International Journal of Technology and Engineering Studies
volume 5 issue 4 pp. 113-120 doi: https://dx.doi.org/10.20469/ijtes.5.10002-4

Improvement of Shoulder-Surfing Resistant Authentication Method Using Hybrid Images

Yutaka Hirakawa *
Department of Computer Science & Engneering,
Shibaura Institute of Technology,
Tokyo, Japan

Kai Motojima
Department of Computer Science & Engneering,
Shibaura Institute of Technology,
Tokyo, Japan

Abstract: A hybrid image blends the high-frequency component of one image with the low-frequency component of a different image. The high-frequency component is easily recognized from a short distance, but difficult to recognize from a long distance. On the other hand, the low-frequency component is easy to recognize from a long distance; however, it is difficult to recognize from a short distance. IllusionPIN, an authentication method based on hybrid images, was proposed in 2017. In IllusionPIN, a user and an observer recognize different digits on the same smartphone display. For example, when the user touches the digit 3 derived from high-frequency components, the observer recognizes 7 derived from low-frequency components. Although IllusionPIN is known to resist shoulder surfing, the authentication success rates and operation times of this method have not been reported. The present evaluation of IllusionPIN revealed a major problem: overlap of the digits derived from the high- and low-frequency components degrades the distinguishing ability, thereby reducing the success authentication rate to unacceptably low levels (approximately 77%). To improve the success authentication rate of IllusionPin, we slightly shift the drawing range of one digit. Evaluation results confirmed that after this improvement, the authentication success rate exceeded 90% without disturbing the shoulder-surfing resistance.

Keywords: *Authentication method, hybrid images, success authentication rate, authentication time*

Received: 29 May 2019; ***Accepted:*** 11 July 2019; ***Published:*** 26 August 2019

I. INTRODUCTION

Internet-based services, such as banking, finance, and shopping, are now commonly used worldwide. All of these systems require user authentication, and many types of authentication methods have been proposed [1, 2]. Here, we focus on password-based authentication because it is relatively simple and provides an occasional backup when other methods fail. The most popular of these methods, known as personal identification number-entry (PIN-entry), involves four-digit numerical passwords and has universally been adopted for ATM machines.

The main problem with password authentication is password leakage. The first research objective is to avoid shoulder surfing, the action of peeping over someones shoulder during the authentication operation to steal the operators password.

Passwords can also be stolen in video-recording attacks, in which a password is deduced from images captured by video cameras. A huge amount of small cameras have entered modern society. Almost everybody has a mobile phone or a smartphone with camera functionality. Moreover, monitoring cameras are installed in every town and every office. If an authentication operation is video-recorded, the candidate passwords are easily narrowed down. In video-recording attacks, a persons authentication operations can also be video-recorded multiple times. This situation is very rare but also extremely dangerous. For example, the authentication operations of the same

*Correspondence concerning this article should be addressed to Yutaka Hirakawa, Department of Computer Science & Engneering Shibaura Institute of Technology Tokyo, Japan . E-mail: hirakawa@shibaura-it.ac.jp

person can be video-recorded on a net-shopping site in the morning and in the afternoon. If authentication operations are video-recorded multiple times, the hacking resistance is greatly reduced.

From a usability viewpoint, the authentication should be adequately successful and completed within a short time. However, conventional authentication methods with strong tolerance need a relatively long operation time. The tradeoff between usability and tolerance is a well-recognized problem in the range of current research approaches.

In 2017, Papadopoulos et al. [3] proposed IllusionPIN , an authentication method based on hybrid images. The discussion in [3] focuses on the human recognition ability of two displayed numbers. IllusionPIN blends a digit described by a high-frequency image with another digit described by a low-frequency image in the same area. The article highlighted the difficulty of recognizing the high-frequency image beyond a distance of 64 cm (25 inches). However, the usability of IllusionPIN was not discussed in [3].

This article discusses IllusionPIN from a usability viewpoint and proposes an improved version with higher success authentication rate than the original version.

II. RELATED WORK

A. *Authentication Method with Shoulder-Surfing Tolerance*

Tolerance against shoulder surfing is discussed in Roth et al. [4] and Zhao et al. [5]. Fig. 1 shows the interface of a tolerant shoulder-surfing method [4]. Each number on the authentication interface is set against a black or white background. A user selects the background colors of his or her password in the display. For example, if the first digit in the password is 3, the user selects the background color of 3 on the interface. In Fig. 1, the background colors are (from left) white, black, white, and black. The selection is performed four times for each password entry. Although this method resists shoulder surfing, each four-digit password requires 16 selection operations, which is time-consuming for the user. Moreover, if the operation is video-recorded, the password is easily leaked.

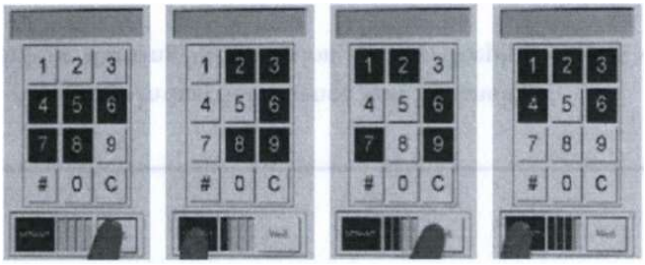

Fig. 1. Authentication interface

B. *Authentication Method with Tolerance to Video-Recording Attacks on at most Two Video-Recordings*

In this subsection, a tolerant authentication method satisfies the following criterion:

- At least 10000 candidates are rested after analyzing the recorded authentication operations.

Initially, these methods have huge password spaces. For example, in the method of [6], each pass-text consists of 50 kinds of characters, including alphabets, digits, and some symbols. On this interface (see Fig. 2), an operator moves the appropriate background color to his or her password position for correct authentication. The details are given in [6].

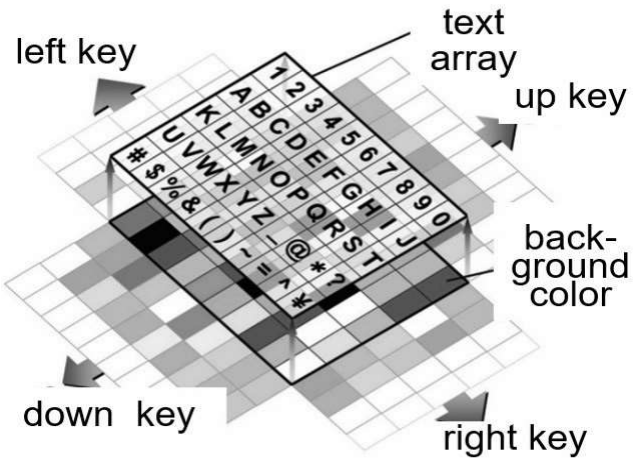

Fig. 2. Authentication interface in the method of Sakurai [6]

As this method uses an 8-length password, the number of password candidates exceeds 1012. When operations are video-recorded at most twice, data analysis in conventional methods [6, 7, 8] obtains over 10000 password candidates. However, the methods are unreliable when authentication operations are video-recorded more than three times, as shown in Fig. 3 [6].

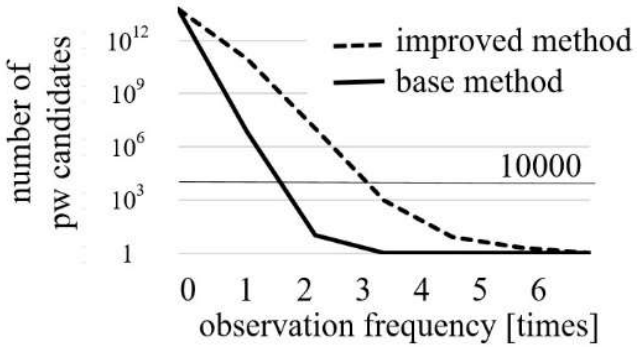

Fig. 3. Evaluation results [6]

C. *Authentication Method with Tolerance To Multiple Video-recording Attacks*

This subsection discusses the tolerance when authentication operations are video-recorded more than three times. Under this condition, there must be no useful information by which attackers can narrow down the password candidates, even when the authentication operations are video-recorded and analyzed.

Tolerance, in this scenario, can be realized by a challenge and response technique. For example, where the pass-text should be placed is regarded as a challenge. The users operationmoving the pass-text to the position designated by the challengedepends on the received challenge.

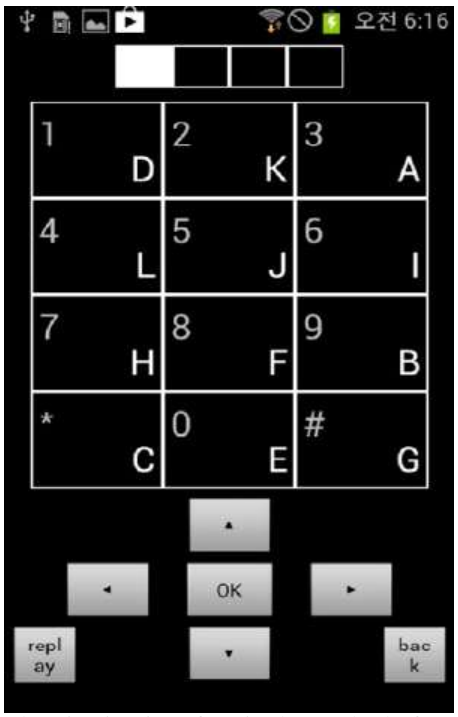

Fig. 4. Authentication interface in the method of [9]

Fig. 4 is an example of the authentication interface in [9]. This interface is a numeric keypad displaying the digits in normal order. Each digit is associated with an alphabetical symbol. The alphabet is displayed as a background, which can be moved by pushing one of the four arrow buttons at the bottom of the keypad. The top of the keypad features an indicator which shows the authentication of the password entry in the case shown in Fig. 1. In this method, an alphabetical letter is vocalized as a challenge. If the first password is *2* and *F* is vocalized, then the correct operation is a move of *F* to the position of *2*. Therefore, the suitable authentication operations are pushing the upward move button twice.

Currently, a challenge is secretly transmitted to an operator by two main approaches: vibrations [10, 11, 12], or through sound or voices [8, 9, 13, 14].

The vibration approach [10, 11, 13] requires over 20 seconds for four-digit password authentication.

The sound or voice approach [10, 11, 12] reduces the time of four-digit password authentication to approximately 15 seconds. Lee et al. [9] described three voice-based authentication methods, only one of which is tolerant to multiple video-recording attacks [12].

Both approaches achieve an adequate correct authentication rate but consume a rather long operation time. More convenient methods are desired.

D. *Authentication Method using Hybrid Images*

Authentication methods based on hybrid images have also been reported [15, 16]. A hybrid image blends an image described by high-frequency components with a different image described by low-frequency components. For example, Fig. 5 merges the high-frequency components of a car image and the low-frequency components of a cat image. The car drawing derived from the high-frequency image is easily recognized from a short distance but it is hard to recognize from a long distance. On the other hand, the cat drawing derived from the low-frequency image is easily recognized from a long distance but it is difficult to recognize from a short distance.

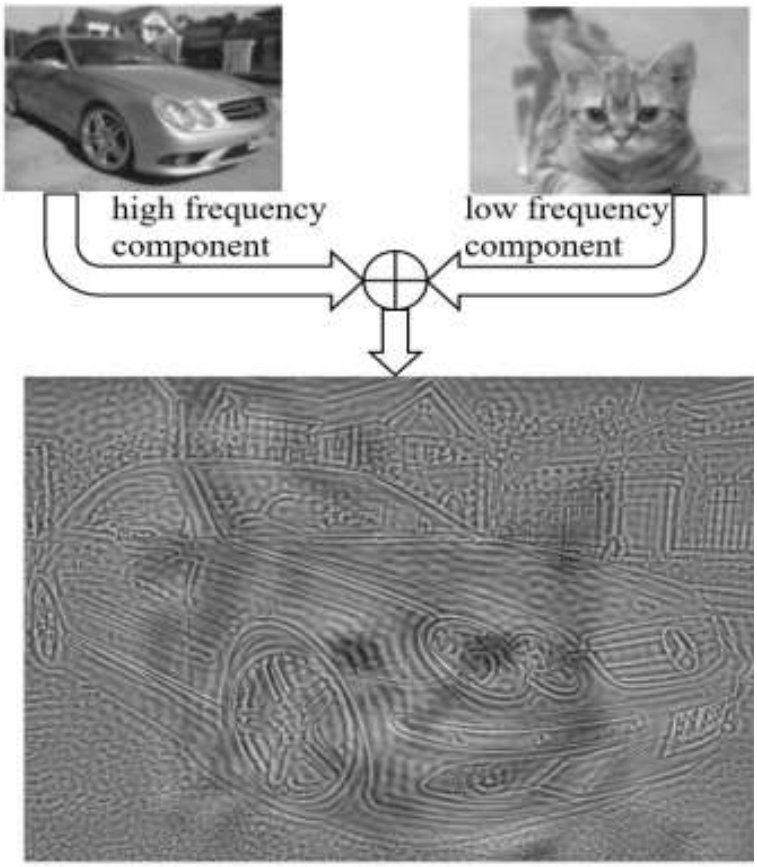

Fig. 5. Hybrid images

IllusionPIN [3] exploits this phenomenon in password authentication. In IllusionPIN, a user and an observer recognize different digits on the same smartphone. When the user touches *3* extracted from the high-frequency components, the observer recognizes *7* extracted from the low-frequency components.

If a digit drawn from the high-frequency components is recognizable by the observer, the password is easily leaked. In the IllusionPIN method [3], the observer reportedly cannot recognize the high-frequency digits from distances exceeding 64 cm (25 inches). However, the success rates and operation times of hybrid image-based authentication have not been reported.

III. PRELIMINARY EXPERIMENT

This section describes the outline and results of a reproduction experiment. Fig. 6 is a hybrid image of the digits *1* described by low-frequency components and 0 described by high-frequency components.

Fig. 7 shows the interface of the experimental system. On the authentication interface, the low-frequency numbers are displayed in their normal order, but the high-frequency numbers are displayed in random order. For example, suppose that the password is *0*, and the authentication interface presents the hybrid image in Fig. 6. When the operator touches the *1* key, this action is recognized by the observer, and the password is not leaked.

The authentication operation of IllusionPIN consists of the following steps:

1. Recognition of the digits extracted from high-frequency images.
2. Touching the password digit.

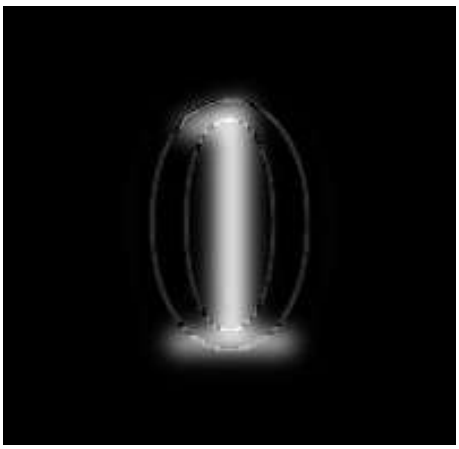

Fig. 6. A hybrid image

As the authentication action is very simple, IllusionPIN can be highly usable if the digits are correctly recognized within a short time.

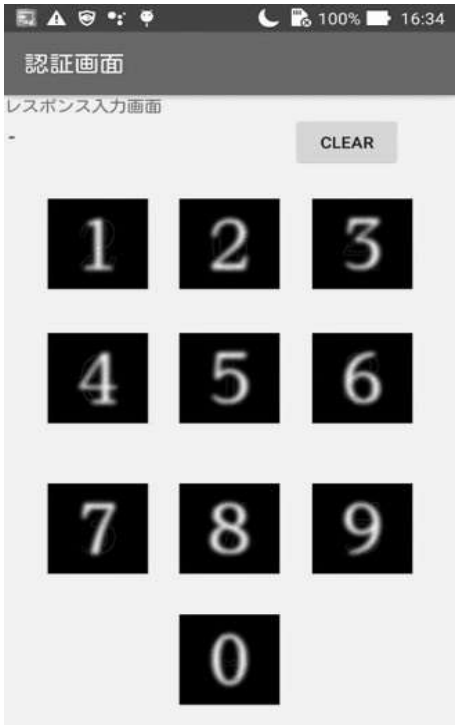

Fig. 7. Authentication interface

The experiment was performed using a Zenpfone 2 Laser, and the hybrid images were created using ImageJ software [17].

Authentication on the hybrid interface was performed by five college students whose age is between 20 and 22. The interface was viewed on a smartphone held at 30 cm from the eyes. Each student performed 20 operations on a one-digit password that was randomly selected before each operation. The average authentication success rate was 77.5%.

This low success rate must be improved in real applications. The average operation time of authenticating one digit was too long (11.2 seconds), but may shorten after adequate learning. In this preliminary experiment, an adequate learning period for the subjects was not considered.

The following suggestion for improvement was made by several of the experimental volunteers:

- As the low-frequency and high-frequency numbers are described in the same drawing area, the high-frequency number is sometimes very hard to distinguish.

IV. TOWARD AN IMPROVED ILLUSIONPIN METHOD

Inspired by the subjects comments, the following variations of IllusionPIN were considered and evaluated:

- The drawing area of the high-frequency number was slightly shifted, as shown in Fig. 8. This shift was expected to increase authentication success rates.
- A background pattern was introduced to the drawing area (e.g., Fig. 9). This pattern was expected to decrease the recognition rate of the observers.

Fig. 8. Hybrid image with a shift in the drawing area of the high-frequency component

Fig. 9. Hybrid image with a background pattern

The evaluations compared the performances of the following four methods:

1. Conventional IllusionPIN
2. IllusionPIN with a drawing-area shift
3. IllusionPIN with a background pattern
4. IllusionPIN with a background pattern and a drawing-area shift

V. EVALUATIONS

A. *Drawing-area Shift and Background Pattern*

Seven volunteers participated in this experiment. Each volunteer operated 20 authentications of randomly designated one-digit passwords. The experimental results are shown in Table 1.

TABLE 1
OPERATION TIME AND SUCCESS RATE (ONE DIGIT)

Method	Op. Time	Success Rate
IllusionPIN	11.2 sec	77.5%
+Area shift	4.6sec	97.1%
+Background pattern	9.2sec	59.3%
+Area Shift and Background pattern	7.7 sec	92.1%

As indicated in Table 1, the area shift effectively improved the authentication success rate while decreasing the operation time. The simultaneous area shift and background pattern were also effective.

B. *Password Leak Rates*

This subsection measures the password leak rate. The operator viewed his or her smartphone from a distance of 30 cm from the eyes, with the display arranged perpendicular to the operators eye line. Meanwhile, the observer viewed the same display from a 40, 50, and 60 cm distance at an angle of 30deg to his or her eye line. This situation mimics a person sitting on a train and peeping at the smartphone display of a person sitting one seat ahead. This is the same threat model used in [3].

Resultant leak rates are shown in Table 2, wherein there are descriptions of 0% that includes random response and no response owing to the recognition difficulty.

TABLE 2
PASSWORD LEAK RATE (ONE DIGIT)

Method	Leak Rate (40cm)	Leak Rate (50cm)	Leak Rate (60cm)
IllusionPIN	16.7%	0%	0%
+Area shift	21.4	18.8%	6.3%
+Background pattern	7.1%	6.3%	0%
Area Shift and Background pattern	14.3%	6.3%	0%

From Table 2, each modification renders the method more recognizable from the viewpoint of observers. However, they are still tolerant of more than 70 cm distance.

C. *Evaluation of Four-digit Password Authentication*

Five volunteers participated in this experiment. Each volunteer applied the following authentication methods five times in random order:

- IllusionPIN
- IllusionPIN with a drawing-area shift
- IllusionPIN with a background pattern and a drawing-area shift

This evaluation was performed on four-digit passwords, which are used for ATMs worldwide. To determine whether the authentication operation times and success rates are comparable with other authentication methods, the subjects were given an adequate learning time. The results are shown in Table 3.

TABLE 3
EVALUATION RESULTS (FOUR DIGIT)

	IllusionPIN	+Area shift	+Area Shift and Background pattern
Op. Time	18.1 sec	9.0 sec	13.9 sec
Success Rate	76%	92 %	96%

As shown in Table 3, the conventional IllusionPIN method required 18 seconds for authentication, and its success rate was 76%. Shifting the drawing area reduced the authentication time to 9 seconds and improved the authentication success rate to 96%.

VI. DISCUSSION

As shown in Table 2, the digits described by the high- frequency component were not recognizable when viewed from 70 cm distance. Therefore, both the original IllusionPIN and the improved methods were apparently tolerant to shoulder surfing.

In video-recording attacks, images of the display can be captured by a super-high-definition camera, increasing the risk of password leakage. However, the password is considered to be difficult to detect in images recorded by an ordinary mobile phone or a security camera. Therefore, both methods are feasibly tolerant to multiple video-recording attacks.

The results depend on several experimental parameters. For example, the numeral font used in this article differed from that in [3]. Although further detailed researches are required, the improved version of IllusionPIN is promising for real-world applications.

VII. CONCLUSIONS AND FUTURE WORK

IllusionPIN is an authentication method based on hybrid images, obtained by blending an image described by high- frequency components with a different image described by low-frequency components. However, as clarified in evaluations, IllusionPIN is hindered by a low authentication success rate and a rather long operation time.

In IllusionPIN, the drawing areas of the two digits extracted from the high- and low-frequency images are completely overlapped. This article proposes an improved method that slightly shifts the drawing area of the high-frequency digit from that of the low-frequency digit, enabling both digits to be viewed clearly.

In the evaluation, the authentication success rate increased from 76% in the original IllusionPIN to 95% in the improved method, and the operation time was approximately halved. The high authentication rate and short operation time confirm the potential usability of the modified IllusionPIN method.

Before applying the modified IllusionPIN method in real applications, the used fonts and image processing parameters must be further investigated.

In video-recording attacks, a more attentive experiment may be necessary to consider the details. However, such an experiment is not performed in [3], and in this article, it is rested as further work.

REFERENCES

[1] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," *International Journal of u-Service and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13–28, 2009.

[2] F. J. Yang, "The user interface design of an intelligent tutoring system for relational database schema normalization," *International Journal of Technology and Engineering Studies*, vol. 2, no. 3, pp. 70–75, 2016. doi: https://doi.org/10.20469/ijtes.2.40002-3

[3] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon, "IllusionPIN: Shoulder-surfing resistant authentication using hybrid images," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2875–2889, 2017. doi: https://doi.org/10.1109/tifs.2017.2725199

[4] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, Washigton, DC, WA, 2004.

[5] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW-07)*. Ontario, CA, 2007.

[6] S. Sakurai and T. Munaka, "Resistance evaluation of user authentication method using matrix against shoulder surfing," *IPSJ Transaction*, vol. 49, no. 9, pp. 3038–3051, 2008.

[7] Y. Hirakawa, "Random board: Password authentication method with tolerance to video-recording attacks," *International Journal of Innovation, Management and Technology*, vol. 4, no. 5, pp. 455–460, 2013. doi: https://doi.org/10.7763/ijimt.2013.v4.441

[8] Y. Hirakawa, K. Kurihara, and K. Ohzeki, "Borderless interface for user authentication method tolerant against multiple video-recording attacks," in *International Conference on Computer Systems, Electronics and Control (ICCSEC)*, Liaoning, China, 2017.

[9] M.-K. Lee, H. Nam, and D. K. Kim, "Secure bimodal PIN-entry method using audio signals," *Computers & Security*, vol. 56, pp. 140–150, 2016. doi: https://doi.org/10.1016/j.cose.2015.06.006

[10] M. Ishizuka and T. Takada, "CCC: Repeated observation attack resilient PIN authentication system using vibration," *IPSJ Transaction*, vol. 56, no. 9, pp. 1877–1888, 2015.

[11] T. Kuribara, B. Shizuki, and J. Tanaka, "Vibrainput," in *Proceedings of the Extended Abstracts of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, Toronto, CA, 2014.

[12] Y. Hirakawa, , F. Hirose, I. Sasano, and and, "PVRotate: An improved vibration-based user authentication method," *International Journal of Future Computer and Communication*, vol. 8, no. 2, pp. 50–54, 2019. doi: https://doi.org/10.18178/ijfcc.2019.8.2.539

[13] Y. Hirakawa, T. Itoh, and K. Ohzeki, "A new numerical password authentication method," *International Journal of Information Technology and Computer Science*, vol. 12, no. 5, pp. 7–15, 2013.

[14] J. Kondo, M. Hirano, and N. Kamiya, "Rm-001: The strong authentic method by voice navigation and relative value input eventing from peeping attack: Invisible authentication," *FIT Forum*, vol. 10, no. 4, pp. 33–38, 2011.

[15] A. Oliva, A. Torralba, and P. G. Schyns, "Hybrid images," *ACM Transactions on Graphics*, vol. 25, no. 3, pp. 527–532, 2006. doi: https://doi.org/10.1145/1141911.1141919

[16] A. Oliva, "The art of hybrid images: Two for the view of one," *Art & Perception*, vol. 1, no. 1-2, pp. 65–74, 2013. doi: https://doi.org/10.1163/22134913-00002004

[17] ImageJ. Image processing and analysis in java. [Online]. Available: https://bit.ly/2YHY6Kp