is presented at the bottom of Fig. 8. If the user authentication is successful, the door will be open.

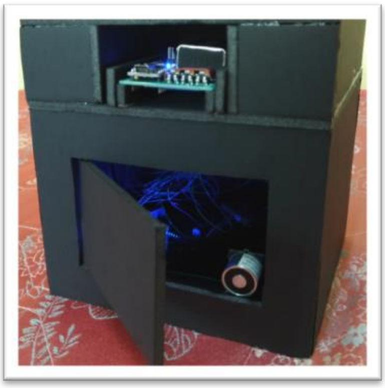

Fig. 8. The actual picture of the application scenario.

After the experiment we found that the sensitivity of optical communications device greatly affects the security of OCCUA. Intensity resolution and color resolution are two indicators that affect sensitivity. Intensity resolution is defined as the same color of light can be resolved into how many copies. Fig. 9 illustrates the relationship between Intensity resolution and password strength. It can be found high intensity resolution that the probability of successful by brute-force attack will be lower. In addition, the other indicator is color resolution, it be defined as how many colors of light can be resolved. Fig. 10 illustrates the relationship between color resolution and password strength. At the same 4-bits resolution, a high color resolution represents the lower the probability of successful by brute-force attack. The number of color in Fig. 10 can be corresponded to number of point in CIE color space. The relationship between these two indicators and the crack probability, as in

$$P = \frac{1}{2^{R*C}} \tag{1}$$

where P is the crack probability of system, R and C represent the intensity resolution and color resolution, respectively.

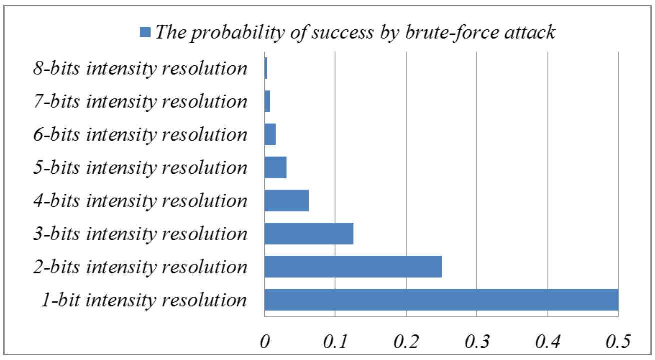

Fig. 9. Relationship between intensity resolution and password strength.

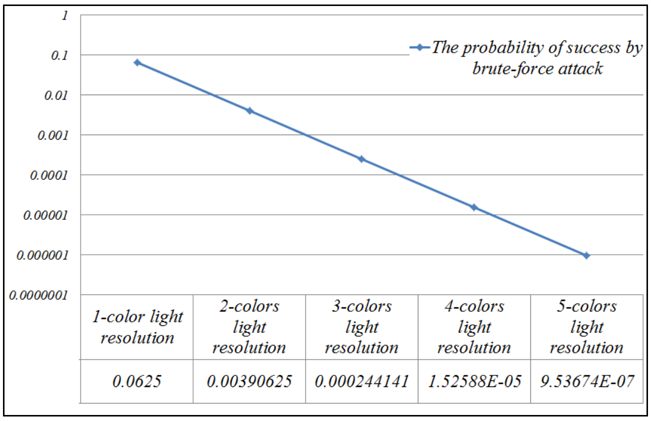

Fig. 10. Relationship between color resolution and password strength.

If a lower sensitivity of the optical communications device will lead to lower password strength. Then the weak password strength causes security crisis. In this case, developers can transmit more light at one time to reduce the crack probability greatly as given

$$P = \frac{1}{2^{R*C}} * \frac{1}{2^{R*C}} * \dots * \frac{1}{2^{R*C}} \tag{2}$$

However, this also means that the user must spend more time to wait for the authentication process. How to adjust the appropriate authentication time is worth to discuss.

B. Compared with Other Technologies

Iris authentication, fingerprint authentication and OCCUA demonstrated their security capabilities in this section. Until 2017, there are 7.5 billion people worldwide. We suppose that each people have different two eyes and ten fingers. According to this, the crack probability of each authentication is illustrated in Fig. 11. OCCUA with 8-bits of intensity resolution and 5-color resolution has lower crack probability than other user authentication. This means that OCCUA have the potential to achieve a more security than existing technologies.

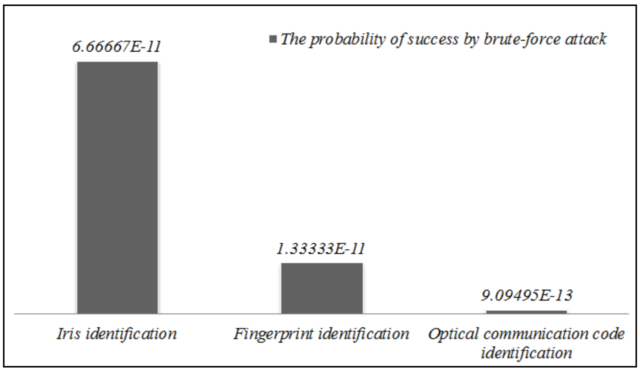

Fig. 11. OCCUA compared with other user authentication technology.

V. Conclusion

In this paper, a new user authentication approach called as OCCUA is presented. The OCCUA combined the optical coding and one-time password to achieve more security. Through the experiment in embedded system, prove OCCUA is feasible and efficiently. And experiment also illustrated the OCCUA can through increase intensity resolution and color resolution to reduce crack probability. Finally, analytical results presented that the OCCUA with 8-bits of intensity resolution and 5-color resolution have lower crack probability than other user authentication. How to adjust the appropriate authentication time is the next issue to explore.

References

[1] A. Behl and K. Behl, "An analysis of cloud computing security issues," *Information & Communication Technologies*, vol. 15, no. 3, pp 109-114, 2013.

[2] Cloud Security Alliance. (2010). Domain 12: Guidance for identity & access management. [Online]. Available: https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

[3] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security & Privacy*, vol. 7, no. 4, pp. 61-64, July-August 2009.

[4] J. L. Fang, "An adaptive user authentication based on context awareness with Bayesian Theorem," Master thesis, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan, 2016.

[5] K. A. A. Bakar and G. R. Haron, "Adaptive authentication based on analysis of user behavior," in *Proc. Science and Information Conference*, 2014, pp. 27-29.

[6] Z. Zhang, C. Wu, and D. W. Cheung, "A survey on cloud interoperability: Taxonomies, standards, and practice," *ACM Sigmetrics Performance Evaluation Review*, vol. 40, no. 4, pp. 13-22, 2013.

[7] Y. Chien and M. J. Shyu, "A usability study on CIELAB based 2D and 3D color picker interface," Mater thesis, Chinese Culture University, 2011.

[8] P. R. Boyce, *Human Factors in Lighting*, 3rd ed. CRC press, pp. 14-15, 1981.

[9] B. J. Yang, "Study on user authentication based on one-time password," Mater thesis, Chao-Yang University of Technology, 2016.

Chia-Fu Su received the bachelor degree in the Department of Electronic Engineering from National Kaohsiung University Science and Technology, Kaohsiung, Taiwan, in 2016. Currently, he is a master student in the Department of Electronic Engineering, National Kaohsiung University Science and Technology. His research areas focus on signal processing and image processing.

Jui-Chieh Kao received the bachelor degree in the Department of Electronic Engineering from National Kaohsiung University Science and Technology, Kaohsiung, Taiwan, in 2017. Currently, he is a master student in the Department of Electronic Engineering, National Kaohsiung University Science and Technology. His research areas focus on embedded system.

Chin-Shiuh Shieh received the Ph.D. degree in the Department of Computer Science and Information Engineering from National Sun Yat-sen University, Kaohsiung, Taiwan. Currently, he is a professor in the Department of Electronic Engineering, National Kaohsiung University Science and Technology. His research areas focus on AI and computer networks.

Jui-Fang Chang received the Ph.D. degree in the Department of Finance from International University, USA. Currently, she is a professor in the Department of International Business, National Kaohsiung University Science and Technology. Her research areas focus on computational intelligence.

Mong-Fong Horng received his bachelor, master and Ph.D. degrees from Control Engineering, National Chiao-Tung University, Hsin-Chu, and the Department of Computer Science and Information Engineering from National Cheng Kung University, Tainan, Taiwan. Currently, he is a professor and department chair with the Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Taiwan. His research areas focus on computational intelligence, computer networks, sensor networks, Internet of Things.