Low-effort User Authentication for Kiosk Systems based on Smartphone User's Gripping Hand Geometry

Ruxin Wang
Louisiana State University
Baton Rouge, LA, USA
rwang31@lsu.edu

Kaitlyn Madden
Louisiana State University
Baton Rouge, LA, USA
kmadde5@lsu.edu

Chen Wang
Louisiana State University
Baton Rouge, LA, USA
chenwang1@lsu.edu

ABSTRACT

Smartphones continue to proliferate throughout our daily lives, not only in sheer quantity but also in their ever-growing list of uses. In addition to communication and entertainment, smartphones can also be used as a credit card to make a contactless payment on Kiosk Systems, such as ordering food, printing tickets and self-checkout. When a user holds the phone close to the Kiosk system to present payment credentials, we propose to also verify the user's identity based on a photo of the back of their smartphone gripping hand, which provides a second security layer. Compared to the widely used facial recognition, the proposed approach addresses the recent struggles of identifying faces under masks and the public concerns of potential privacy erosion, racial bias and misuse. We find that the geometry of each individual's hand, when it grips a phone, is identifiable and then design a vision-based approach to extract the gripping hand biometrics. In particular, we develop hand image processing schemes to detect and localize the gripping hand while denoising and normalizing the hand images (e.g., size and color). Furthermore, we develop a Convolutional Neural Network (CNN)-based algorithm to distinguish smartphone users' gripping hand images for authentication. Experiments with 20 participants show that the system achieves 99.5% accuracy for user verification.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; • **Security and privacy** → **Biometrics**; **Multi-factor authentication**.

KEYWORDS

Kiosk, Two-factor Authentication, Gripping Hand Geometry

ACM Reference Format:
Ruxin Wang, Kaitlyn Madden, and Chen Wang. 2022. Low-effort User Authentication for Kiosk Systems based on Smartphone User's Gripping Hand Geometry. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3491101.3519817

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9156-6/22/04…$15.00
https://doi.org/10.1145/3491101.3519817

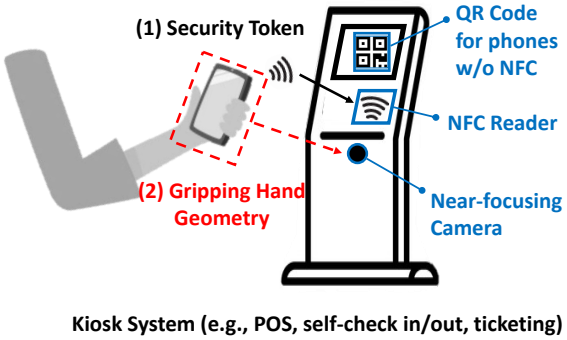

Figure 1: Proposed two-factor authentication.

1 INTRODUCTION

Kiosk Systems have been increasingly deployed in public places for a variety of self-services, including self-checking in/out, auto ticketing, ordering food and making a payment [7, 11, 23]. It not only brings convenience and flexibility but also saves tremendous human labor. In the recent Covid-19 pandemic, self-testing Kiosks enable the virus testing to be contactless, much faster and more widely accessible [12, 15]. It is important to note that these Kiosk services are all identity-dependent, requiring human-kiosk interaction for authentication before service. This work focuses on the secure access of Kiosks, which has not yet received sufficient attention and exploration as other IoT devices (e.g., voice assistants). Since they are broadly deployed in public places to offer identity-based services, they are more prone to be the target of an adversary.

Traditionally, the user needs to enter a password and scan an ID card or a passport into the Kiosk for authentication, which is cumbersome and insecure. Due to pervasive smartphone use, current Kiosk systems support establishing authentications with the user's smartphone within seconds, which is mainly achieved by two contactless technologies respectively, Near Field Communication (NFC) [19] and Quick Response (QR) code [9]. Specifically, the user with an NFC-enabled smartphone can hold the phone close to the Kiosk's contactless reader to exchange authentication tokens via NFC radios. The user can also use the smartphone camera to scan the QR code on the Kiosk's screen to initiate an authentication session and then enter a PIN/password on the phone to complete the authentication. However, these methods only verify users by their phones or passwords but not who they are. Thus, any person getting the device or knowing the password could spoof the user's identity to access Kiosks.

To address identity spoofing issues, some recent Kiosks start to adopt facial recognition technologies for biometric-based authentication [28, 29]. Users only need to show their face to an embedded camera of the Kiosk before requesting Kiosk services, and smartphones are not needed. However, facial recognition is difficult to be used for Kiosks widely due to the following reasons: (1) Face ID is extremely private personal information, and the use of facial recognition in public places may lead to privacy erosion, societal fear, racial bias and power abuse, which has been banned by many states [5]. (2) It is hard to verify users who wear masks, especially during the Covid-19 pandemic; 3) Relying on a single face factor is still not secure enough, given that faces can be forged or synthesized [6].

In this work, we improve the authentication security of current Kiosks for smartphone users by adding a biometric factor. We find that when a user holds a phone, the unique gripping hand geometry is identifiable. Thus, we propose a two-factor authentication system by integrating the traditional tokens (hardware or software) and this new biometric to provide enhanced security. This human-kiosk interaction requires minimal user efforts and is still contactless. As illustrated in Figure 1, when the user normally holds a phone close to the Kiosk to exchange security tokens for authentication (via NFC or QR code), a near-focusing camera of the Kiosk snapshots the back of the gripping hand to extract biometrics for the second authentication factor. To verify the user's gripping hand image, we develop a Convolutional Neural Network (CNN)-based user authentication approach. The approach first processes the obtained hand image with color normalization, hand detection, background removal and scaling. The processed image is fed into our per-user CNN model for verification, which is designed with three convolution layers. Specifically, based on the user identity claimed during the token exchange process, the Kiosk selects the corresponding user's CNN model to verify the presented gripping hand biometric. The user only passes authentication when the security token and the gripping hand biometric are correct simultaneously. Moreover, the Kiosk camera's focal distance can be physically limited (e.g., < 20cm) to avoid capturing people's faces.

Our contributions are summarized as follows:

- We propose a two-factor authentication system for Kiosks to interact with smartphone users, which integrates the traditional security tokens and the novel gripping hand biometric to provide enhanced security without requiring additional user effort.
- We find that the geometry of each individual's hand when it grips a phone is unique. Moreover, it is easy to acquire simultaneously when the user holds a phone to a Kiosk to make a payment or check-in/out.
- We develop a CNN-based algorithm to extract and distinguish people's gripping hand biometric features for authentication. Hand image processing schemes are developed to extract the gripping hand geometry features while normalizing and de-noising the hand image.
- Experiments with 20 participants show that our approach achieves high accuracy of verifying a user by the back of the gripping hand.

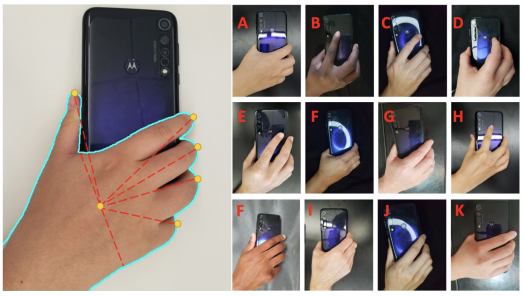

Figure 2: The new gripping hand biometrics.

2 EXTENDING HAND GEOMETRY TO GRIPPING HAND BIOMETRICS

Hand geometry is a well-known biometric used by many practical user authentication methods. In particular, a person's hand geometry can be uniquely described by the handshape features, including the hand contour, the palm width and the finger shapes (e.g., length, width, thickness), and vision sensors are mainly used to capture this biometric [1, 10, 13, 16]. However, the current hand geometry biometric is only limited to the shape of a stretched flat hand, and the user needs to press the hand against a surface for the biometric data collection, which requires active user participation and is not easy to use in many situations.

This work aims to find a new biometric that can be obtained with low user effort and is easy to integrate with current Kiosk authentication. We propose to extend the traditional hand geometry biometric to the shape of the gripping hand and explore the potential of extracting such biometrics using an ordinary camera. The intuition is that when a user grips a device, the shape of the gripping hand resulting from the combination of the device and the individual hand should also be identifiable. More specifically, people tend to adjust their hand pose according to the device dimension/shape to grip it comfortably and tightly. Thus, the gripping hand shape is individually unique and dependent on the specific device. This is a reflection of Anthropometry and is also related to the user's behavioral traits.

To illustrate how different people grip a device, we ask 20 participants to hold the same phone (Motorola G8). Some of their hand images are shown in Figure 2. We find that the shapes of gripping hands are distinctive among all these participants. Such differences can be found in the contours of the gripping hand, the positions and spacing of fingers, knuckle positions, skin colors, tendons, vein patterns, and the distance from each detected finger "tip" to the center of the palm. The geometric relationships between the hand and the handheld device are also unique for each participant. Thus, using a camera to verify a user by the gripping hand is feasible. It is important to note that the gripping hand shapes become even more distinctive if more than one phone models are involved.

3 APPROACH DESIGN

3.1 System Overview

The architecture of the proposed two-factor authentication system is shown in Figure 3. When the user holds a phone close to the Kiosk to initiate the authentication, the system takes both the security token and the image of the gripping hand. It then performs

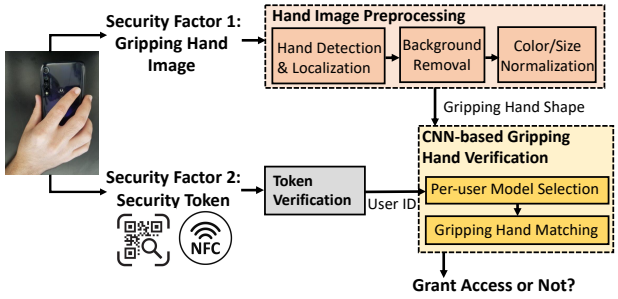

Figure 3: Flow of the proposed two-factor authentication system for Kiosks.

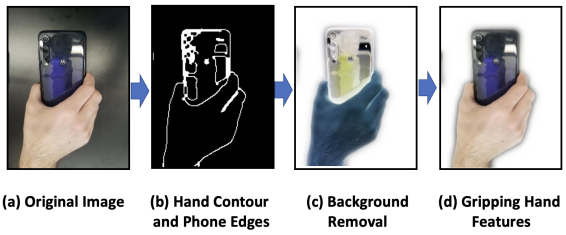

Figure 4: Gripping hand detection and segmentation.

image pre-processing schemes to calibrate the hand image, including normalizing the image colors, detecting and localizing the hand on the image, removing the background pixels and re-scaling the extracted hand. The obtained hand shape is fed into our CNN-based gripping hand verification model, which is trained for each user during the user registration and stored at the server-side. During authentication, the server selects the CNN model based on the user ID claimed by the token to perform profile matching. Only when the security token and the gripping hand biometric are both correct, the authentication is successful, and the access permission is delivered to the Kiosk.

3.2 Hand Image Processing

We develop image processing schemes to extract gripping hand features from the image, including hand detection, background removal and normalization. The resulting color image of the segmented gripping hand contains three major types of hand features: (1) the hand contour, (2) the geometry shape of the hand described by the finger joints, knuckles, valleys, tendons and veins, and (3) the skin color patterns.

Hand Detection & Localization. To capture the gripping hand characteristics, we apply the Canny Edge Detector [4] to find and localize the gripping hand in the image, which includes the contour of the hand and the edges of the gripped phone. Specifically, we use a Gaussian filter to smooth the image, remove the pixel noise, and then search for the intensity gradients of the image. Next, we apply the gradient magnitude thresholding and the lower bound cut-off suppression to eliminate spurious responses to the edge detection algorithm. A double threshold-based method is then used to determine the possible edges of the interested region. At last, we track the detected edges to finalize the hand contour and phone edge detection while suppressing the weak and disconnected edges. To further improve the hand detection result, we perform dilation to widen the boundaries of the hand and the phone with the foreground pixels and then erode the boundaries for a clear hand contour and phone edges, which is further expressed in a mask (binary image) as shown in Figure 4(b).

Segmentation & Background Removal. After hand detection, we continue to remove the background pixels of no interest and keep the foreground regions to highlight the hand and the phone in a clear view. Specifically, we perform the flood fill to the above mask to connect each pixel to its neighbors if their difference to this pixel is zero. Next, we apply a Gaussian filter to smooth the resulting mask and perform dilation and erosion to highlight the hand-phone area. Then this mask is used to generate a 3-channel alpha mask to describe the degree of transparency of R, G, B values to determine how a pixel is rendered when they are blended. We then blend the alpha mask with the original image to segment the hand-phone area from the background as illustrated in Figure 4(c). At last, we restore the original colors for only the detected hand and phone, while the background is removed as shown in Figure 4(d).

Color/Size Normalization. We perform both size and color normalization to the hand images to reduce the impacts from different hand-camera distances and light conditions. Specifically, we normalize the size of the hand using a fixed size circle and resale it into a 200p ×150p image. Furthermore, we use a Grey World algorithm to normalize the image color and cope with different illuminations.

3.3 CNN-based Gripping Hand Verification

We develop a CNN-based algorithm to analyze the biometric features presented by the gripping hand image. The algorithm is designed as a binary CNN classifier and is respectively trained for each user, where the user's gripping hands and a nonuser data set are used. In the authentication phase, the pre-trained CNN model is selected based on the user ID obtained from the token. The gripping hand shape is then verified, resulting in two confidence scores for the two classes (e.g., user and nonuser). Based on that, we determine whether the user identity is as claimed.

The architecture of our CNN-based hand verification model is shown in Figure 5, where the input is a 2D gripping hand matrix with a dimension of 200 x 150 x 3, and the output is the class probability distribution. The input is first passed through a convolutional layer with a kernel size of 3 x 3 to be transformed into high-level features. The Rectified Linear Unit (ReLU) is used as the activation function to speed up training. Followed by the convolutional layer, a 2 x 2 max-pooling layer is added to downsample the feature maps both vertically and horizontally, which aims to reduce the number of parameters and thus reduce the computational costs. The same architecture is repeated three times, and the resulted features are passed through a flatten layer to be converted into a 1D vector. A dropout layer is then added to prevent the network from memorizing specific features of the training data, thus preventing over-fitting, after which three fully connected dense layers are deployed to shrink the size of the vector. Finally, a softmax layer is applied to turn the vector from dense layers into a vector of two real values (i.e., the class probability distribution) that sum to 1. During training, the multi-class cross-entropy is used as the loss function.

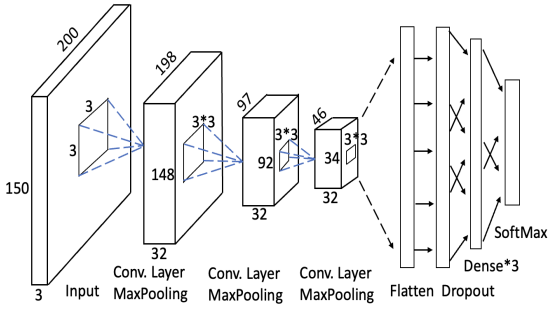

Figure 5: CNN-based hand verification model.

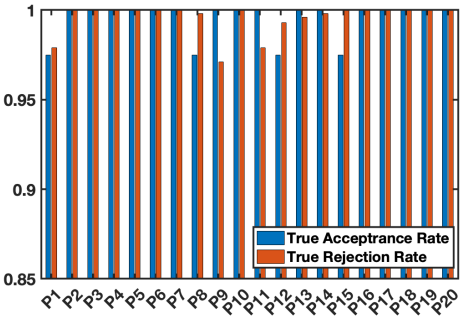

Figure 6: User verification performance.

4 PERFORMANCE EVALUATION

4.1 Experimental Setup and Data Collection

We recruit 20 participants (15 males and 5 females with the ages from 19 to 61) to study the potential of user verification via gripping hand images. We find people tend to use their dominant hand to hold the phone for Kiosk authentication and different phone models influence the gripping hand shape. Given that it is much easier to distinguish between right and left hands and different phone models, this paper considers a more challenging scenario assuming that their dominant hand is the right hand and they all use the same phone (e.g., a Motorola G8 phone), The experiments were conducted in a typical indoor office scenario with regular ceiling lights. Before data collection, the participants were asked to use the phone for 10 minutes to get used to the device shape like they were the owner. During the experiment, each participant was asked to hold the phone to a vertically placed camera (Samsung S8) 100 times. The participant must re-grab the phone each time to present behavioral inconsistency that may occur in practical smartphone use, including the slightly different gripping positions and the variant angles and distances from the hand to the camera. In total, 2,000 RGB images are collected. 60% are used for training and the rest are for testing.

4.2 User Verification Performance

We first evaluate the performance of our system to verify users by their gripping hands. Figure 6 presents the True Acceptance Rate (TAR) and the True Rejection Rate (TRR) of verifying 20 users, respectively. We observe that our system performs well for verifying all users. In particular, the system achieves 99.5% TAR and 99.6% TRR on average. More than half of these users achieve 100% TRR while 80% of them obtain 100% TAR. The results indicate that the system accepts a legitimate user with a high rate while a non-user is rejected. An adversary now has to break both the security tokens and the gripping hand biometrics simultaneously to pass the Kiosk authentication, which is more difficult. Moreover, the system is able to tolerate the behavioral inconsistency, including the slightly varying gripping positions and the different distances and angles from the hand to the camera in practical use.

4.3 User Classification Performance

We further study how well the gripping hand biometrics could distinguish people and consider a multi-class user classification scenario. Figure 7 presents the confusion matrix of our approach to classify 20 participants. We find the system achieves a high accuracy of distinguishing people's gripping hands. In particular, our approach achieves 99.1% accuracy on average to classify these users. 90% of users achieve over 97% accuracy, and 75% of them reach 100% classification accuracy. The result confirms that the gripping handshape is human identifiable. It also demonstrates the gripping hand shape as an extension of the traditional hand geometry biometric in the handheld device scenario.

4.4 Comparing Gripping Hand Features

We now compare the gripping hand features obtained from the color, grayscale, and contour of each hand. The hand contour image only provides the outline of the gripping hand; The greyscale image further adds the detailed shape features of the hand, including finger joints, knuckles, tendons and veins; The color image includes the skin color patterns in addition to the above two types of features. Figure 8 shows the accuracy performances of using the three types of images for user classification. The color image shows the highest accuracy, which is 99.1%. The reason is that the color images contain all three major types of gripping hand features. In comparison, the grayscale image achieves 98.1% accuracy, and the hand contour achieves the lowest accuracy, which is 97.9%. The results show that the hand contour exhibits significant and stable biometric features for user identification, while the hand shape features and the skin color patterns can further improve the identification performance. The results also indicate the potential of using a depth camera to replace the RGB camera for gripping hand verification, which better preserves the user's privacy and suffers less from the background colors and different light conditions.

4.5 Impact Of Light Conditions

At last, we evaluate the impact of the light condition by examining the hand images under different illuminance levels. Specifically, we calculate the average brightness of each image [26] and estimate its illuminance between 0 and 1 by referring to the brightness map [27]. For example, the original illuminance of our hand images collected indoor is mostly between 0.4 and 0.5. We then use the ImageEnhancer.Brightness() method in OpenCV's PIL Library to modify the illuminance of the images to simulate different light conditions. The resulting images are fed into the system as the input. Figure 9 shows the user classification accuracy under nine different illuminance levels from 0.2 to 0.9. We find that our approach achieves good

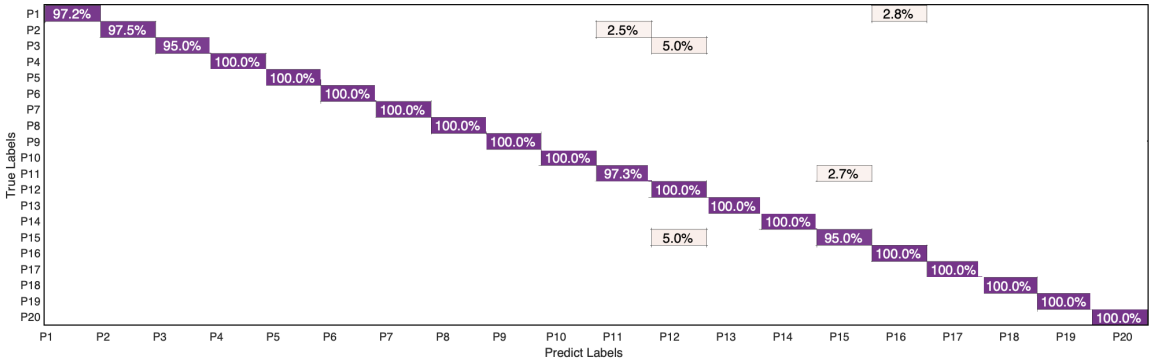

Figure 7: User classification performance.

performance for all these illuminance levels. The highest performance is obtained with 0.45 illuminance, which is 99.1%. The result indicates that the proposed approach works well for most indoor light conditions. Furthermore, we find the performance slightly degrades when the illuminance level increases or decreases. For example, when the illuminance is 0.3 and 0.4, the accuracy is 97.8% and 98.0%, respectively. When it increases to 0.6 and 0.8%, the accuracy is 98.6% and 98.2%, respectively. These performances are all above that achieved by only using the hand contour. The reason is that the brightness of the hand image affects its contrast ratio and the color saturation, which may bring noises to the hand detection/segmentation process and the extracted features. Nevertheless, because our approach relies more on the hand contour than greyscales and color patterns as illustrated in Section 4.4, it is able to tolerate a wide range of illuminance levels.

5 RELATED WORK

Many works have been on extracting biometric information from the user's hand for authentication. For example, the geometry of the back of a human hand is shown to be uniquely identifiable, which can be obtained by a top-hung camera when the hand is placed on a flat surface with the palm facing downwards [22, 24]. The finger lengths, widths, angles and the distances between them are extracted as biometric features. There are also works on scanning the palm face of the hand by placing an image sensor under the flat surface [17, 20], and both the hand geometry and the palm print patterns are used for authentication. More recent works focus on extracting hand biometrics with contact-free data acquisition methods [14, 18] or using low-cost mobile device cameras to lower the hardware cost [8]. However, these methods are intrusive by requiring high installation overhead or active user participation, such as asking the user to press the palm against a scanner or take a stretched palm photo. They are thus hard to be deployed widely.

The latest development of Kiosks shows an increasing trend to adopt biometrics for authentication. For example, Sawetsutipun*et al.* [25] explore integrating the facial image verification technique with government Kiosks, which allows citizens to access their welfare data and receive services through a Kiosk instead of going to a government office. To further enhance the security, AlRousan*et al.* [2] propose a multi-factor authentication approach, that asks users to input a One-Time Password (OTP) received by their smartphone together with their face and fingerprint. Pichetjamroen*et al.* [21] develop a two-factor authentication system for Kiosks, whose authentication process remains to be contactless. In particular, the users need to both verify the face and show a QR code received by their phone to the Kiosk. Different from the above methods, which require more user efforts to provide additional biometric inputs, our two-factor authentication system acquires the user's gripping hand biometrics simultaneously with the current NFC or QR code-based authentication when the user holds the phone close to the Kiosk.

6 DISCUSSION & FUTURE WORK

This work extends the traditional hand geometry biometrics to the more practical handheld device scenarios. It demonstrates the potential of using this novel biometric for Kiosk authentication without incurring additional user efforts. Future work is needed to perform extensive evaluations to establish the gripping hand geometry as a reliable biometric, by recruiting more participants and testing more light conditions, camera distances and angles and backgrounds (e.g., clothes). Additionally, we will continue to address the following challenges to accelerate the deployment of this technique on real Kiosks:

Other Impact Factors. In addition to behavioral inconsistency and light conditions, it is also important to investigate the impacts of wearing hand jewelry, a cut on the hand and different phone models. Specifically, consistently wearing some jewelry pieces (e.g., rings, bracelets, and watches) can add additional security features, but changing the jewelry or a new cut on the hand may increase the false rejection rate. We need to quantify their impacts before leveraging or removing them from images. Furthermore, the shapes and dimensions of different phone models may lead to different gripping hand shapes for a user, which may bring inconvenience if the user switches to a new phone. But the phone model differences also result in more easily distinguished gripping hands among users, which enhances security. We will study both the usability and the security to determine whether the system can tolerate model differences or an update of the biometric profile is needed for switching phones.

Training Efforts. Our current approach requires the user to re-grab the phone multiple times to obtain the gripping hand images for creating the user profile. During this process, behavioral inconsistency is considered. For the next step, we will study the impact of training size and identify the minimum training efforts required for each user. Beside, data augmentation methods will be explored

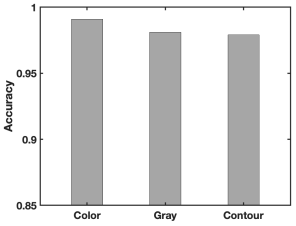

Figure 8: Comparing differ-ent gripping hand features.

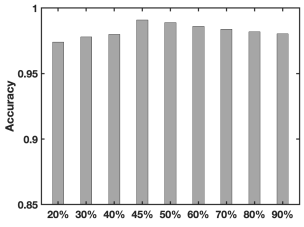

Figure 9: Impact of illumi-nance.

to increase the training data size and cover more practical scenarios. Furthermore, we will explore other deep learning approaches efforts (i.e., Siamese Network) and more advanced biometric features to further reduce training efforts and improve system robustness under the above-mentioned impacts. In addition, the feasibility of transferring the biometric features from one phone model to the other is worth exploring, which saves the effort of retraining.

Potential Attacks. In addition to the in-person identity spoofing, an attacker may physically forge the target user's gripping hand with a photo or a 3D-printed fake hand. Thus, liveness detection is needed to defend against such attacks. One solution is to take video frames instead of static pictures to verify the user's gripping hand, which has been shown successfully in differentiating real and fake hands [3]. Moreover, it is also interesting to explore using an infrared camera to replace the RGB camera for both gripping hand shape extraction and liveness detection.

7 CONCLUSION

This work proposes a gripping hand verification approach, which adds a biometric factor to the current token-based Kiosk authentication without requiring additional user efforts. In particular, the approach uses an ordinary camera to take a photo of the back of the user's hand for verification when it grips a phone. We develop the hand image processing schemes for hand detection, background removal and normalization. The extracted gripping hand features are fed into a three-convolutional-layer CNN model to recognize whether the gripping hand belongs to the user identity claimed by the traditional security token. Experiments with 2000 images show that the gripping hands can be used as a biometric factor to identify the user during contact-free human-kiosk interaction.

ACKNOWLEDGMENTS

This work was partially supported by LEQSF(2020-23)-RD-A-11.

REFERENCES

[1] Irfan Ahmad and Manzoor Khan. 2017. *Hand recognition using palm and hand geometry features.* LAP LAMBERT Academic Publishing.

[2] Mohammad AlRousan and Benedetto Intrigila. 2020. Multi-Factor Authentication for e-Government Services using a Smartphone Application and Biometric Identity Verification. *Journal of Computer Science* (2020).

[3] Özge Aydoğdu, Zhaleh Sadreddini, and Murat Ekinci. 2018. A Study on Liveness Analysis for Palmprint Recognition System. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 1–4.

[4] John Canny. 1986. A computational approach to edge detection. *IEEE Transactions on pattern analysis and machine intelligence* 6 (1986), 679–698.

[5] Electronic Privacy Information Center.epic.org. 2019. EPIC - State Facial Recognition Policy. https://epic.org/state-policy/facialrecognition/

[6] Anh Dang. 2020. Facial Recognition: Types of Attacks and Anti-Spoofing Techniques. https://towardsdatascience.com/facial-recognition-types-of-attacks-and-anti-spoofing-techniques-9d732080f91e

[7] Grandviewresearch.com. 2020. Interactive Kiosk Market Size, Share and Trends Analysis Report By Component (Hardware, Software, Services), By Type (ATMs, Self-service Kiosks), By End Use (BFSI, Healthcare), By Region, And Segment Forecasts, 2021 - 2028. https://www.grandviewresearch.com/industry-analysis/interactive-kiosk-market

[8] Ahmad Hassanat, Mouhammd Al-Awadi, Eman Btoush, Amani Al-Btoush, Esra'a Alhasanat, and Ghada Altarawneh. 2015. New mobile phone and webcam hand images databases for personal authentication and identification. *Procedia Manufacturing* 3 (2015), 4060–4067.

[9] iClassPro. 2021. How Do QR Codes Work with the Check-In Kiosk? https://support.iclasspro.com/hc/en-us/articles/360024943634-How-Do-QR-Codes-Work-with-the-Check-In-Kiosk-

[10] Md Khaliluzzaman, Md Mahiuddin, and Md Monirul Islam. 2018. Hand geometry based person verification system. In *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*. IEEE, 1–6.

[11] KIBIS. 2019. Types of kiosks that are assisting us in everyday life. https://medium.com/kibis/types-of-kiosks-that-are-assisting-us-in-everyday-life-ed8337f8bead

[12] Kaila Lafferty (KING5). 2021. Seattle's COVID-19 self-testing kiosks run risk of false negatives, FDA warns. https://www.king5.com/article/news/health/coronavirus/curative-covid-19-testing-kiosks-may-result-in-false-negatives-fda-says/281-2de491a0-7916-4797-94c7-ac352a4ccc31

[13] Marek Klonowski, Marcin Plata, and Piotr Syga. 2018. User authorization based on hand geometry without special equipment. *Pattern Recognition* 73 (2018), 189–201.

[14] Rafael M Luque-Baena, David Elizondo, Ezequiel López-Rubio, Esteban J Palomo, and Tim Watson. 2013. Assessment of geometric features for individual identification and verification in biometric hand systems. *Expert systems with applications* 40, 9 (2013), 3580–3594.

[15] DAN MESSINEO. 2021. Seminole County Adds COVID-19 Self-Testing Kiosk. https://www.mynews13.com/fl/orlando/news/2021/03/15/seminole-county-adds-covid19-self-testing-kiosk

[16] Neha Mittal, Madasu Hanmandlu, and Shantaram Vasikarla. 2018. An Authentication System based on Hybrid Fusion of Finger-Shapes & Geometry. In *2018 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*. IEEE, 1–7.

[17] Hesham Hashim Mohammed, Shatha A Baker, and Ahmed S Nori. 2021. Biometric identity Authentication System Using Hand Geometry Measurements. In *Journal of Physics: Conference Series*, Vol. 1804. IOP Publishing, 012144.

[18] Laura Gulyás Oldal and András Kovács. 2020. Hand geometry and palmprint-based authentication using image processing. In *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY)*. IEEE, 125–130.

[19] Frank Olea. 2015. How NFC tech can improve your kiosk. https://www.kioskmarketplace.com/blogs/how-nfc-tech-can-improve-your-kiosk/

[20] Michael Goh Kah Ong, Tee Connie, Andrew Teoh Beng Jin, and David Ngo Chek Ling. 2003. A single-sensor hand geometry and palmprint verification system. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*. 100–106.

[21] Sasakorn Pichetjamroen, Ekkachan Rattanalerdnusorn, Chalee Vorakulpipat, and Achara Pichetjamroen. 2021. Multi-Factor based Face Validation Attendance System with Contactless Design in Training Event. In *2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. IEEE, 637–640.

[22] Arun Ross, Anil Jain, and S Pankati. 1999. A prototype hand geometry-based verification system. In *Proceedings of 2nd conference on audio and video based biometric person authentication*. 166–171.

[23] NATALLIA SAKOVICH. 2020. Benefits of Self-Service Kiosks for Businesses and Users. https://www.sam-solutions.com/blog/the-value-of-interactive-kiosks-for-your-business/

[24] Raul Sanchez-Reillo, Carmen Sanchez-Avila, and Ana Gonzalez-Marcos. 2000. Biometric identification through hand geometry measurements. *IEEE Transactions on pattern analysis and machine intelligence* 22, 10 (2000), 1168–1171.

[25] Srirath Sawetsutipun, Thananop Kobchaisawat, and Thanarat H Chalidabhongse. 2020. Facial Image Verification for Government Kiosk System. In *2020 17th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. IEEE, 65–70.

[26] Michael W Schwarz, William B Cowan, and John C Beatty. 1987. An experimental comparison of RGB, YIQ, LAB, HSV, and opponent color models. *ACM Transactions on Graphics (TOG)* 6, 2 (1987), 123–158.

[27] StackOverflow.com. 2021. What are some methods to analyze image brightness using Python? https://stackoverflow.com/questions/3490727/what-are-some-methods-to-analyze-image-brightness-using-python

[28] Sur-id. 2021. Contactless Check-In Kiosk. https://www.sur-id.com/?gclid=CjwKCAjwoP6LBhBlEiwAvCcthKrwMIkDtwqv6-lw3rL5OMl2FXsIHw-blZbI1v1fPcHI5Ca-1vfNfRoCTpQQAvD_BwE

[29] Staff Writer. 2020. Facial Recognition Photo Kiosks. https://kioskindustry.org/facial-recognition-photo-kiosks/