**ISBN** 978-981-11-0008-6
**Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)**
*Tokyo, Japan, 17-19 June, 2016, pp. 214-219*
doi: 10.18178/wcse.2016.06.034

# Mutual Authentication Based on Visual Cryptography and OCR for Secure IoT Service

Dana Yang[+], Inshil Doh and Kijoon Chae

Ewha Womans University, Seoul, Korea

**Abstract.** Recently, various devices providing many services to users have appeared in IoT (Internet of Things). For these services, users as well as devices have to obtain authentication from server system, and they need to authenticate server system, too. In this work, we suggest a mutual authentication between device and server based on visual cryptography. Visual cryptography depends on human eyesight, and it is very simple because no calculation is required for encryption or decryption of the information. We also adopt OCR (Optical Character Recognition) to recognize the information for authentication. OCR plays the role of humans and reads the overlapped images. For evaluation of our proposal, we simulated the authentication mechanism using RaspberryPI II.

**Keywords:** IoT, mutual authentication, visual cryptography, OCR.

## 1. Introduction

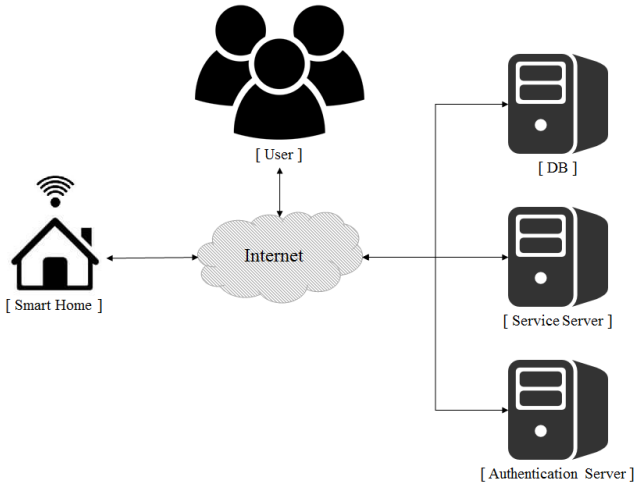


Fig. 1: Simple infrastructure in IoT.

In "Internet of Things" (loT), the requirement of the communication with devices and concerns, such as, the optimization of the human environment, the management of security, the improvement of living quality, and the effective management of production, has become explosive growth [1]. According to this demand, the field of security is very important, especially for authentication [2]. For example, a smart boiler at smart home, such as infrastructure of Fig. 1 [3], supports remote control service basically that can be on or off power and control temperature for an outside owner. In this case, before the owner is provided by this service in service server, the owner as well as smart boiler must obtain authentication from authentication server because that has to certify real server and device to the owner nor phishing server and counterfeit

[+] Corresponding author. Tel.: + 02-3277-3506.
*E-mail address*: yangzzzzz@ewhain.net.

device for attacker. So we suggest simple authentication system for IoT device using visual cryptography not to calculate some encrypted and decrypted mathematics, also to assure confidentiality. Actually it is implemented to make more than two images including a code (authentication number, message etc) and to overlap the images, then to confirm the code through eyesight, because it is dependent only on vision of human to decrypt the code. For this reason, this originally can't apply to machine in IoT, however in order to solve the problem, we used OCR (Optical Character Recognition) that can read authentication code at device like human.

Authentication utilizing images is almost a type of watermarking [4], therefore it can certify only server or information about copyright. But our suggestion is mutual authentication between device and server. As the result through this authentication, device can exactly recognize real server not to be phishing server, also server can realize the real device not to be counterfeit device.

## 2. Related Work

### 2.1. Visual Cryptography [5], [6]

Visual cryptography was proposed by Naor and Shamir in 1994 and a lot of researches have been done so far. It applies higher color contrast of character than background based on gray being half contrast of black. Also it consists of shared images derived from origin image including a message to send to a receiver, but it is lower computational cost to encrypt, decryption algorithm is not required and it is very simple to make the shared images. When you send the message to receiver by using it, you can send by e-mail besides FAX and post. Differently from other cryptographies, decryption of visual cryptography is dependent on only the vision of receiver. In Fig. 2, we can learn the process to make final image by overlapping shared images. Also Fig. 3 shows that each pixel shape in shared images comprised of background and letter is processed to overlap.

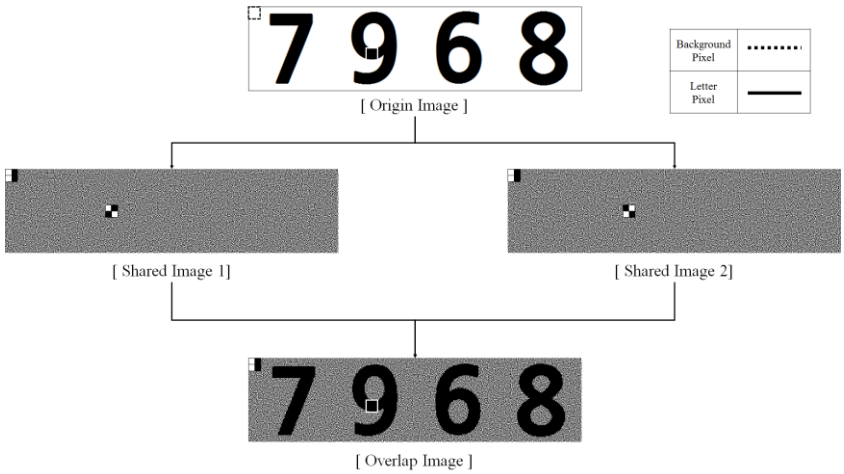


Fig. 2: Process of making and overlapping the shared images using visual cryptography.

| shape no | Background Pixel □ | | | | | Letter Pixel ■ | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Share1 | | Share2 | | overlap | Share1 | | Share2 | | overlap |
| 1 | ▀ | + | ▀ | = | ▀ | ▀ | + | ▄ | = | ■ |
| 2 | ▄ | + | ▄ | = | ▄ | ▄ | + | ▀ | = | ■ |
| 3 | ▌ | + | ▌ | = | ▌ | ▌ | + | ▐ | = | ■ |
| 4 | ▐ | + | ▐ | = | ▐ | ▐ | + | ▌ | = | ■ |
| 5 | ▚ | + | ▚ | = | ▚ | ▚ | + | ▚ | = | ■ |
| 6 | ▞ | + | ▞ | = | ▞ | ▞ | + | ▞ | = | ■ |

Fig. 3: Method of making the background pixel and letter pixel in visual cryptography.

For example, initially you have to prepare origin images expressing the number “7968” as in Fig. 2. For making shared image 1, it is defined randomly one of pixel patterns of first column in background pixel of Fig. 3 like choosing shape number 4, as represented upper right in ‘Shared Image 1’ of Fig. 1. Then for making a shared image 2, it is decided a background pixel of line set in shape number 4. If you should create one of pixels in “9” of origin image, at random, you must determine a shape of patterns in letter pixel column of Fig 3 as making background pixel. In this case, each shared image has made by shape 5 in letter pixel. When you finally overlap share image 1 and share image 2, you can see gray background and black number “7968” not to be pixel pattern because eyesight of human is low. If shared image 2 is not made to be a bit suitable for shared image 1, you can’t see the number.

## 2.2. OCR [7], [8]

OCR is a technology which converts numbers or characters in an image or hand_writing papers into text type electronic data utilized by document files mainly in public offices such as banks, polices, hospitals, etc. For simple instance, if you want to send an e-mail quickly but only have a printed paper with important information, you can translate the printed information into a type of text in document by executing a program utilizing OCR. There are various programs and algorithms on the online market. “Tesseract” algorithm made by google is the most famous one. It provides high recognition rate on image composed of white background and black characters on it.

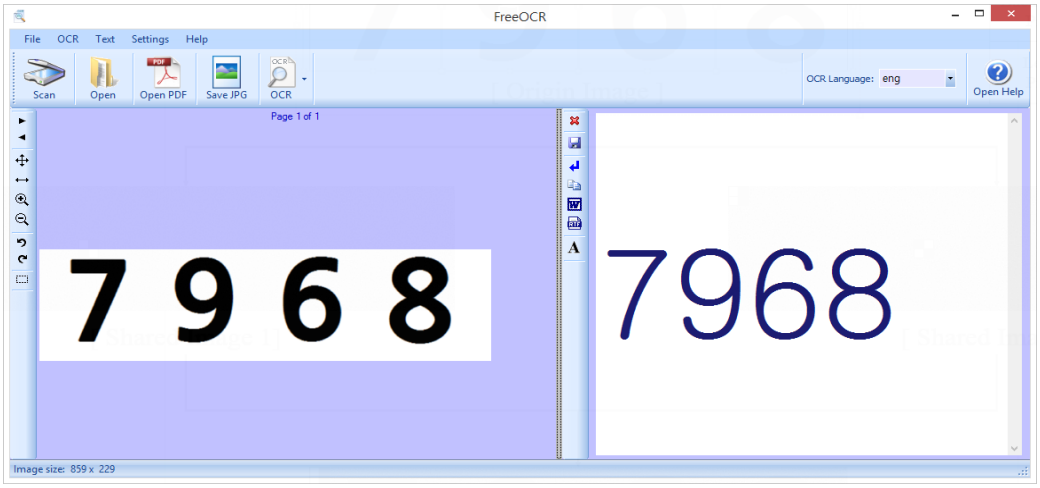


Fig. 4: Result of “FreeOCR” program.

Fig. 4 shows the result of FreeOCR to get numbers. FreeOCR adopts Tesseract algorithm. The left part in Fig. 3 is the image including number “7968” and the right part shows the result after applying the FreeOCR to get the numbers from the image in text representing “7968”. Because OCR can read the images and turn the image type information into text type data, we have adopted FreeOCR based on Tesseract algorithm for our proposal to get the advantage of high recognition rate in open sources.

# 3. Mutual Authentication Mechanism for IoT Devices

In this section, we propose a mutual authentication mechanism for IoT devices adopting visual cryptography and OCR. In IoT environment, various devices and server systems need to recognize one another rapidly and dynamically. Fig. 5 shows the process for our proposal.

We assume that a device for IoT and a server receive shared image 1 on visual cryptography from third trust party in safe manner. When the device needs the service, it requests authentication to the server system. On receiving the request, server generates four digit authentication code as in Fig. 4. Based on visual cryptograph, server makes shared image 2 which looks gray because it hides the information in visual cryptography. Now, the server sends shared image 2 to the device and so that the device can overlap two images, shared image 1 which has been delivered at the bootstrap stage and image 2 which has been delivered by the server system. Then the device removes background pattern looking gray so that the

overlapped image represents origin number image clearly. This step is required to decrease the possibility of OCR reading failure. After the background color removal, device extracts text type authentication code composed of 4 digit numbers from overlapped image applying OCR Tesseract. After getting the authentication code in text, the device hashes the result and then sends it back to the server. Server compares hashed result of the authentication code and the value delivered from the device, and decides the authenticity of the device. Based on the result, server sends success or failure message to device.

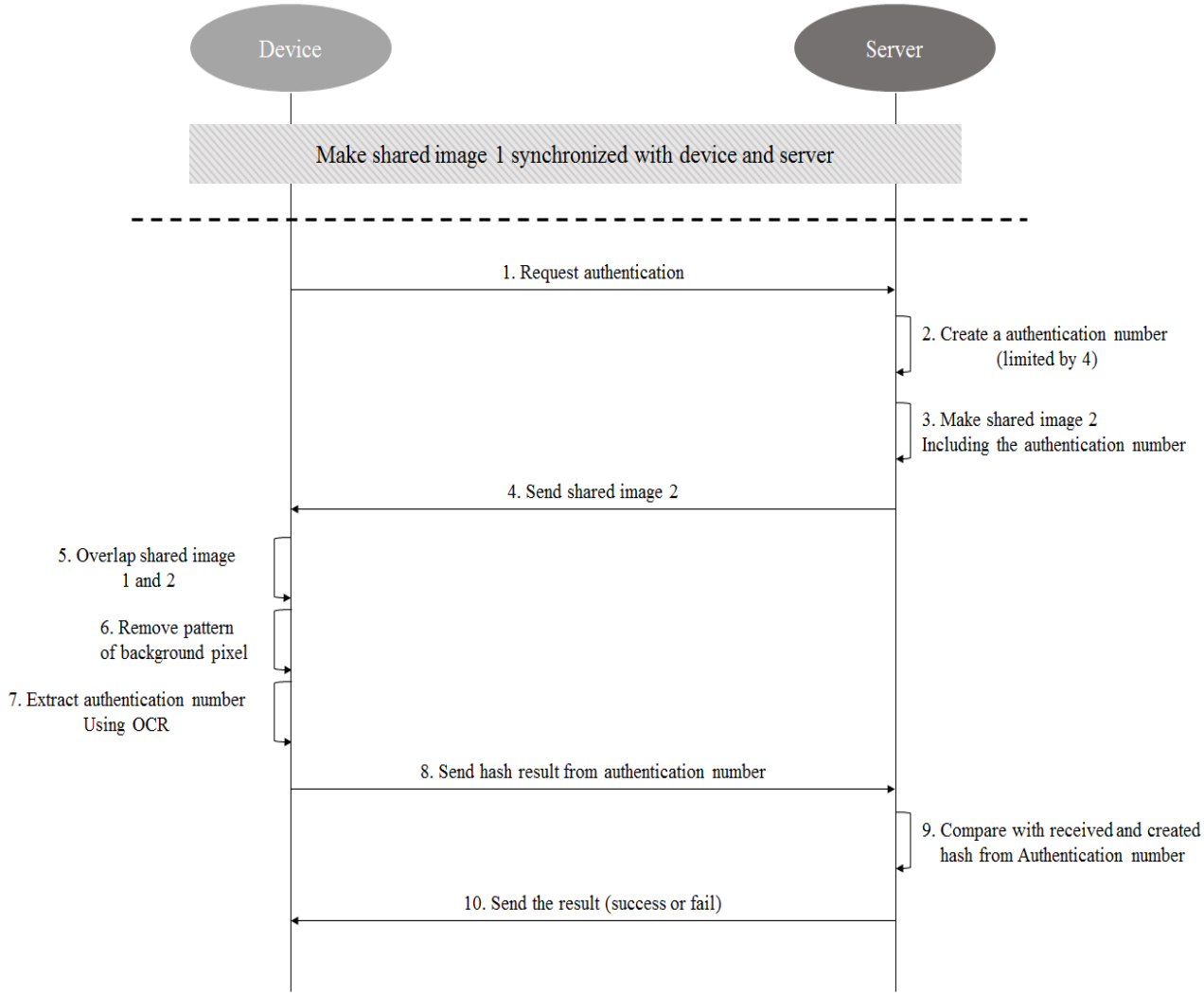


Fig. 5. Sequence diagram for mutual authentication between device and server.

## 4. Implementation and Security Evaluation

In this section, we describe the result of our proposal simulation. We have used Raspberry PI II for the IoT devices and desktop computer as the server system.

### 4.1. Simulation Environment

Table 1 represents simulation environment. We used Raspberry PI II on device part and general desktop on server part, and then developed applications for each entity. We also installed operating systems (OS) for respective systems, RASPBIAN JESSIE on Raspberry PI II for device part and window 7 on general desktop PC for server part. After connected with each device and internet especially using static IP, it has opened 9002 port on server part. We have developed java application suited to each part and we used JDK 7 as socket programming. We also applied classes for generating random numbers and creating images as in <Table 1>.

Table 1. Environment for Simulation

| Part | Device | Server |
|---|---|---|
| | Application | Application |
| **Device type** | Raspberry PI II | General Desktop |
| **OS** | RASPBIAN JESSIE | Window 7 |
| **IP** | ~ | 203.xxx.xxx.69 |
| **Port** | ~ | 9002 |
| **Program** | JDK 7 | JDK 7 |
| **Library** | java.io.*<br>java.net.*<br>java.awt.*<br>javax.imageio.*<br>java.util.* | java.io.*<br>java.net.*<br>java.awt.*<br>javax.imageio.*<br>java.util.* |

### 4.2. Security Evaluation

On lower computation of visual cryptography for encryption, we can know that it is appropriate to authenticate each machines in dynamic and rapidly changing IoT environment. So we have considered during communication with device and server whether an attacker can see authentication number from shared image 2, and what happen if other attacker send different shared image to targeted device. The first case is that the attacker never can see and know authentication number from shared image 2 made on real server in the reason of viewing just gray image because it is consisted of random pixel pattern. In the another case, although the device receives shared image 2 from attacker to be similar with making by real server, there is a reason that it can't see the number even if pattern of share image 2 derived from shared image 1 is a little different. Therefore our suggestion can prove trustable and mutual authentication between a device of IoT and server. Additionally we found abbreviated process time making share image 2 having the size of 1718 x 458 px.

## 5. Conclusion

In this work, we have suggested mutual authentication mechanism between device and server for IoT service applying visual cryptograph and OCR. We also simulated our proposal using Raspberry PI II and desktop computer similarly with IoT environment. The mechanism has substantial adaptability because it does not require heavier computation or longer process time by applying visual cryptography than general algorithm of authentication. At the result, our proposal prevents man in the middle attack and provides secure authentication between server and the device. Proposed mechanism can be applied for various IoT authentication including future human and intelligent robot interaction for institution like corporation, school.

## 6. Acknowledgements

The work is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2011788).

## 7. References

[1] Miao Yun, Bu Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, 2010 International Conference on Advances in Energy Engineering, pp. 69 – 72, 2010

[2] Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmadjid Bouabdallah, A Systemic Approach for IoT Security, 2013 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 351 – 355, 2013

[3] Yihe LIU, Yao LI , Construction and Strategies in IoT Security System, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, pp. 1129 – 1132, 2013

[4] Ping Wah Wong, Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, IEEE Transactions on Image Processing (Volume:10 , Issue: 10 ) , pp. 1593 – 1601, 2002

[5] M. Naor and A. Shamir, Visual Cryptography, Advances in Cryptology EUROCRYPT94 LNCS, Vol. 950, pp. 1-12, 1995

[6] Jiyoung An, Jaeyeon Lee, Aeyoung Kim, Sang-Ho Lee, User Authentication Scheme for Mobile Banking using Visual Cryptography, Korea Computer Congress , 2013

[7] R. Smith, An Overview of the Tesseract OCR Engine, ICDAR, pp. 629-633, 2007.

[8] Zohra Saidane and Christophe Garcia, Robust Binarization for Video Text Recognition, ICDAR 2007. Ninth International Conference, Volume 2, pp. 874 - 879, 2007.