IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 12, 2021, accepted November 18, 2021, date of publication November 30, 2021,
date of current version December 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131551

On-Air Hand-Drawn Doodles for IoT Devices Authentication During COVID-19

ABDELGHAFAR R. ELSHENAWAY AND SHAWKAT K. GUIRGUIS
Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, Alexandria 21526, Egypt
Corresponding author: Abdelghafar R. Elshenaway (igsr.abdelghafar_refat@alexu.edu.eg)

ABSTRACT In this paper, a new natural human interaction authentication method is proposed for Internet of Things (IoT) devices. In this method, the user draws a doodle on the air for authentication. On-air drawing refers to virtually drawing free hand-drawn doodle passwords through hand gestures on the air without touching anything that is recommended during COVID-19. This study uses the Google Quick Draw Doodle dataset for password doodles. The proposed method is based on a typical video camera, two lightweight convolutional neural networks (CNNs) and a Kalman filter. The first CNN for hand gesture classification was used to overcome dynamic hand gesture challenges on the air. Second CNN for authentication verification. A Kalman filter was used to correct and smooth the path drawn on the air. Two main goals must be achieved to accept the new authentication method: usability and security. The usability evaluation was based on the ISO 9241-11:2018 standard usability model. The results revealed that the accuracy of the proposed authentication method was 95%, efficiency was 94%, and user satisfaction was acceptable. The evaluation of security was based on two threats related to IoT devices: guessing and physical observation. The results show that the password strength of the proposed authentication method is stronger than the traditional 4-digits PIN password. The proposed authentication method is also resistant to physical observation threats.

INDEX TERMS Convolutional neural networks (CNNs), data augmentation, Kalman filter, human-computer interaction (HCI), hand gesture recognition, doodle, air writing, graphic password, Raspberry Pi.

I. INTRODUCTION

In the world of the Internet of Things, all things are smart enough to communicate with each other. However, the question is how humans interact with smart things. Traditional methods such as computers, mobile devices, smart watches, or embedded touchscreens, which depend on the graphical user interface, are not suitable and are not effective in interacting with smart things. Hence, a new method of human natural interaction is required to interact with smart things. Authentication is the most important and first step in the interaction between IoT devices and humans. Authentication plays an important role in security systems and operations. This study proposes a simple and secure natural interaction authentication method. It is simple because it is based on hand gesture interaction and is secure because we cannot see the drawing on the air. On-air drawing or writing is also suitable in many situations, for example:

1. During the spread of epidemics through touch. For example, the spread of COVID-19.

2. Virtual reality applications for drawing or writing in virtual environments.

3. Writing messages on a mobile device without using keys or touch screens.

4. Controlling smart IoT devices without traditional keypads or remotes.

5. In some cases, when we are not able to write on paper, for example, for partially sighted, writing underwater, or writing on the Moon, where there is no gravity.

On-air drawing or writing is not only drawing but also requires some commands to control the operation, such as drawing, erasing, and saving. Therefore, this study proposes three hand gestures to control drawing operations. There are two types of hand gestures: static and dynamic. In the static state, the hand remained constant in front of the camera. However, the proposed method of on-air writing is based on dynamic hand gestures because the hand moves in three dimensions during writing on air. Dynamic hand gesture recognition has many challenges, which are very difficult and

The associate editor coordinating the review of this manuscript and approving it for publication was Huiyan Zhang.

complex tasks, especially with IoT devices that have little computational ability and small memory. Fig.1 illustrates the dynamic hand gesture challenges.

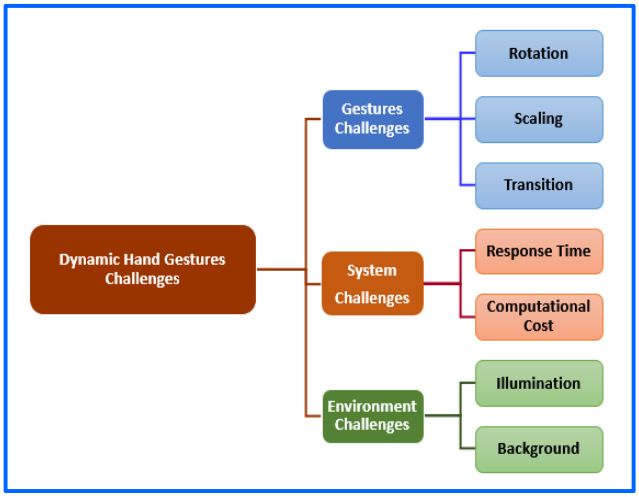


FIGURE 1. Dynamic hand gesture challenges.

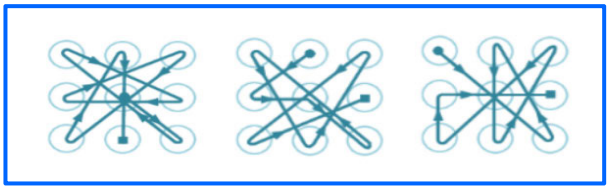
The second problem with on-air writing is the zigzagging of the drawn line path on the air, as shown in Fig.2.

FIGURE 2. Zigzagged path problem of on-air drawing.

The distortion of the on-air drawing path is due to the lack of stability of the hand in the air during drawing. This distortion makes it more difficult to recognize drawing symbols on the air using a CNN for the authentication verification stage.

The current and most popular hand-drawn passwords are pattern grid passwords. However, pattern-grid passwords exhibit certain defects. The pattern grid method was restricted to grid points while drawing, and the number of grid points. It was difficult to remember and memorize pattern passwords when using a large number of grid points. Fig.3 (a) shows three examples of the complex-pattern grid passwords. It was also difficult to remember and memorize several passwords. In particular, there are many smart devices in IoT environments. For example, a smart home contains ten smart devices. In this case, it was difficult to memorize and remember the ten password patterns.

In contrast to the above, the proposed hand-drawn symbol method is not restricted by the grid points, direction, or symbol size. The user only draws a shape -somehow– close to the shape of the password symbol. The proposed method is based on well-known symbols that facilitate the process of remembering and memorization. Fig.3 (b) shows three examples of complex hand-drawn symbol passwords.



(a) Pattern grid password.

(b) Proposed hand-drawn symbol password.

FIGURE 3. Three examples of complex passwords.

Therefore, it is very suitable for the Internet of Things to remember and memorize many passwords.

A. NOVELTY AND CONTRIBUTION

The principal contributions of this paper:

1- This work proposes an on-air drawing technique that is based on only three hand gestures without touching anything that is recommended during COVID-19.

2- Free hand-drawn symbols password without being restricted to size, grid, or orientation.

3- This work proposes a lightweight CNN that is trained on an adapted artificial image dataset to overcome dynamic hand gesture challenges.

4- This work proposes to solve the problem of zigzagging of the on-air drawn path based on the Kalman filter by tuning its parameters.

To evaluate the proposed system, a prototype was implemented using TensorFlow on the Google Colab platform. The CNN models were transformed into TensorFlow Lite models that were deployed on the Raspberry Pi board. A Raspberry Pi camera was used to capture video images. Fig.4 shows the proposed and traditional methods.

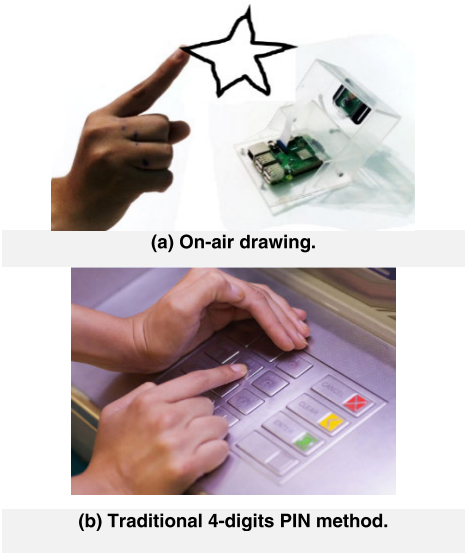
The remainder of this paper is organized as follows. Section II discusses significant previous studies. Section III provides a detailed description of the proposed authentication scheme. Section IV presents the materials and methods used in this study. Section V discusses the evaluation of the proposed system. Section VI presents the results and discusses the results. Section VII presents the conclusions.

II. RELATED WORKS

There are two main categories of related work. The first category involved the on-air writing challenges. The second category involved hand-drawing symbols for the graphical passwords. The following subsections present the latest research papers for all the categories.

A. ON-AIR WRITING TECHNIQUE

There are four main techniques for related work to overcome the on-air writing challenge. These techniques are based on



(a) On-air drawing.

(b) Traditional 4-digits PIN method.

FIGURE 4. Proposed and traditional methods.

radio waves, devices, wearable sensors, and computer vision. The following subsections present the latest studies on each technique.

1) RADIO WAVES-BASED TECHNIQUE

Uysal and Filik [1] proposed the use of radio frequency (RF) waves for human-machine interaction, such as air writing. They proposed a device-free system based on a machine-learning air-writing recognition framework called RF-Wri, which can effectively distinguish 26 capital letters. Two-channel low-cost software-defined radios (SDR) and oppositely polarized antennas are used to provide polarization diversity, which makes the classification accuracy superior. It is verified with various real measurements that the proposed framework, RF-Wri, achieves 95.15% accuracy in the classification of all 26 air-written letters and outperforms the fairly new WiFi-based air-writing recognition approaches.

Regani *et al.* [2] proposed a millimeter wave (mmWave), the first high-precision passive handwriting tracking system using a single commodity mmWave radio. By leveraging the short-wavelength and large bandwidth of 60 GHz signals and the radar-like capabilities enabled by the large phased array, mmWrite transforms any flat region into an interactive writing surface that supports handwriting tracking with millimeter accuracy.

Chen *et al.* [3] presented a three-dimensional (3D) pen-like positioning system based on a high-precision 3D ultrasonic positioning method. The high-precision 3D ultrasonic positioning method can achieve millimeter-level accuracy in 3D positioning within a working area of 2 m $\times$ 1.5 m $\times$ 1.5 m.

Lin *et al.* [4] proposed the WiFi Write, an accurate device-free handwriting recognition system that allows writing on air without the need to attach any device to the user. Specifically, they used **c**ommercial **o**ff-**t**he-**s**helf (COTS) WiFi hardware to achieve fine-grained finger tracking.

Arsalan *et al.* [5] proposed using only one or two radars to sense the local hand trajectory. They proposed the use of a 1D temporal convolutional network (TCN) for simultaneous feature extraction and temporal modeling to recognize the drawn character from the local target trajectory. The results showed that the accuracy was 99.11% and 91.33% for the two radar and one radar-based solutions, respectively, outperforming other deep architectures.

Wang *et al.* [6] proposed a prototype of a gesture air-writing tracking system based on a 24-GHz frequency-modulated continuous-wave (FMCW) radar system-on-chip (SoC). The transmitted chirp signal of this radar chip covers up to a 4-GHz bandwidth, which provides sufficient range resolution to track hand gestures. With the development of single-input and multiple-output (SIMO) antennas, air-writing symbols can be reconstructed in an observation plane.

Fang *et al.* [7] proposed a WiFi-based system called Wima, which recognizes letters written in air by hand. Unlike existing WiFi-based handwriting recognition systems, Wima extracts features directly from the original CSI and then transmits them to subsequent classifiers immediately, and a deep-learning-based method is first introduced in this system to automatically extract high-level features.

Khan *et al.* [8] proposed an impulse radio ultra-wideband (IR-UWB) radar-based system that can recognize alphanumeric characters in midair without the need for any handheld device. The hardware consisted of four IR-UWB radar sensors with rectangular geometry.

Leem *et al.* [9] proposed classifying digits written in mid-air using hand gestures. Impulse radio ultra-wideband (IR-UWB) radar sensors were used for data acquisition, with three radar sensors placed in a triangular geometry.

Lu *et al.* [10] proposed a virtual writing tablet system, VPad, for traditional laptops without touch screens. VPad leverages two speakers and one microphone, which are available in most commodity laptops, for trajectory tracking without additional hardware. It employs acoustic signals to accurately track hand movements and recognize characters that the user writes in the air. Specifically, the VPad emits inaudible acoustic signals from two laptop speakers. Then, VPad applies the sliding window overlap Fourier transformation technique to find the Doppler frequency shift with higher resolution and accuracy in real time.

Zhang *et al.* [11] proposed WiFi, a high-accuracy letter recognition in an air system that could detect and recognize a letter written by a user by analyzing its influence on surrounding WiFi signals.

2) DEVICES-BASED TECHNIQUE

David *et al.* [12] proposed a leap motion controller to detect the position of the user's finger, which acts as the ''pen'' in air-writing English capital letters, and dynamic time warping to recognize air-drawn letters. They evaluated the overall reliability of the system by allowing users to test the system by air-writing each of the 26 letters numerous times.

Bastas *et al.* [13] proposed a deep learning architecture for the air-writing recognition problem in which a person writes text freely in three-dimensional space. They focus on handwritten digits, namely, from 0 to 9, which are structured as multidimensional time-series acquired from a leap motion controller (LMC) sensor.

Yan *et al.* [14] proposed a three-dimensional pen interaction technique based on pen roll angle in normal writing or drawing. Two experiments were conducted to evaluate the proposed system. In Experiment 1, the range of the pen's pitch angle, yaw angle, and roll angle due to normal writing and drawing unconsciously in 3D space were explored to show that the roll angle is used only a small part of the possible range, so it could be used in interactive control. In experiment 2, the ranges of roll angle, accuracy, and efficiency were further investigated under conscious interaction. Two independent variables, angular width and angular distance, were introduced to evaluate the performance of the system. The experimental results show that the available angle range $[-135°, -20°]$ and $[20°, 135°]$ together with an angle resolution $W = 10°$ are the preferred parameter combinations.

Xu *et al.* [15] proposed a new authentication method. This method is based on the user writing a password in air using Leap Motion.

Taktak *et al.* [16] proposed a 3D handwriting character recognition algorithm based on a symbolic representation of the angular velocity signal generated from a gyroscope sensor included in a smartphone. The characters were written in a 3D air space by a user via a smartphone device.

Wang *et al.* [17] proposed a wireless flying mouse to satisfy the requirements for air writing. They designed a wireless flying mouse model. First, according to the characteristics of low power consumption, the main part of the wireless flying mouse was chosen as follows. The LPC54100 Series MCU was chosen as the main controller. The motion sensor module, MPU6050, was used to obtain hand control information. Two Bluetooth supporting low-power devices were used as communication modules.

3) WEARABLE SENSORS-BASED TECHNIQUE

Luo *et al.* [18] proposed a wearable air-writing system that allows users to write the English alphabet in a three-dimensional space without any write rules. The proposed system is based on an inertial measurement unit (IMU) and uses dynamic time warping (DTW) as the main recognition algorithm.

Behera *et al.* [19] proposed a new method to verify air signatures by analyzing finger movements and cerebral activities together with the help of sensors in next-generation CE devices. Signatures were first identified by analyzing the 3D geometrical features of finger movements during signing. Concurrent EEG responses were analyzed for verification.

Pal [20] proposed a technique for writing in air using a Micaz mote. The application, named MicaPen, is low-cost and can be used by people with disabilities who do not have fingers or limbs. Patients can wear the mote as a wrist watch or bracelet and move their hands based on the character they want to write. The mote detects the movement pattern using the accelerometer of the MTS310 sensor board and displays the characters on the screen.

Chandel *et al.* [21] proposed a novel 3-D tracking solution, 'AiRite' for commercial-grade smart wearables/mobiles using only their onboard IMU. Our tracking method mitigates the manifested inertial errors using a novel progressive zero correction, yielding superior results both for 2-D and 3-D trajectories.

Chen *et al.* [22] investigated real-time fingertip detection in RGB images/frames captured from wearable devices, such as smart glasses. A modified mask regional convolutional neural network (Mask R-CNN) is proposed with a region-based CNN for hand detection and another three-layer CNN for locating the fingertip.

Sankhe *et al.* [23] proposed a fingertip detection system that can be efficiently used by smart wearables. This approach is free of markers and centroid-based techniques that are traditionally used to detect fingertips.

Meli *et al.* [24] proposed hand in air tapping (HAT), a wearable input interface which allows interactions through finger tapping. It consists of Bluetooth low-energy rings that enable wireless communication with a compatible device. The proposed system was evaluated in two user studies, both on text input: (1) user learning curve in terms of writing speed; (2) rate of text entry comparison between the proposed interface and that of numpad-style keyboards.

Lu *et al.* [25] proposed a new finger-gesture-based authentication method in which the in-air handwriting of each user is captured by wearable inertial sensors. This approach is characterized by the utilization of both the content and the writing convention, which are proven to be essential for the user identification problem in experiments. A support vector machine (SVM) classifier was built based on the features extracted from the hand-motion signals.

4) COMPUTER VISION-BASED TECHNIQUE

Malik *et al.* [26] presented a novel method for end-to-end deep learning-based in-air signature verification using depth sensor cameras. In this regard, they proposed a new medium-scale in-air signature dataset that was created using an accurate convolutional neural network based on a 3D hand pose estimation algorithm. The verification approach achieved an EER of 0.055%.

Puranik *et al.* [27], in this study, was a point-gesture detector-cum-identifier. They used computer vision to trace the trajectory of the finger and machine learning to recognize the word (out of the image that is formed through the action of motions).

Alam *et al.* [28] proposed a trajectory-based air-writing character recognition system using a convolutional neural network (CNN). The trajectories were collected using a depth camera as a three-dimensional (3D) sequence.

Li *et al.* [29] proposed a human-computer interaction (HCI) system for entertainment or education based entirely

on computer vision via a depth-sensing camera from the Kinect to predict the hand position, making the tracking smooth and robust.

Hegde *et al.* [30] proposed a cascade of networks, consisting of a CNN with a differentiable spatial-to-numerical transform (DSNT) layer for fingertip regression, followed by bidirectional long short-term Memory (Bi-LSTM), for a real-time pointing hand gesture classification.

Joseph *et al.* [31] proposed a combination of computer vision and convolution neural networks to detect drawn gestures and recognize them.

Roy *et al.* [32] proposed an air-writing framework based on a generic video camera and convolutional neural network. Gestures are performed using a marker of fixed color in front of a generic video camera, followed by color-based segmentation to identify the marker and track the trajectory of the marker tip.

Lakshmi and Harish [33] designed a finger writing system that displays data written in air without the need for an extra handheld device. A camera was used to capture the finger movements.

B. DRAWING PASSWORD AUTHENTICATION

Wazir *et al.* [34] proposed an approach for real-time size and coordinate matching of doodles in an AR environment for user authentication. The creation of doodle passwords in an AR space is performed by touch gesture recognition on a smartphone.

Liu *et al.* [35] proposed a secure and user-friendly MFUA system, namely BioDraw, which utilizes four categories of biometrics (impedance, geometry, composition, and behavior) of the human hand and a pattern-based password to identify and authenticate users. A user only needs to draw a pattern on an RFID tag array, while four biometrics can be simultaneously collected.

Khan and Chefranov [36] presented a graphical password scheme under the impact of security and ease of use for user authentication.

Tolosana *et al.* [37] proposed enhanced password scenarios through two-factor authentication by asking users to draw each character of the password instead of typing them as usual. This study presents a novel MobileTouchDB public database, acquired in an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices.

Tolosana *et al.* [38] proposed enhanced traditional authentication systems based on personal identification numbers (PINs) and one-time passwords (OTP) through the incorporation of biometric information as a second level of user authentication. In the proposed approach, users draw each digit of the password on the touchscreen of the device instead of typing them as usual. A complete analysis of our proposed biometric system is carried out regarding the discriminative power of each handwritten digit and the robustness when increasing the length of the password and the number of enrolment samples.

Ku *et al.* [39] presented a novel mechanism based on pattern lock, in which behavioral biometrics were employed to address these problems. The basic idea starts from turning the lock pattern into public knowledge rather than a secret and leveraging touch dynamics. Users do not need to create their own lock patterns or memorize them. Instead, our system shows a public pattern, along with guidance on how to draw it. All users must perform authentication by drawing a pattern.

Fayyadh *et al.* [40] proposed a new hybrid graphical password scheme using two-dimensional (2D) shapes to create passwords. In this new scheme, users are asked to use certain 2D shapes to draw graphical passwords during registration.

Schwab *et al.* [41] proposed a picture PassDoodle that uses free-form drawing to increase security and uses a background picture that has many points of interest to achieve usability features.

Riesen *et al.* [42] proposed a novel framework for user authentication based on freehand sketches. The basic idea is that during the registration phase, a user draws an arbitrary sketch in a specific drawing canvas (rather than typing a password).

Martinez-Diaz *et al.* [43] studied authentication using freeform sketches. Verification systems using dynamic time warping and Gaussian mixture models have been proposed based on dynamic signature verification approaches.

C. RESEARCH GAP

The first three techniques in the related works provided solutions for writing on the air with high accuracy, but depend on special devices, sensors, and they are considered expensive. In addition, they require special settings that are not suitable for the Internet of Things (indoor or outdoor). The fourth technique depends on computer vision and follows the movement of the hand while writing on the air using a single camera, multi-camera, or deep camera. This method is easy, simple, and inexpensive. However, this technique has the problem of a zigzagged line. Therefore, the contribution of this work depends on computer vision using a single camera and proposes to solve the problem of zigzagging of on-air drawn paths based on the Kalman filter by tuning its parameters. It also proposes free hand-drawn symbols passwords without being restricted by size, grid, or orientation instead of writing numbers for authentication, which increases confidentiality, as will be discussed in the security section evaluation.

III. THE PROPOSED SYSTEM

The proposed system consists of four parts such as shown in the following Fig.5.

First, a computer vision technique was used for hand detection and the creation of a virtual pen. This virtual pen is automatically picked up by the hand when the hand is in front of the camera. Second, a lightweight deep CNN for dynamic hand gesture recognition was used to classify three-hand gestures. An open-index finger gesture was used for the drawing. An open-hand gesture was used for the erasing.

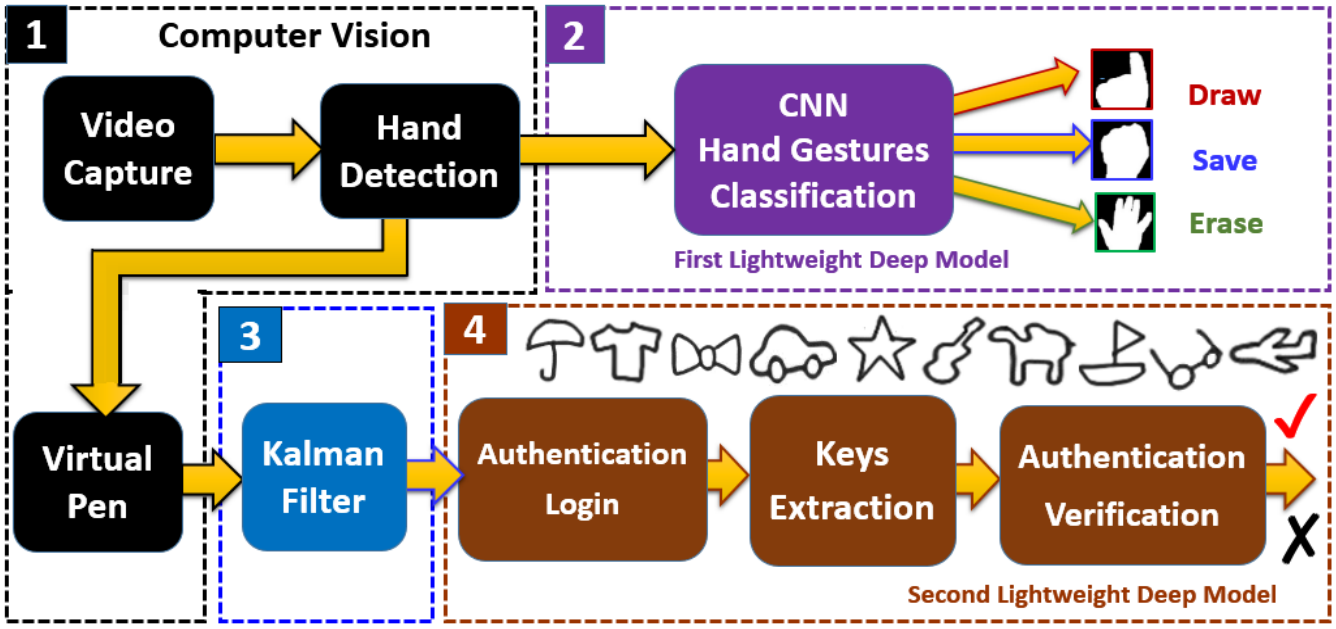


FIGURE 5. Main parts of on-air hand-drawn Doodle authentication.

A closed-hand gesture was used to save. Third, the Kalman filter is a simple and lightweight algorithm. This algorithm was used to smooth hand-drawn symbols on the air. Fourth, login authentication and verification consists of three stages. First, the authentication key symbols are drawn to the login. Second, keys were extracted. Third, a lightweight deep CNN was used to verify authentication keys. The following subsections provide an in-depth explanation for each part.

A. HAND DETECTION AND CATCH VIRTUAL PEN

The aim of this stage was to achieve three goals. First, the hand is detected based on skin color. Second, the center of the hand was determined. Third, the topmost point of the hand representing the fingertip was determined. These three goals were achieved by capturing a hand image using a camera. The image of the hand then passes through several filters, as shown in Fig.6. The following subsections provide an in-depth explanation for each part.

1) COLOR FILTER

This is the preliminary processing step and the most important step because failure in this stage leads to failure in all the following stages. This stage depends on the color of the skin of the hand used to detect the hand in the image. However, the color of the skin varies from person to person or due to the difference in the level of illumination in the place, which may lead to the failure of this stage. To avoid this problem, the proposed system performs calibration prior to the validation process. Calibration was performed by placing the hand in front of the camera for five seconds before the on-air drawing process. Finally, the camera captures the color of the skin of the hand to determine the appropriate skin tone for each user based on the level of illumination.

2) MASK TECHNIQUE (BACKGROUND SUBTRACTION)

The mask technique involves image processing to subtract the background. The proposed system uses a mask to obtain only the hand object and ignores the rest of the background of the image.

3) BINARY IMAGE CONVERTER (BITWISE AND FILTER)

A binary image converter or bitwise AND filter is used to convert the image into white and black images. In this filter, a particular pixel is turned off (black pixel) or turned on (white pixel). If the pixel value is zero, it is turned off (black pixels). If the pixel value is greater than zero, it is turned on (white pixels). The proposed system applies this filter to the resulting images from the mask filter. The result of the filter is a binary image with noise.

4) OPENING FILTER

An opening filter was used to remove small noise around the hand object. The opening filter was an erosion filter, followed by a dilation filter.

5) DILATION FILTER

The proposed system uses another dilation filter to highlight the features of the hand object because the dilation filter joins the broken parts of the hand object in the image, which increases the area of the hand object.

6) HAND CONTOUR DETECTION

Hand contour detection is based on finding the largest contour in the entire image, which is the hand object, as shown in Fig.7(a).

The proposed system determines the center of the largest contour in the entire image, which is the center of the hand,

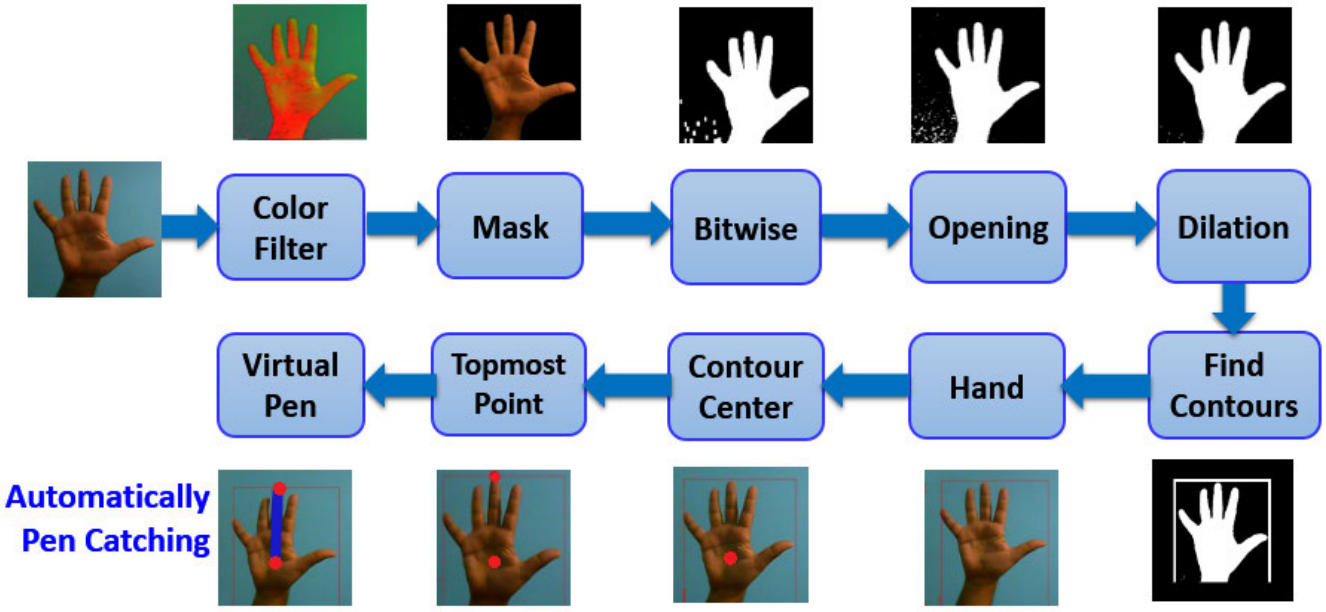


FIGURE 6. Steps for hand detection and the creation of a virtual pen.

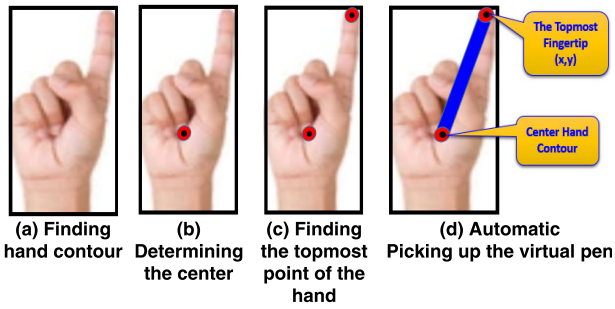


FIGURE 7. Steps for catching the virtual pen.

as shown in Fig.7 (b). It then finds the topmost point of the hand object, as shown in Fig.7(c), which is the fingertip that is the virtual pen top tip and is used to draw on the air. The virtual pen is automatically picked up by hand by determining the center and topmost point of the hand object when the hand is in front of the camera. The tips of the virtual pen were the tip of the fingertip and the center of the hand, as shown in Fig.7 (d).

B. HAND GESTURES CLASSIFICATION MODEL

The proposed solution to overcome the challenges of dynamic hand gesture recognition is a lightweight deep-learning CNN model. This CNN model is trained on an artificial image dataset that is tuned to hand gesture movements for drawing on air. There are two stages in this part: the training and prediction stages, as shown in Fig.8.

In the training stage, an artificial image dataset was created and then tuned to train the CNN model. In the prediction stage, the trained CNN model was used to predict the hand gestures. The following subsections provide an in-depth explanation of each stage.

1) ADAPTIVE TRAINING BY ARTIFICIAL IMAGES

In this study, the trained image dataset was created in two steps. First, a program was created to collect 300 trained images for each of the three hand gestures. These images were collected under different situations of on-air drawing in real time. Fig.9 shows the GUI ''graphical user interface'' of the program.

The proposed system uses only the upper part of the hand image because the upper part of the hand is the most important for distinguishing the three hand gestures (open index finger, open hand, and closed hand), as shown in Fig.10.

Then, the dimensions of the images were reduced to 64 for their height and width to decrease the image processing during hand prediction in real time. This leads to a fast response for IoT devices and is more efficient for gesture recognition.

The proposed system is based on an adaptive artificial image technique to overcome the challenges of dynamic hand gesture recognition. This technique is used to generate 40,000 artificial images for each hand gesture by using the images collected in the previous step. Each generated artificial image contains a hand gesture that is influenced by one of the previous challenges (rotation, zooming, clipping, shifting, and illumination) or a random combination of challenges, as shown in Fig.11.

The following subsections present the adaptive artificial image technique. Then, an in-depth explanation of how they have been tuned to overcome dynamic hand gesture challenges in the proposed on-air drawing system.

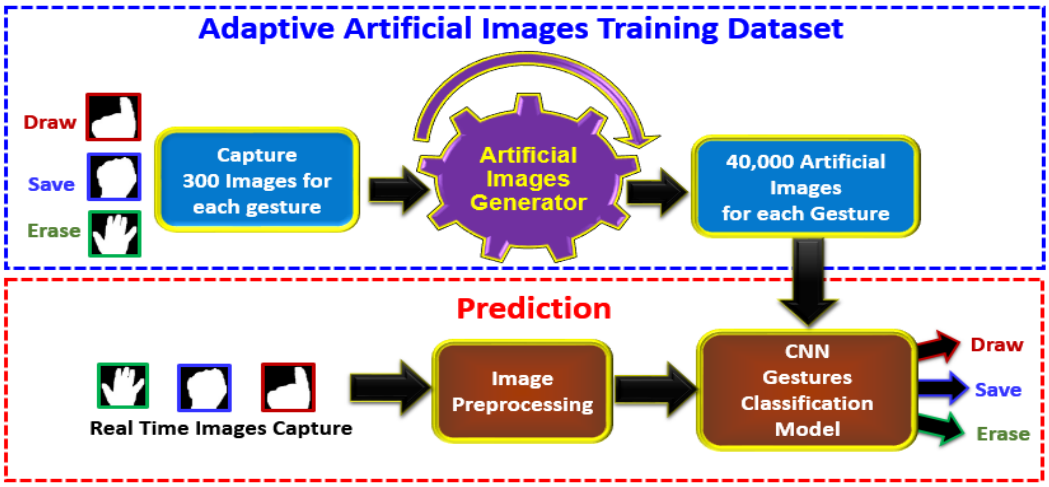


FIGURE 8. Steps for the training and prediction stages of hand gesture recognition.

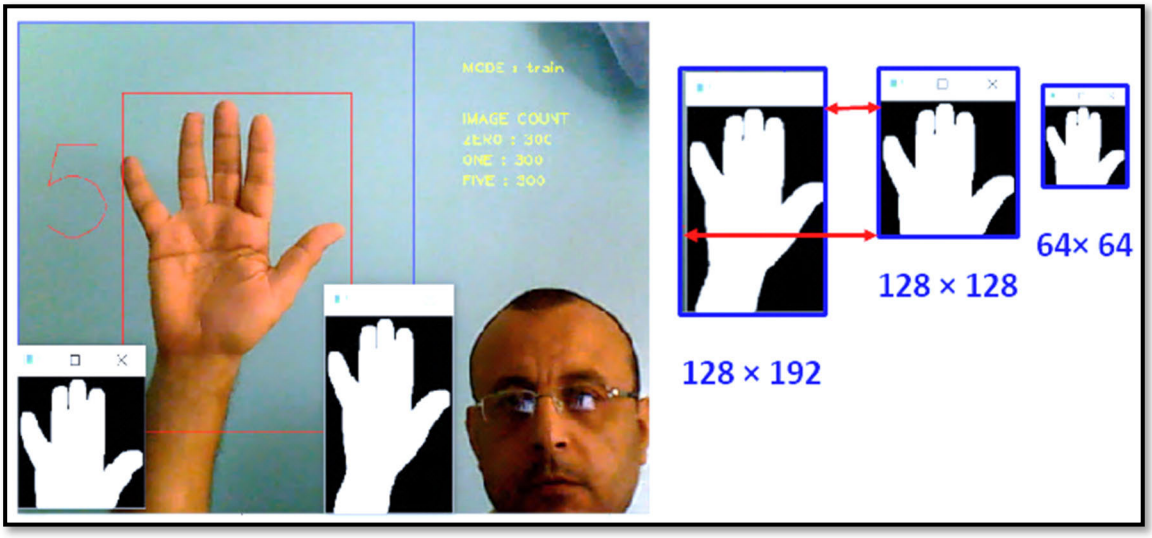


FIGURE 9. GUI of the program for collecting gestures image dataset.

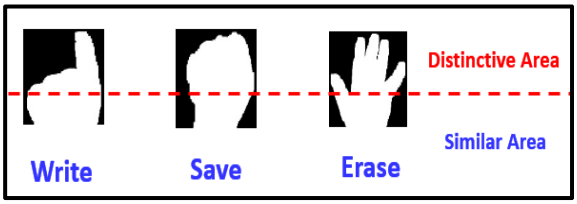


FIGURE 10. The upper part is more distinct than the lower part.

a: HAND ROTATION

Rotation of the hand while drawing on the air at an angle, right and left in front of the camera. This causes misrecognition of hand gestures because of the angle difference. Therefore, the artificial images were tuned to create images for each gesture. These adaptive artificial images are rotated at different angles from 30° to −30°, which is suitable for movement while drawing on air, as shown in Fig.12.

Therefore, after training the CNN on the rotated images, hand gestures can be recognized independently of hand orientation.

b: CAMERA ZOOMING IN OR OUT

Moving the hand near or away from the camera changes the size of the hand image captured by the camera. When the hand is near the camera, the captured image is enlarged, and vice versa, as shown in Fig.13.

This causes misclassification of hand gestures because of the difference in the hand image size. Therefore, the artificial image generator was tuned to create images with different zooming in and out based on the most remote distance between the camera and the hand. Therefore, after training the

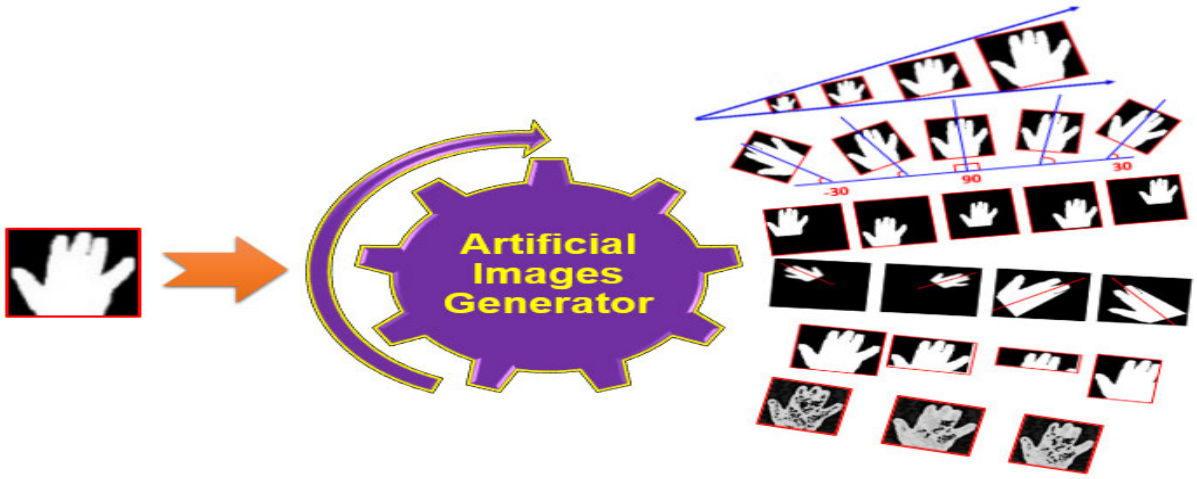


FIGURE 11. Adaptive artificial images generator.

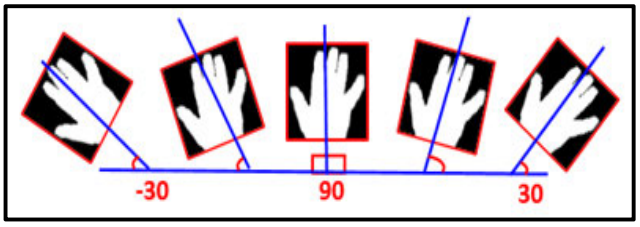


FIGURE 12. Adaptive rotation of artificial images for on-air drawing.

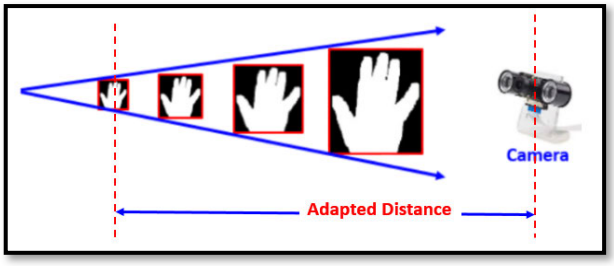


FIGURE 13. Effects of camera zoom and adapted distance.

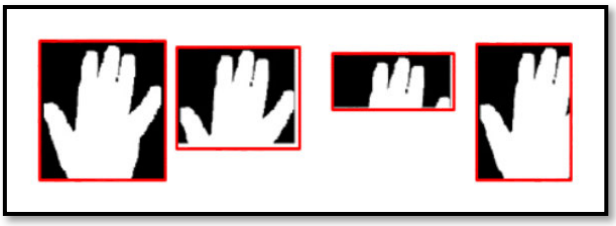


FIGURE 14. On-air drawing and camera angle effects.

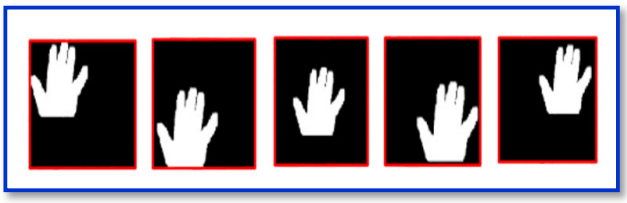


FIGURE 15. On-air drawing and hand location shifting.

CNN on gesture images of different sizes, hand gestures can be recognized independently of the hand size or the distance between the hand and camera.

c: IMAGE CLIPPING

Moving the hand out of the angle of view of the camera cuts off parts of the hand image, so that the captured hand image from the camera is clipped, as shown in Fig. 14.

This causes misclassification of hand gestures because of the cropped image of the hand. Therefore, the artificial image generator was tuned to create clipped images, some parts of which were randomly clipped. Therefore, after training the CNN on the clipped images, hand gestures can be recognized based on part of the image.

d: IMAGE SHIFTING HORIZONTAL AND VERTICAL

In the on-air drawing, the hand moves up, down, left, or right away from the center of the lens of the camera. This movement causes a change in the location of the hand in the captured image, as shown in Fig.15.

This causes misclassification of hand gestures due to the shifted hand location. Therefore, the artificial images generator was tuned to create images of a hand with randomly shifted locations. Therefore, after training the CNN on the shifted images, hand gestures can be recognized independently of the location of the hand.

e: ILLUMINATION

In the air drawing process, the hand moves freely in the three dimensions during drawing. This movement causes differences in the intensity of illumination on some parts of the captured image, as shown in Fig.16.

FIGURE 16. On-air drawing, and illumination effect.

FIGURE 17. Combination of random challenges.

This causes misclassification of hand gestures because of differences in the level of illumination. Therefore, the artificial image generator was tuned to create images of the hand with a random level of illumination. Therefore, after training the CNN on these images, hand gestures can be recognized using different illuminations.

f: RANDOM CHALLENGES COMBINATION

The previous challenges of dynamic hand gesture recognition can come together at the same time or come with different combinations, as shown in Fig.17. Fig. 17 (a) shows a combination of rotation and shifting. Fig.17 (b) shows a combination of zooming in, rotation, and clipping. The random combination challenge is the biggest challenge that leads to more errors. Therefore, the artificial image generator was tuned to create images with different random combinations of the previous challenges. Therefore, after training the CNN on these images, the CNN can classify hand gestures if these challenges come together with different combinations.

Finally, the lightweight CNN with the architecture shown in Fig.18 was trained on 100,000 images and tested on 20,000 images. The proposed CNN network consists of input and output layers composed of multiple hidden layers, including convolution, pooling, and activation layers. The input layer was a 64 × 64 dimensional image. The two convolution stages consisted of three layers containing 64, 128, and 192 channels for feature extraction. The ReLU activation function was used for all cases except the output layer. A dropout rate of 0.5 was used to reduce the possibility of overfitting during training. Adam was used as an optimizer with a learning rate of 0.0001 and categorical cross-entropy as a loss function. The softmax layer was used to convert the output of the fully connected layer into three gesture classes (open hand, closed hand, or open index finger).

2) MODEL PREDICTION

In real time, a hand-gesture image is captured by a camera. Then, the image goes to the processing stage to make its properties (size and black background color) similar to the previously trained images. Finally, the trained model predicts and classifies the image as one of the three hand gestures based on the training parameters of the model. The accuracy of the proposed lightweight CNN gesture classification architecture was 98.8%. This accuracy is satisfactory with a lightweight CNN architecture that is suitable for running on IoT device capabilities with a fast response time.

C. KALMAN FILTER

This work proposes a Kalman filter to correct the drawn line path on the air by finding the nearest correct location of the virtual pen tip in the air. It has been used in two dimensions once for the X coordinate and the other for the Y coordinate. The Kalman filter is based on a Gaussian distribution GD. This is true in a real environment where there is no pure signal from the sensors. The readout produced by any sensor is not accurate, but has an error rate that depends on the accuracy of

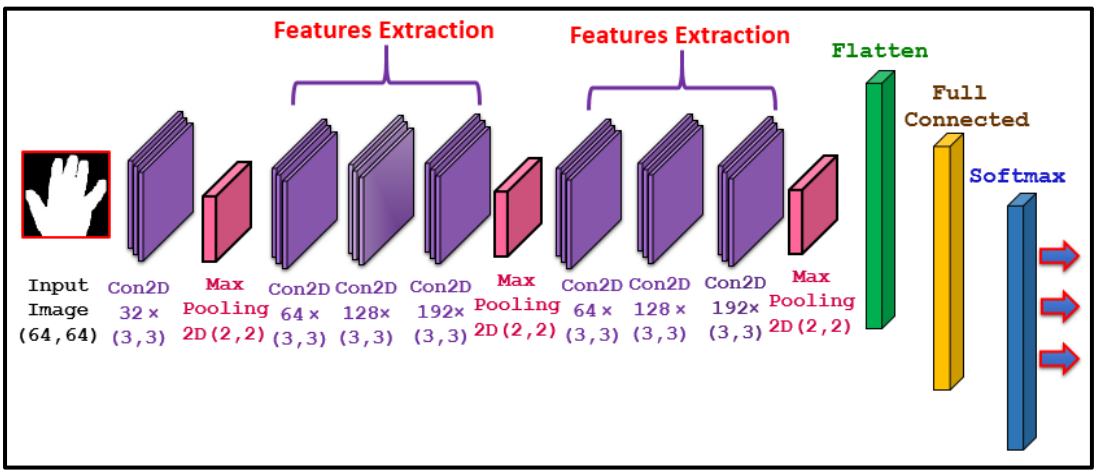


FIGURE 18. Hand gestures recognition CNN.

the sensor. A Gaussian distribution is a continuous probability distribution that is completely described by two parameters: the mean (μ) and variance ($\sigma 2$). The Gaussian distribution formula is expressed as Equation (1):

$$f(x,\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(x-\mu)^2/\sigma^2} \quad (1)$$

For example, if we obtain the Y coordinate of the virtual pen tip location 30 times per second, and each time it returned a value between 17 and 23. Therefore, based on the Gaussian distribution, as shown in Fig.19, all the produced readouts are centered around 20.

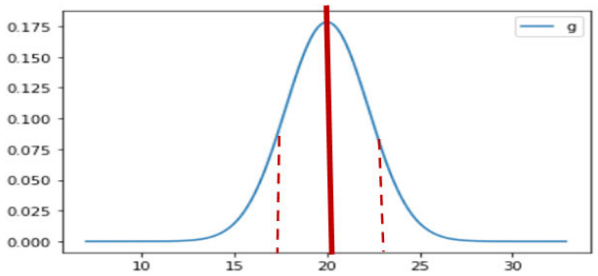


FIGURE 19. Gaussian distribution GD = (μ = 20, σ 2 = 3).

Therefore, the real Y coordinate of the hand location should be very confident close to somewhere, to 20.

1) HOW DOES KALMAN FILTER WORK

A Kalman filter is used to smooth the noise of zigzagging writing on air based on the location of the virtual pen tip detected in the previous frames. The Kalman filter process consists of a prediction step and an updated step, as shown in Fig.20.

As shown in the previous figure, the Kalman parameters are represented by a Gaussian distribution. The Kalman filter algorithm repeats the prediction step and updated step for each new input location, such as the following steps:

The prediction step:

The new location of the virtual pen tip is predicted based on the previous measurement location and movement step, such as in Equation (2):

$$\textbf{Prediction Location estimation} = \textbf{Previous location} + \textbf{movement step} \quad (2)$$

However, the location and movement steps are based on a Gaussian distribution, which has a mean and variance (error rate). Therefore, the new location is the summation of two Gaussians, as shown in Equation (3).

$$\begin{aligned} \mathbf{GD}(\boldsymbol{\mu}\mathbf{1}, \mathbf{V1}) &= \mathbf{GD}(\boldsymbol{\mu}\mathbf{i}, \mathbf{Vi}) + \mathbf{GD}(\boldsymbol{\mu}\mathbf{m}, \mathbf{Vm}) \\ &= \mathbf{GD}(\boldsymbol{\mu}\mathbf{i} + \boldsymbol{\mu}\mathbf{m}, \mathbf{Vi} + \mathbf{Vm}) \end{aligned} \quad (3)$$

where μi and Vi are the mean and variance (error rate) of the previous location, respectively. where μm and Vm are the mean and variance (error rate) of the movement step, respectively. The prediction location is a Gaussian distribution with the mean that equals (μi +μm) and the variance that equals (Vi + Vm).

The updated step:

The updated step is used to correct the location of the virtual pen tip by simply multiplying the two Gaussian distributions, the prediction location estimation GD (μ1, V1), and the measurement or current location GD (μ2, V2). The result of the multiplication is Gaussian of optimal location estimation GD (μ, V), and its mean is the nearest position of the correct location of the virtual pen tip. Then, the optimal location estimation GD (μ, V) is used in the next prediction step.

2) KALMAN FILTER PARAMETERS TUNING

In the Kalman filter, some of its parameters should be tuned according to the required application. For example, using a Kalman filter to predict the location of a space rocket in space is different from Kalman's prediction of the location of a car on the street. This is the difference in velocity between the rocket and car, as well as the difference in the surrounding environment. Therefore, to use the Kalman filter to predict and correct the drawn line path on the air, its parameters should be tuned. Fig.21 shows the control loop of the Kalman filter and its two main tuning parameters.

The first parameter is the variance of the Gaussian distribution for the movement step that controls the allowable level of the zigzagging of the air drawing. The second parameter is the mean of the Gaussian distribution for the movement step, which controls the velocity of the air drawing. These two parameters strongly affect the shape of the drawn symbols when drawing on air, which leads to the misclassification of symbols.

3) ADJUST THE ZIGZAGGING FOR AIR DRAWING

The variance of the movement step controls the allowable level of zigzagging. Several variance values were tested while maintaining a constant mean. Fig.22 shows the effect of the Kalman filter on the incoming data to obtain the optimal path of the air drawing path with different variances at a constant mean for the movement step.

The horizontal axis represents time. The vertical axis represents the prediction locations, measurement locations, and optimal locations with different colors in only one dimension for simplification (Y-axis). From Fig.22, we derive the important notes as follows:

1- In the case of low variance, the zigzagging of the optimal path location is reduced, and this appears to be good, as shown in Fig.22(a). However, strongly killing the zigzagging leads to a distortion in the shape of the drawn symbols on the air, especially the symbols that are characterized by curves.

2- When the variance increases, the zigzagging of the optimal path location increases, which leads to a distortion in the shape of the symbols, as shown in Fig.22(c).

3- Therefore, it is necessary to choose an appropriate average value that reduces the zigzagging of the optimal location

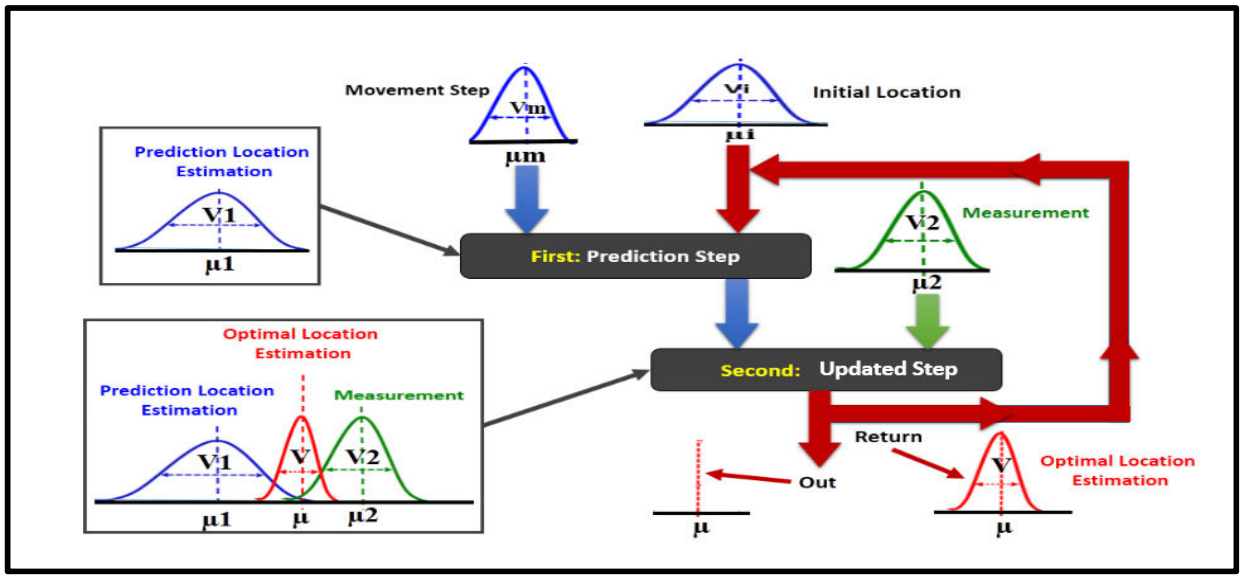


FIGURE 20. The sequence of Kalman filter algorithm.

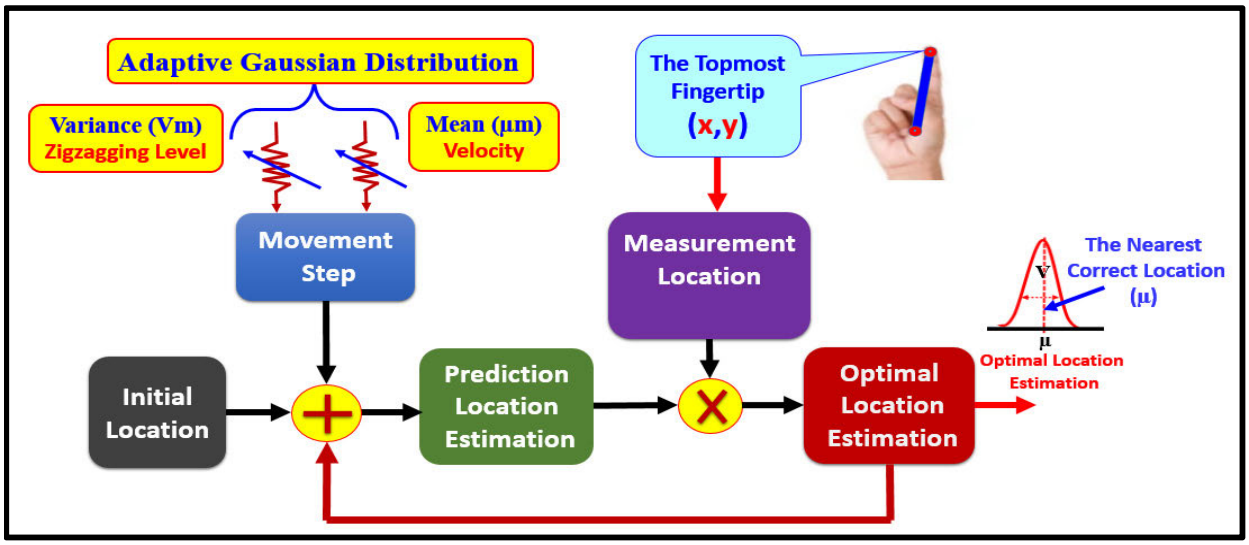


FIGURE 21. Kalman filter control loop and its two main tuning parameters.

and preserves the well shape of the symbols, as shown in Fig.22 (b).

4) ADJUST THE VELOCITY OF AIR DRAWING

The mean of the movement step controlled the velocity of the air drawing. To obtain an acceptable velocity, several mean values were tested while maintaining a constant variance. Fig.23 shows the effect of the Kalman filter on the incoming data to obtain the optimal velocity of drawing on air with different means at constant variance for the movement step.

The horizontal axis represents time. The vertical axis represents the prediction locations, measurement locations, and optimal locations with different colors in only one dimension for simplification (Y-axis). From Fig.23, we derive the important notes as follows:

1. When the value of the step length is negative, the direction of movement of the optimal location (moving down with time) is opposite to the direction of the measured movement (moving up with time), which is, of course, not desirable in drawing on air, as shown in Fig.23(a).

2- When the value of the step length is positive, the optimum location movement velocity is greater than the measured movement velocity. As shown in Fig.23(c), the optimal location tended to be higher than the measured value, which is undesirable for drawing on air.

3- Therefore, it is necessary to choose an appropriate step length value that does not move away from the right track of the movement, as shown in Fig.23 (b).

D. AUTHENTICATION LOGIN AND VERIFICATION

This section contains three stages. The following sections will explain in detail the proposed method of hand-drawn symbols password and the three stages of authentication login and verification.

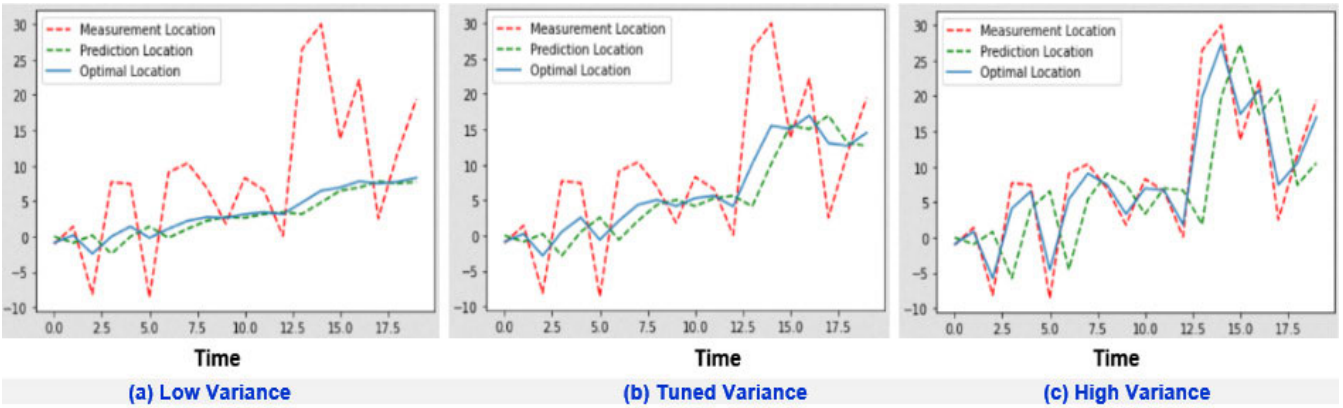


FIGURE 22. Kalman filter with different variances at a constant mean for movement step.

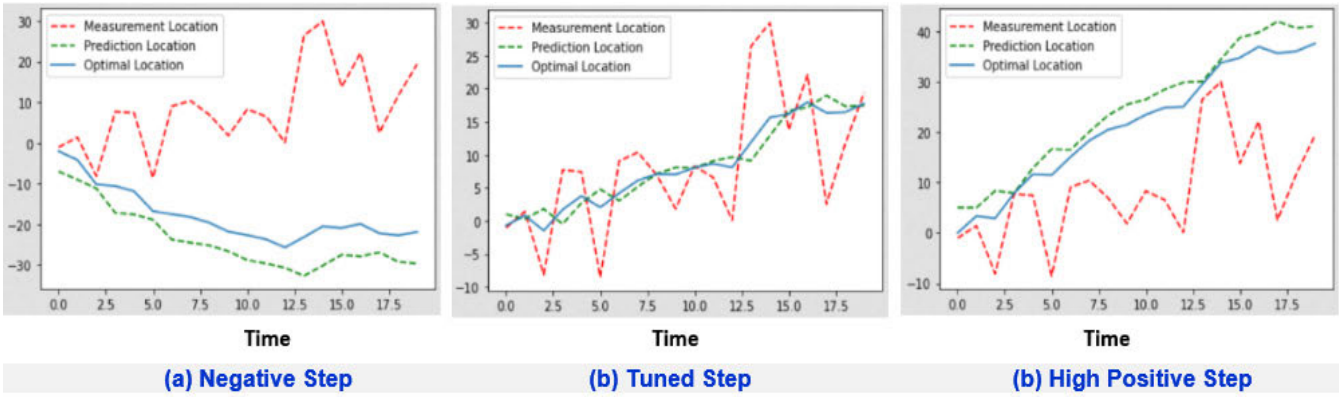


FIGURE 23. Kalman filter with different mean at a constant variance for movement step.

1) HAND-DRAWN DOODLES PASSWORD

This study proposes an on-air predefined drawing graphical symbol password. These graphic symbols were obtained from Google Quick Draw project. This is a unique data set that can help developers train new neural networks that help researchers to see patterns in how people draw around the world. The Quick Draw dataset is a collection of 50 million drawings across 345 categories, contributed by users of the Quick, Draw! project [44]. However, not all 345 categories of graphical symbols are suitable for authentication because some categories are complex or similar. Therefore, 47 symbols were proposed and, of course, they could be increased in future work. Symbols were chosen for three reasons.

1- Symbols should be suitable for the authentication process and should not contain many details to be easy to draw and remember. Therefore, three levels of symbols (easy, medium, or complex) were selected. Thus, it can be easily drawn for most users and is suitable for all ages and the ability to draw. Such as in Fig.24. Ten easy symbols, Twenty-nine medium symbols and eight complex symbols.

2- Symbols are varied in different fields such as sports, medicine, transportation, animals, music, etc. Therefore, they are suitable for users in most fields and are difficult to predict by attackers.

3- Each symbol has been chosen to be distinctive and not close in detail with the rest of the symbols. This is important for obtaining more verification accuracy and avoiding similarity problems. Therefore, it is easy to classify them in the verification stage using a lightweight CNN. Therefore, the proposed lightweight CNN model achieved acceptable classification accuracy and a fast response time. This is suitable for IoT devices with limited computational ability and small memory requirements.

a: ADVANTAGES OF USING GOOGLE DRAW

The goal of authentication on the device is to prevent unauthorized access. This requires that the authentication mechanism be secured against the associated threat models. However, regardless of how the system is secured, it will not be effective if it is difficult to use and is not approved by users. Thus, for the authentication method to be widely accepted, security and usability must be achieved, as shown in Fig.25.

(i) USABILITY

1- Google Quick Draw dataset contains several thousand ways to draw at different levels of complexity because the Google Quick Draw project has collected many methods

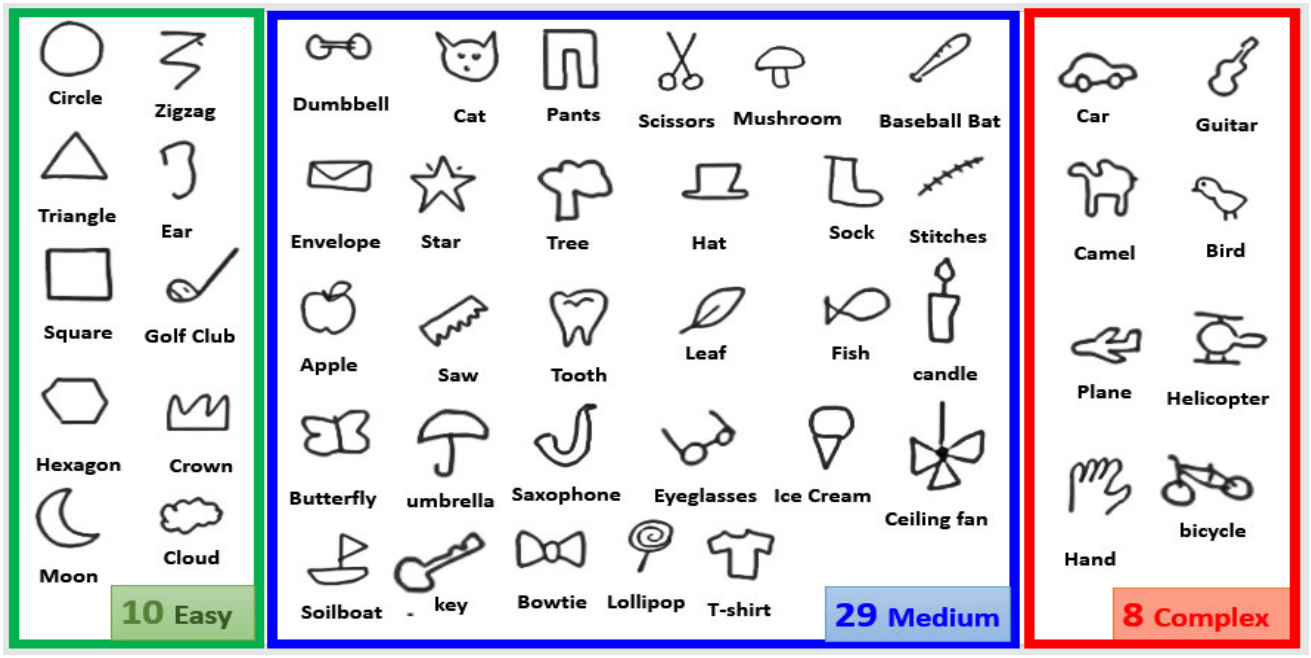


FIGURE 24. The proposed authentication symbols groups.

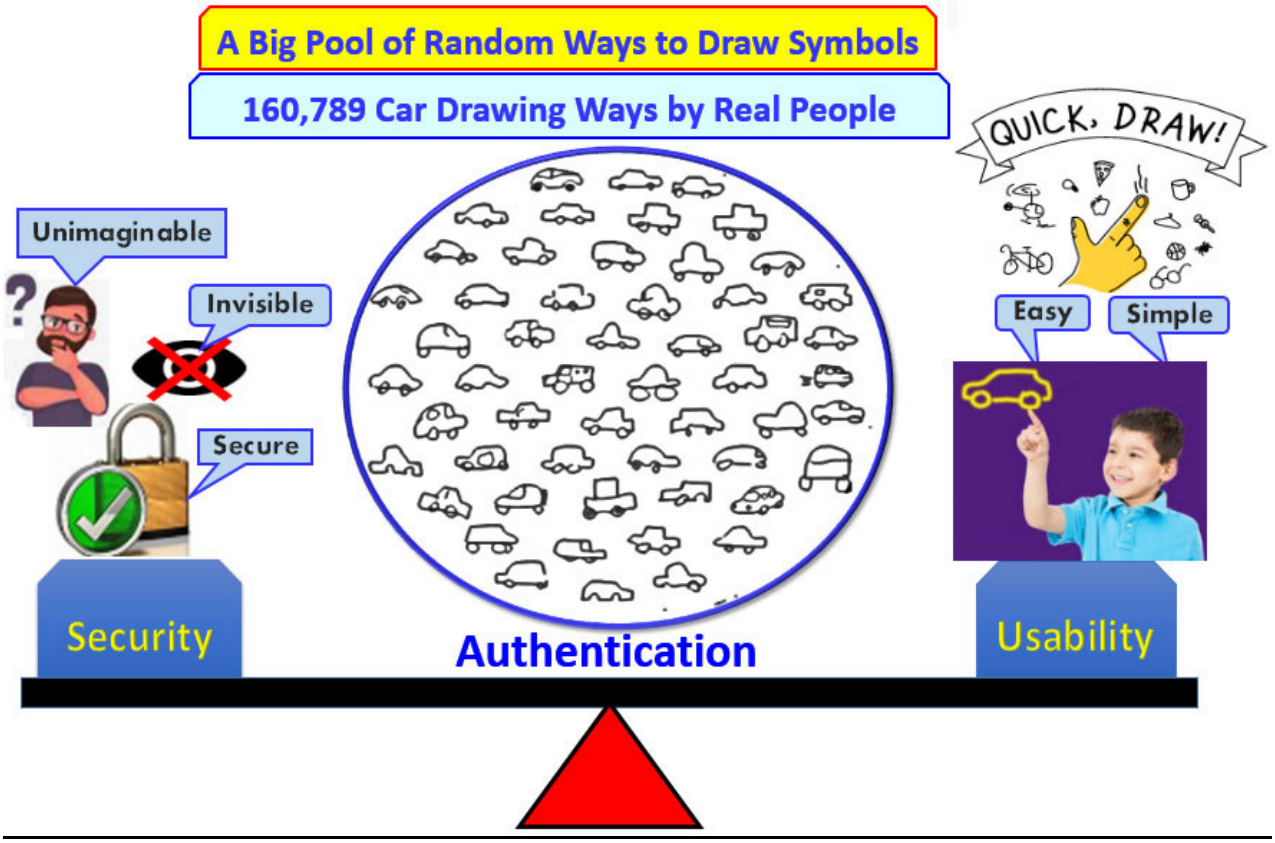


FIGURE 25. The advantages the proposed method.

for drawing symbols from 15 million users worldwide. Of course, each user will find many easy ways to draw each symbol. For example, in the Google Quick Draw project, the dumbbell symbol has 136062 ways to draw it. Fig.26 shows only five ways to draw a dumbbell in different ways, from easy to complex.

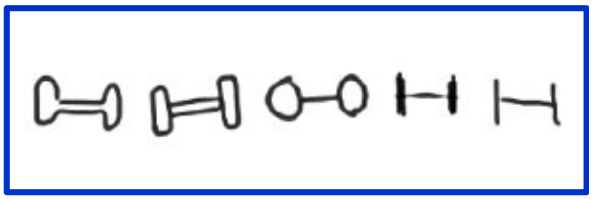


FIGURE 26. Five ways to draw a dumbbell.

The proposed CNN was trained in all different ways to draw the dumbbell. Thus, the CNN can identify dumbbells by drawing a shape close to one of the shapes that it has already trained on. This allows each user to choose an easy and comfortable way for him and pass the hand-drawn symbol to the CNN model to be recognized.

2- The user is free to draw the symbol on air without any special restrictions in specific orientation, size, or grid, as in the grid pattern password.

3- The hand-drawn symbol passwords are easy to remember and memorize, especially in the world of the Internet of Things, where there are many smart things; therefore, the user needs to remember a large number of passwords because the user can easily link each symbol with a device in a private and secret relationship, such as what will be discussed in the following section.

(ii) SECURITY

1- In all authentication methods, the user logins, in the same way, every time login. For example, in the traditional 4-digits PIN authentication method, the user login with the same 4-digits PIN every time login. This means that the user repeats his/her PIN every time they log in. However, in the proposed method, the user can log in different ways of drawing the same symbol every time login. This means that the user does not repeat the method of drawing symbols every time login.

2- The proposed method is more secure because the graphic password is stronger than the password of the traditional method 4-digits PIN such as what will be shown in the security evaluation section.

b: ADVANTAGES OF DRAWING ON THE AIR

1- On-air drawing, without touching anything, is recommended at the time of the spread of epidemics through touch. For example, the current time of the spread of the COVID-19.
2- On-air drawing increases security because on-air drawing is not visible.

2) FIRST STAGE: DRAWN AUTHENTICATION SYMBOLS

The on-air drawing of the password symbols was performed using a virtual pen. The processes of drawing, erasing, and saving using hand gestures are illustrated in Fig.27.

The raised index finger is used to draw, the closed hand is used to save, and the open hand is used to erase. The proposed length of the hand-drawn symbol password comprises three symbols for the authentication key. The user enters each symbol in three steps. First, the user raises his/her index finger to draw a symbol. Second, the user closes his/her hand for two seconds to save the symbol. Third, the user opens his hand for two seconds to erase the symbol to draw the next symbol.

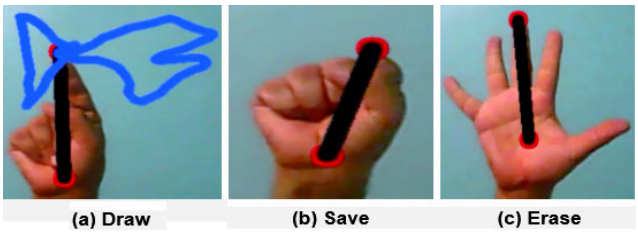


FIGURE 27. The three hand gestures of on-air drawing.

a: USER REGISTRATION STEPS

First, the user should choose three symbols from the previous 47 symbols. Second, the user should choose one or more appropriate ways to draw each symbol. Third, the user should be trained to draw the symbol several times to ensure that the symbols can be drawn in different ways. Through the experiment, five times was sufficient for most participants. Fourth, when the user chooses symbols for authentication in the IoT world, there are many smart devices. The user should set confidentiality and privacy a relationship between his symbols for each password to facilitate memorization and remembering them. For example, Fig.28 shows the three symbols used for smart refrigerator authentication.

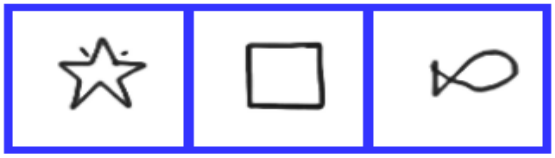


FIGURE 28. Smart refrigerator password.

The first symbol: ''star'' is the user's logo which indicates to the user. The second symbol: ''rectangle'' is the device's logo which indicates to the device because refrigerator is a rectangular in shape. The third symbol: is ''fish'' which indicates to the relationship between the user and the refrigerator. The relationship is: ''The user's love for eating fish''

b: ADVANTAGES OF DOODLES PASSWORDS FOR MANY IoT DEVICES

First, password symbols are easy to memorize and remember where there are a large number of devices in the IoT world. This is because the user can easily link each symbol with a device in a private and secret relationship. Fig.29 shows the authentication passwords for smart TV, smart door, smart piano, and smart car.

1- The symbols are easy to memorize and remember because the graphical shape of the symbol is linked to the device based on the user.

2- The first symbol indicates the user's logo, which is repeated for every password. In the proposed method, repetition does not affect security because each time the symbol

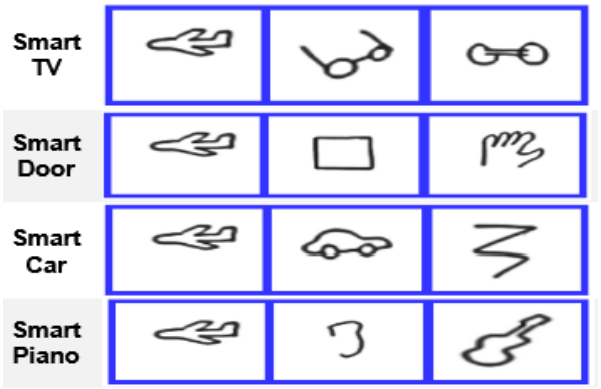


FIGURE 29. Authentication symbols passwords for many devices.

can be drawn in different ways, which means that each time the different movements in the air make it difficult for the attacker to guess the shape.

Second, the proposed method is characterized by a small amount of storage space for passwords because only the label of each class or symbol is stored. The proposed method does not store each symbol as an image but stores each symbol class label or number. This means that each password consists of three symbols stored in three numbers so that we do not need additional storage than the current traditional 4-digits PIN.

3) SECOND STAGE: AUTHENTICATION KEYS EXTRACTION

In real time, the user draws a password symbol. The authentication symbol image is extracted and processed. Finally, the authentication symbol image is input to the CNN model to verify it, as shown in Fig.30.

The keys or symbols extraction stage consists of several filters to obtain the symbol only from the entire image, as in the previous figure. First, the grayscale filter converts images into grayscale (one color channel, such as a trained image dataset). Second, the threshold filter converts the grayscale image into a binary image. Third, the dilation filter increases the symbol object area in the image. Fourth, the largest contour in the entire image is extracted, which is the symbol. Finally, in the preprocessing stage, the size and background color of the symbol images were adjusted to be the same as the size and background color of the trained image dataset.

4) THIRD STAGE: AUTHENTICATION VERIFICATION

Symbol verification is based on lightweight CNN deep learning models. The CNN verification model was trained on a sub-dataset of the Google Quick Draw hand-drawn dataset. This sub-dataset for 47 symbols contains 100,000 for each symbol. Each symbol image is a 28 $\times$ 28 grayscale image. The lightweight CNN with the architecture shown in Fig.31 classifies the on-air drawing 47 symbols.

The input layer was a 28$\times$ 28-dimensional image. The three convolution layers contained 16, 32, and 64 channels for feature extraction. The flattened layer converts the data into a 1-dimensional array for inputting it to the next layer. The dense layer is a deeply connected neural network layer. The final dense layer converts the output of the fully connected layer into 47 classes. The CNN was trained on 95% of the entire dataset and tested on the remaining 5%. The accuracy of the proposed lightweight CNN symbol classification architecture was 96%. This accuracy is satisfactory with a lightweight CNN architecture and a fast response for authentication operations. The previous research by Tsai *et al.* [45] who used Google Quick Draw dataset achieves was 85% accuracy.

IV. MATERIALS AND METHODS

This section presents the general methods used in this study. This contains the study objectives, participants, prototype development, resources required, experiments, and experimental procedures. The experimental results were used to evaluate the proposed authentication method.

A. STUDY OBJECTIVES

The main objective is to verify that the proposed authentication method is acceptable based on the following criteria:

1- Usability.
2- Security.
3- Authentication Time

B. PARTICIPANTS

Participants were 20 healthy users who participated in the study. The participants were chosen from different age ranges and education. Their ages ranged from 10 to 40 years. The samples were carefully selected from different ages and abilities to be representative of the community. It was statistically tested according to the normal distribution, which is based on the Shapiro–Wilk test for small samples ($<$ 50) using the Statistical Package for the Social Sciences (SPSS) program.

C. PROCEDURES

First, the proposed authentication method was introduced by watching a video. Second, the Google Quick Draw Project was introduced. Then, explanations of how graphical symbols were chosen for the experiment and different ways to draw symbols have been shown to participants on the Google Quick Draw project website. Third, participants were asked to choose ten graphical passwords for ten smart devices: smart TV, mobile, car, door, refrigerator, conditioning, electric fireplace, vacuum cleaner, wardrobe, and money safe box. Each password contained three symbols. The first symbol indicates the user. The second symbol indicates the device. The third symbol indicates the privacy relationship between the user and the device. Fourth, the participants were trained on their graphical passwords and then registered. Finally, the participants were asked to log using their graphical passwords, and authentication success, failure, and authentication time were recorded.

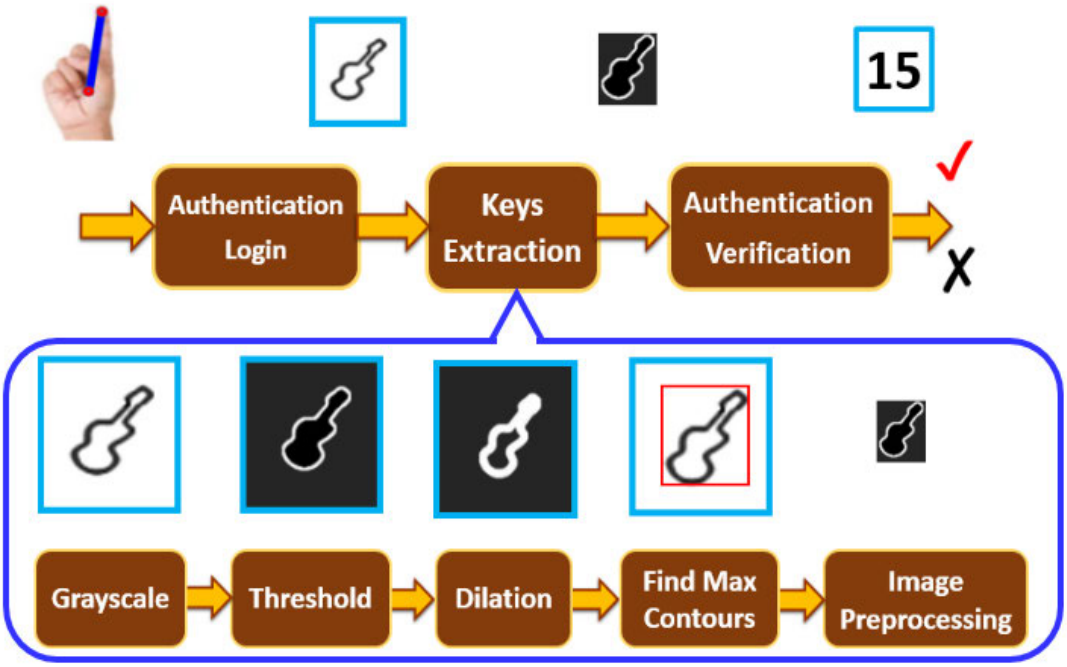


FIGURE 30. Symbol extraction stage filters.

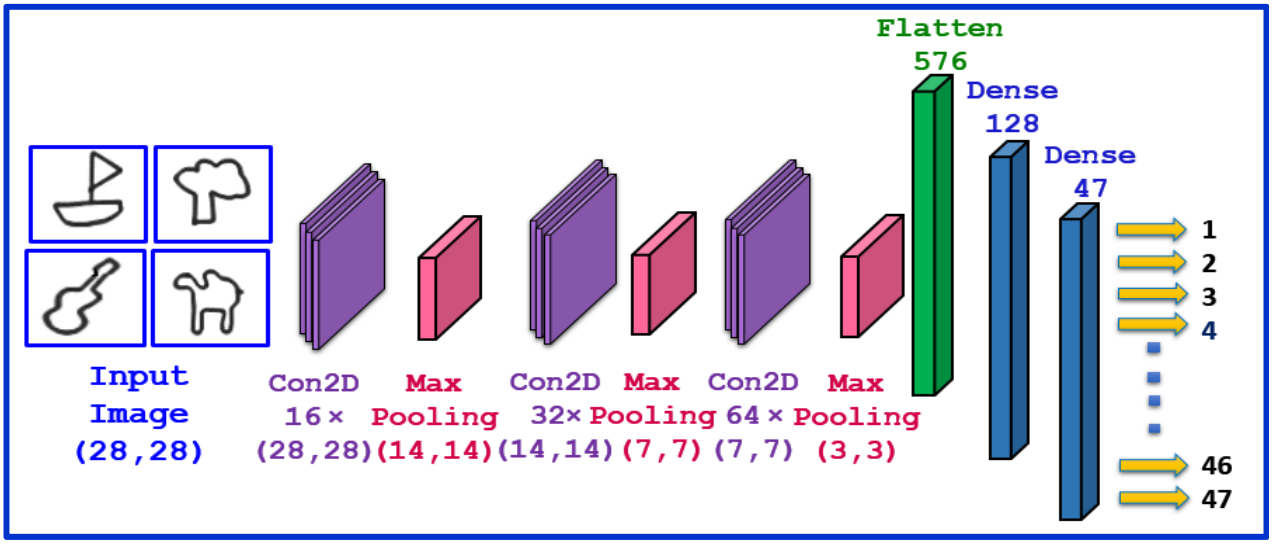


FIGURE 31. The lightweight CNN for Symbols verification.

D. HARDWARE (DESIGN REQUIREMENTS)

The Raspberry Pi3 board is an example of an IoT device with 1.2 GHz CPU speed and 1 G byte RAM. The operating system is Raspbian, which is a Linux distribution. Raspberry Pi camera for video capture.

E. PROTOTYPE DEVELOPMENT

The proposed lightweight CNN networks for hand gestures and graphical symbol classification models were implemented, trained, and tested in TensorFlow on the Colab Google platform. The trained TensorFlow models were converted to TensorFlow Lite models to run on the Raspberry Pi board as an example of an IoT device. The GUI graphical user interface and Kalman filter algorithm were implemented using the Python programming language. Computer vision filters for hand detection were implemented using the OpenCV library (Open Source Computer Vision Library).

F. EXPERIMENTAL DESIGN

Experiments were conducted in a comfortable room. The participants were seated in a comfortable chair a meter away from the screen and the camera. The participants were logged

using graphical passwords. They entered each symbol by symbols in three steps. First, the user raises his/her index finger to draw a symbol. Second, the user closes his/her hand for two seconds to save the symbol. Third, the user opens his hand for two seconds to erase to draw the next symbol.

G. EXPERIMENTAL RESULTS

Table 1 lists the data obtained from prototype experiments.

TABLE 1. The experiment results.

Users	1	2	3	3	5	6	7	8	9	10
User_1	44	38	41	48	45	24	42	28	26	40
User_2	48	28	24	43	32	36	55	51	27	38
User_3	35	43	29	41	37	55	56	41	40	28
User_4	25	51	45	54	35	26	36	52	48	45
User_5	28	39	33	41	45	28	33	43	36	53
User_6	48	44	43	44	33	39	60	28	32	38
User_8	51	43	28	36	42	30	37	27	48	37
User_9	44	41	27	51	29	37	50	48	32	52
User_10	42	37	41	36	43	30	48	41	57	41
User_11	49	50	60	41`	36	47	44	45	27	46
User_12	32	37	38	38	45	38	35	42	31	26
User_13	35	33	46	25	41	36	44	53	39	35
User_14	37	45	45	37	33	42	31	38	49	40
User_15	26	50	32	46	31	29	35	54	38	50
User_16	32	55	53	38	53	25	47	33	27	45
User_17	42	42	24	42	46	37	31	42	55	37
User_18	58	25	38	43	47	35	48	41	60	37
User_19	36	35	37	48	44	45	37	34	36	34
User_20	31	37	30	44	42	57	42	49	30	34

1- The red cells indicate the failed attempts of the users, and the remaining cells are successful attempts.
2- Values in the cells represent the time in seconds to complete the task
3- Some Statistical information showing the time spent on the task to draw three symbols for authentication.

- Average time for successful attempts (40 s).
- Median time for successful attempts (39 s)
- Mode time for successful attempts (37 s).
- Maximum time for successful attempts (60 s).
- Minimum time for successful attempts (24 s).

V. EVALUATION

In this research, the usability and security of the on-air drawing graphical symbol authentication method were evaluated. The usability evaluation is based on the ISO 9241-11:2018 usability standards model [46], [47]. The security evaluation is based on two threats related to the IoT device authentication method derived from Elshenaway and Guirguis [47]. The following subsections briefly present the two evaluation methods.

A. USABILITY EVALUATION

The ISO - 9241-11 ISO 9241-11:2018 usability standards model recommends that usability metrics include accuracy, efficiency, and user satisfaction [47].

1) ACCURACY

In this study, accuracy is the percentage of the successful number of logins divided by the total number of logins for all users using the proposed authentication method. Accordingly, the accuracy of the proposed authentication method is calculated as shown in Equation (4).

$$\textbf{Aaccuracy} = \frac{\textbf{Number of successful logins for all users}}{\textbf{Total number of logins for all users}} \times 100 \quad (4)$$

In this work, to calculate the accuracy, 20 users attempt 10 logins with different passwords every time.

2) EFFICIENCY

Efficiency is measured in terms of authentication time. Thus, the efficiency can be calculated as the percentage of the total time in seconds of successful logins for all users divided by the total time of logins for all users. Accordingly, the efficiency of the proposed authentication method is calculated as shown in Equation (5).

$$\textbf{Efficiency} = \frac{\textbf{Total time of successful logins of all users}}{\textbf{Total time of logins of all users}} \times 100 \quad (5)$$

3) USER SATISFACTION

The ISO-9241 standard defines user satisfaction with the product as ''comfort and relevance of application,'' and user satisfaction is measured using questionnaires. In this study, a questionnaire was distributed to 20 users after the experiment to obtain feedback on the proposed authentication method. The questionnaire consists of three questions based on a Likert scale questionnaire with five levels of user satisfaction, which are on a scale of 1and 5 (1 = strongly disagree, disagree = 2, neutral = 3, agree = 4, and 5 = strongly agree) such as shown in Fig.32.

B. SECURITY EVALUATION

Security evaluation considers two threats related to IoT devices. These are physical observation threats and guessing threats. The following subsections briefly present these two threats [47].

1) GUESSING THREAT

In this scenario, an attacker attempts to guess the authentication password to the login. The quality or security of the authentication method is based on password strength. The main challenge with the strength of the password is how easy (or how hard) it can be ''guessed'' by an attacker. The password strength evaluation of the proposed method is based on electronic authentication guidelines for the National Institute of Standards and Technology (NIST) [48]. NIST estimates password strength by measuring password entropy. Entropy essentially measures the number of prognoses that an attacker needs to predict. The password entropy is calculated as shown in Equation (6).

$$\textbf{Password Entropy} = \textbf{Log}_2\, \textbf{S}^{\textbf{L}} \quad (6)$$

where **L** is the password length. Where **S** is the size of possible symbols. Therefore, the password of the proposed

No.	Questions	Disagree Strongly	Disagree	Neutral	Agree	Strongly Agree
1	"On-air drawing" is easy use?					
2	"Hand gestures" are easy to control on-air drawing?					
3	"On-air drawing graphical symbols authentication" is easy use?					

FIGURE 32. The three questions for user satisfaction questionnaire.

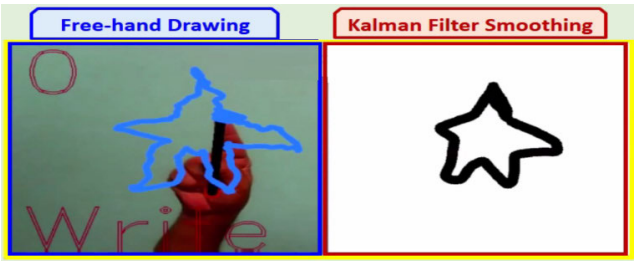


FIGURE 33. Kalman filter to smooth hand-drawn symbols.

method is evaluated by comparing it with the traditional PIN 4-digits.

2) PHYSICAL OBSERVATION THREAT

Here, the attacker learns authentication credentials by monitoring the victim (during entry) that are entered into the authentication system. This type of attack is called a ''shoulder-surfing attack'' or a ''display attack.''

VI. RESULTS AND DISCUSSION

A. ACCURACY

The results show that the overall accuracy of the prototype is 95%, which can be explained as follows.

1- The use of a Kalman filter to correct the hand-drawn path and smooth the zigzag, which leads to an improvement in the drawing of symbols, which facilitates the process of identifying symbols by the CNN during the authentication verification process, as shown in Fig.33.

2- Good and fast architecture of the CNN for authentication verification, especially that it had a high accuracy of 96%.

B. EFFICIENCY

The results show that the overall efficiency of the prototype is 94%, which can be explained as follows.

1- Efficiency and facility of using freehand gestures in on-air drawing and controlling the authentication process, which helps users succeed in the registration process in a short time.

2- Good architecture of the CNN for hand gesture classification and fast response was in short real-time with a high accuracy of 98.8%.

C. USER SATISFACTION

1 - The first question concerns the ease of on-air drawing. Fig.34 shows the percentage of the strongly agreed response, which is 40%, the neutral response is 25%, and the agreed response is 20%.

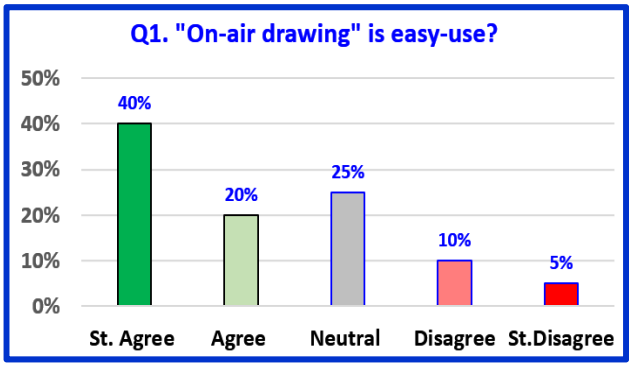


FIGURE 34. Results of the first question.

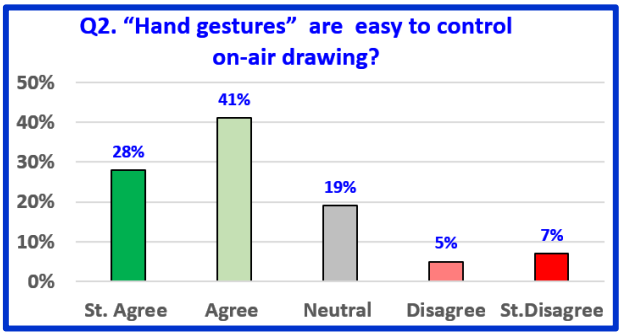


FIGURE 35. Results of the second question.

Overall, this indicates the ease of on-air drawing. All participants also agreed to use ''drawing on the air'' as a good method in case of the spread of diseases by touching, as is the case with the spread of COVID-19.

2 - The second question concerns the ease of using hand gestures to control on-air drawing. Fig.35 shows the percentage of the agreed response, which is 41%, the strongly agreed response is 28%, and the neutral response is 19%.

Overall, this indicates the ease of on-air drawing. The reasons for the high approval ratings are as follows:

1- Only three gesture methods were used for the authentication.

2 - The choice of gestures is suitable and comfortable for controlling the on-air drawing password. Open index finger gestures are suitable for writing, and open and closed hand gestures are suitable for erasing and saving.

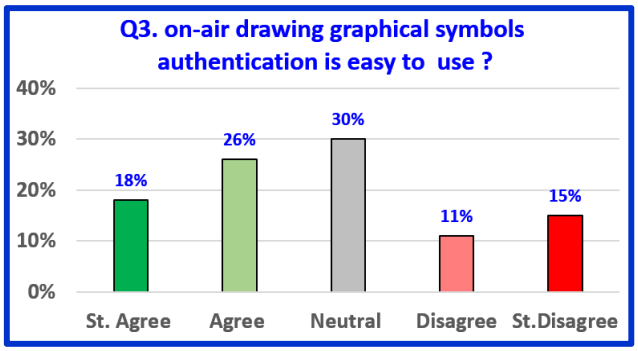


FIGURE 36. Results of the third question.

3- The fast response of hand gestures that facilitates and speeds up the control of the on-air drawing operation.

3 - The third question concerns the ease of the on-air drawing graphical symbol for authentication. Fig.36 shows the percentage of the neutral response with 30%, the agreed response with 26%, and 18% for the strongly agreed response.

These results reflect the ease of performing tasks during the experiment, but 15% strongly disagree. When the password symbols were reviewed, we found that they belonged to the category of hard (complex) symbols. Therefore, they had several options to solve this problem, including the following:

1- Choose one of the symbols from the category of easy or medium symbols.

2- There are thousands of ways to draw the same symbols. Thus, in general, we can conclude that the overall usage of the prototype is acceptable and easy.

D. GUESSING THREAT

The password strength of the proposed method was evaluated by comparing it with the traditional PIN 4-digits password. The traditional PIN 4-digits password contains 10 different symbols of numbers with a length of four digits. Therefore, based on equation (6), the password entropy for the PIN 4-digits password is 13.28, where ($S = 10, L = 4$). However, the proposed graphical password contains 47 symbols with a length of three symbols. Therefore, based on equation (6), the password entropy for the proposed graphical password is 16.66, where ($S = 47$, $L = 3$). Thus, the results show that the entropy for the graphical symbols password is greater than the PIN 4-digits password. Therefore, the graphical symbols password is stronger than the 4-digits PIN password by 3.38. In addition, the strength password of symbols can be increased by increasing the number of symbols, as shown in Table 2.

E. PHYSICAL OBSERVATION THREAT

First, the proposed method was based on drawing on air. Therefore, it is safe because we cannot see the drawing on the air, especially when the movement of the hand is fast and also

TABLE 2. Effect of number of symbols on the password entropy.

Number of Symbols	Password Entropy
100	19.93
150	21.69
200	22.93
250	23.90
300	24.69

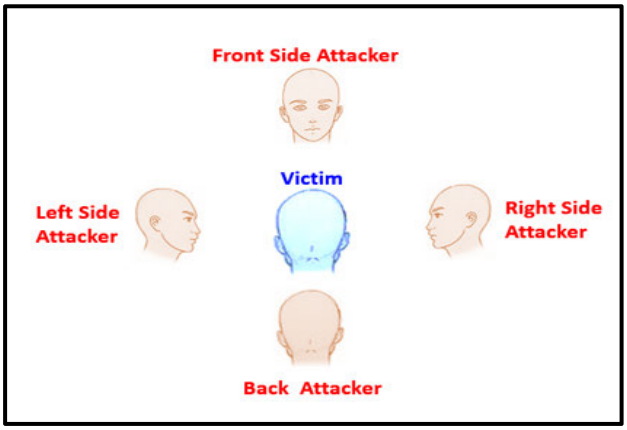


FIGURE 37. Shoulder-surfing attack vision.

with the increase in the number of graphic symbols, which makes it difficult to predict the password symbol.

Second, in the proposed method, there are thousands of ways to draw each symbol. Therefore, the Google Quick Draw symbols dataset is considered to be a large pool of random ways to draw each symbol. This means that there is no repetition of hand movements of the same symbol. This provides an additional layer of protection against random guessing, as well as physical observation threats. This makes it difficult for the attacker to guess the shape of the symbol through hand movements because it is different in hand movements on-air every time login. Clearly, it is also difficult for an attacker to imitate the behavior of a user learned from physical observation to know the common characteristics each time, so that he can derive the password symbol.

Third, when analyzing the attacker's observation of the victim from several vision angles, as shown in Fig. 37, we note the following:

1- The attacker from the front side sees the movement of the hand in the air reversed as in the mirror, which leads to an increase in the difficulty of observation and prediction.

2- The attacker from the right or left side sees only the vertical movement of the hand in the air, so it is safe from both sides.

3- The attacker from the backside sees the horizontal and vertical movements of the hand in the air. Therefore, one of the important security precautions for the proposed method is that, when drawing, the user must hide his hand movement by putting his hand in front of his body, not to the right or the left of the body.

F. COST TIME (AUTHENTICATION TIME)

The authentication time ranged from 24 to 60 s, and the average authentication time was 40 s. When analyzing passwords that took longer than 30 s, it was found that users used complex methods to draw symbols. Therefore, authentication time can be reduced by using medium-complexity graphics because users have thousands of options for drawing symbols. It is also expected to reduce the authentication time with training and frequent use.

VII. CONCLUSION

This paper proposes a new authentication method for Internet of Things IoT devices based on air hand-drawn passwords. The proposed method is based on a computer vision technique with a single camera, two lightweight deep CNN models, and a Kalman filter for signal processing to correct the drawn line path on the air. This combination is the main advantage of this framework over the existing approaches. The results showed that the proposed authentication method for usability parameters, such as accuracy, efficiency, and user satisfaction, is accepted and significant. In addition, the proposed method is secure and resistant to physical observation threats. This method is fully independent of any devices, wearable sensors, or depth cameras. In the future, the proposed method will be easy, simple, and suitable for controlling smart devices such as smart TVs, smartwatches, smart fridges, and smart air conditioning. The disadvantage of the proposed method is that it does not work in the dark.

REFERENCES

[1] C. Uysal and T. Filik, "RF-Wri: An efficient framework for RF-based device-free air-writing recognition," *IEEE Sensors J.*, vol. 21, no. 16, pp. 17906–17916, Aug. 2021, doi: 10.1109/JSEN.2021.3082514.

[2] S. D. Regani, C. Wu, B. Wang, M. Wu, and K. J. R. Liu, "MmWrite: Passive handwriting tracking using a single millimeter-wave radio," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13291–13305, Sep. 2021, doi: 10.1109/JIOT.2021.3066507.

[3] J. Chen, F. Yu, J. Yu, and L. Lin, "A three-dimensional pen-like ultrasonic positioning system based on quasi-spherical PVDF ultrasonic transmitter," *IEEE Sensors J.*, vol. 21, no. 2, pp. 1756–1763, Jan. 2021, doi: 10.1109/JSEN.2020.3016292.

[4] C. Lin, T. Xu, J. Xiong, F. Ma, L. Wang, and G. Wu, "WiWrite: An accurate device-free handwriting recognition system with COTS WiFi," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Nov. 2020, pp. 700–709, doi: 10.1109/ICDCS47774.2020.00079.

[5] M. Arsalan, A. Santra, and V. Issakov, "Radar trajectory-based air-writing recognition using temporal convolutional network," in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2020, pp. 1454–1459, doi: 10.1109/ICMLA51294.2020.00225.

[6] P. Wang, J. Lin, F. Wang, J. Xiu, Y. Lin, N. Yan, and H. Xu, "A gesture air-writing tracking method that uses 24 GHz SIMO radar SoC," *IEEE Access*, vol. 8, pp. 152728–152741, 2020, doi: 10.1109/ACCESS.2020.3017869.

[7] Y. Fang, Y. Xu, H. Li, X. He, and L. Kang, "Writing in the air: Recognize letters using deep learning through WiFi signals," in *Proc. 6th Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Jul. 2020, pp. 8–14, doi: 10.1109/BigCom51056.2020.00008.

[8] F. Khan, S. K. Leem, and S. H. Cho, "In-air continuous writing using uwb impulse radar sensors," *IEEE Access*, vol. 8, pp. 99302–99311, 2020, doi: 10.1109/ACCESS.2020.2994281.

[9] S. K. Leem, F. Khan, and S. H. Cho, "Detecting mid-air gestures for digit writing with radio sensors and a CNN," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 4, pp. 1066–1081, Apr. 2020, doi: 10.1109/TIM.2019.2909249.

[10] L. Lu, J. Liu, J. Yu, Y. Chen, Y. Zhu, X. Xu, and M. Li, "VPad: Virtual writing tablet for laptops leveraging acoustic signals," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 244–251, doi: 10.1109/PADSW.2018.8644615.

[11] L. Zhang, J. Wang, Q. Gao, X. Li, M. Pan, and Y. Fang, "LetFi: Letter recognition in the air using CSI," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647830.

[12] J. J. David, J. C. L. Genavia, T. L. Laplana, L. F. O. Rodrigo, D. A. Rodriguez, and R. E. Tolentino, "Hand gesture recognition model using standard deviation-based dynamic time warping technique," in *Proc. 5th Int. Conf. Comput. Methodolog. Commun. (ICCMC)*, Apr. 2021, pp. 1043–1050, doi: 10.1109/ICCMC51019.2021.9418237.

[13] G. Bastas, K. Kritsis, and V. Katsouros, "Air-writing recognition using deep convolutional and recurrent neural network architectures," in *Proc. 17th Int. Conf. Frontiers Handwriting Recognit. (ICFHR)*, Sep. 2020, pp. 7–12, doi: 10.1109/ICFHR2020.2020.00013.

[14] X. Yan, X. Sun, and H. Wang, "Research on conscious interactive angle of pen in 3D contactless air-drawing and writing," *IEEE Access*, vol. 8, pp. 162683–162691, 2020, doi: 10.1109/ACCESS.2020.3021401.

[15] W. Xu, J. Tian, Y. Cao, and S. Wang, "Challenge-response authentication using in-air handwriting style verification," *IEEE Trans. Depend. Sec. Comput.*, vol. 17, no. 1, pp. 51–64, Jan. 2020, doi: 10.1109/TDSC.2017.2752164.

[16] M. Taktak, S. Triki, and A. Kamoun, "3D handwriting characters recognition with symbolic-based similarity measure of gyroscope signals embedded in smart phone," in *Proc. IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2017, pp. 319–326, doi: 10.1109/AICCSA.2017.28.

[17] K. Wang, W. Zeng, C. Ma, C. Cheng, P. Sun, L. Wang, and W. Cai, "The design of wireless air mouse based on LPC54100," in *Proc. 36th Chin. Control Conf. (CCC)*, Jul. 2017, pp. 6409–6413, doi: 10.23919/ChiCC.2017.8028374.

[18] Y. Luo, J. Liu, and S. Shimamoto, "Wearable air-writing recognition system employing dynamic time warping," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–6, doi: 10.1109/CCNC49032.2021.9369458.

[19] S. K. Behera, P. Kumar, D. P. Dogra, and P. P. Roy, "A robust biometric authentication system for handheld electronic devices by intelligently combining 3D finger motions and cerebral responses," *IEEE Trans. Consum. Electron.*, vol. 67, no. 1, pp. 58–67, Feb. 2021, doi: 10.1109/TCE.2021.3055419.

[20] A. Pal, "MicaPen: A pen to write in air using mica motes," in *Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2020, pp. 151–154, doi: 10.1109/DCOSS49796.2020.00035.

[21] V. Chandel, S. Singhal, and A. Ghose, "AiRite: Towards accurate & infrastructure-free 3-D tracking of smart devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2020, pp. 1–6, doi: 10.1109/PerComWorkshops48775.2020.9156072.

[22] Y.-H. Chen, P.-C. Su, and F.-T. Chien, "Air-writing for smart glasses by effective fingertip detection," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Oct. 2019, pp. 381–382, doi: 10.1109/GCCE46687.2019.9015389.

[23] T. Sankhe, P. Puranik, and M. Mulla, "Futuristic finger and its modern day applications," in *Proc. Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, Sep. 2019, pp. 1–7, doi: 10.1109/ICICT46931.2019.8977629.

[24] L. Meli, D. Barcelli, T. L. Baldi, and D. Prattichizzo, "Hand in air tapping: A wearable input technology to type wireless," in *Proc. 26th IEEE Int. Symp. Robot Hum. Interact. Commun. (RO-MAN)*, Aug. 2017, pp. 936–941, doi: 10.1109/ROMAN.2017.8172415.

[25] D. Lu, K. Xu, and D. Huang, "A data driven in-air-handwriting biometric authentication system," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 531–537, doi: 10.1109/BTAS.2017.8272739.

[26] J. Malik, A. Elhayek, S. Guha, S. Ahmed, A. Gillani, and D. Stricker, "DeepAirSig: End-to-end deep learning based in-air signature verification," *IEEE Access*, vol. 8, pp. 195832–195843, 2020, doi: 10.1109/ACCESS.2020.3033848.

[27] P. Puranik, T. Sankhe, A. Singh, V. Vishwakarma, and P. Rane, "AirNote—Pen it down," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–7, doi: 10.1109/ICCCNT45670.2019.8944690.

[28] M. S. Alam, K.-C. Kwon, and N. Kim, "Trajectory-based air-writing character recognition using convolutional neural network," in *Proc. 4th Int. Conf. Control, Robot. Cybern. (CRC)*, Sep. 2019, pp. 86–90, doi: 10.1109/CRC.2019.00026.

[29] K. Li, J. Cheng, Q. Zhang, and J. Liu, "Hand gesture tracking and recognition based human-computer interaction system and its applications," in *Proc. IEEE Int. Conf. Inf. Autom. (ICIA)*, Aug. 2018, pp. 667–672, doi: 10.1109/ICInfA.2018.8812508.
[30] S. Hegde, G. Garg, R. Perla, and R. Hebbalaguppe, "A fingertip gestural user interface without depth data for mixed reality applications," in *Proc. IEEE Int. Symp. Mixed Augmented Reality Adjunct (ISMAR-Adjunct)*, Oct. 2018, pp. 395–396, doi: 10.1109/ISMAR-Adjunct.2018.00113.
[31] V. Joseph, A. Talpade, N. Suvarna, and Z. Mendonca, "Visual gesture recognition for text writing in air," in *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Jun. 2018, pp. 23–26, doi: 10.1109/ICCONS.2018.8663176.
[32] P. Roy, S. Ghosh, and U. Pal, "A CNN based framework for unistroke numeral recognition in air-writing," in *Proc. 16th Int. Conf. Frontiers Handwriting Recognit. (ICFHR)*, Aug. 2018, pp. 404–409, doi: 10.1109/ICFHR-2018.2018.00077.
[33] D. U. Lakshmi and B. Harish, "A novel air writing recognition system using raspberry Pi for the control and interaction of digital systems," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 3800–3804, doi: 10.1109/ICECDS.2017.8390175.
[34] W. Wazir, H. A. Khattak, A. Almogren, M. A. Khan, and I. U. Din, "Doodle-based authentication technique using augmented reality," *IEEE Access*, vol. 8, pp. 4022–4034, 2020, doi: 10.1109/ACCESS.2019.2963543.
[35] J. Liu, X. Zou, J. Han, F. Lin, and K. Ren, "BioDraw: Reliable multi-factor user authentication with one single finger swipe," in *Proc. IEEE/ACM 28th Int. Symp. Quality Service (IWQoS)*, Jun. 2020, pp. 1–10, doi: 10.1109/IWQoS49365.2020.9212855.
[36] A. Khan and A. G. Chefranov, "A captcha-based graphical password with strong password space and usability study," in *Proc. Int. Conf. Electr., Commun., Comput. Eng. (ICECCE)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICECCE49384.2020.9179265.
[37] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "BioTouchPass2: Touchscreen password biometrics using time-aligned recurrent neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2616–2628, 2020, doi: 10.1109/TIFS.2020.2973832.
[38] R. Tolosana, R. Vera-Rodriguez, and J. Fierrez, "BioTouchPass: Handwritten passwords for touchscreen biometrics," *IEEE Trans. Mobile Comput.*, vol. 19, no. 7, pp. 1532–1543, Jul. 2020, doi: 10.1109/TMC.2019.2911506.
[39] Y. Ku, L. H. Park, S. Shin, and T. Kwon, "Draw it as shown: Behavioral pattern lock for mobile user authentication," *IEEE Access*, vol. 7, pp. 69363–69378, 2019, doi: 10.1109/ACCESS.2019.2918647.
[40] B. E. Fayyadh, K. Mansour, and K. W. Mahmoud, "A new password authentication mechanism using 2D shapes," in *Proc. 8th Int. Conf. Comput. Sci. Inf. Technol. (CSIT)*, Jul. 2018, pp. 113–118, doi: 10.1109/CSIT.2018.8486188.
[41] D. Schwab, L. ALharbi, O. Nichols, and L. Yang, "Picture PassDoodle: Usability study," in *Proc. IEEE 4th Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Mar. 2018, pp. 293–298, doi: 10.1109/BigDataService.2018.00052.
[42] K. Riesen, T. Hanne, and R. Schmidt, "Sketch-based user authentication with a novel string edit distance model," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 3, pp. 460–472, Mar. 2018, doi: 10.1109/TSMC.2016.2601074.
[43] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical password-based user authentication with free-form doodles," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 4, pp. 607–614, Aug. 2016, doi: 10.1109/THMS.2015.2504101.
[44] *Google Quick, Draw Data Web Site*. Accessed: 2021. [Online]. Available: https://quickdraw.withgoogle.com/data/
[45] T.-H. Tsai, P.-T. Chi, and K.-H. Cheng, "A sketch classifier technique with deep learning models realized in an embedded system," in *Proc. IEEE 22nd Int. Symp. Design Diag. Electron. Circuits Syst. (DDECS)*, Apr. 2019, pp. 1–4, doi: 10.1109/DDECS.2019.8724656.
[46] *Ergonomics of Human-System Interaction—Part 11: Usability: Definitions and Concepts*, document ISO 9241-11:2018(en), 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:en
[47] A. R. Elshenaway and S. K. Guirguis, "Adaptive thresholds of EEG brain signals for IoT devices authentication," *IEEE Access*, vol. 9, pp. 100294–100307, 2021, doi: 10.1109/ACCESS.2021.3093391.
[48] W. Burr, D. Dodson, R. Perlner, W. Polk, S. Gupta, and E. Nabbus, "NIST special publication, 800-63-3, electronic authentication guideline," Comput. Secur. Division, Inf. Technol. Lab., Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-63-3, Jun. 2017.

ABDELGHAFAR R. ELSHENAWAY received the B.Sc. degree in electronics communications from Alexandria University, Egypt, in 1998, and the Diploma and M.Sc. degrees in information technology from the Department of Information Technology, Institute of Graduate Studies and Research (IGSR), Alexandria University, in 2001 and 2010, respectively, where he is currently pursuing the Ph.D. degree. From 2011 to 2016, he worked as a Lecturer in information technology at the Institute of Public Administration, Saudi Arabia. He participated as a Judge in the first Egyptian competition for skills in mobile applications with the Arab Academy for Science and Technology, Alexandria, in 2018. He participated as a Judge in the third Egyptian competition for skills in the Internet of Things with the Arab Academy for Science and Technology, in 2021. His current research interests include brain–computer interface (BCI), human–computer interaction, artificial intelligence, robots, embedded systems, machine learning, deep learning, computer vision, and the Internet of Things.

SHAWKAT K. GUIRGUIS received the B.Sc. and M.Sc. degrees in computer science and automatic control from the Faculty of Engineering, Alexandria University, Egypt, in 1981 and 1984, respectively, and the Ph.D. degree in electronics and communication co-supervised by Cairo University and the Imperial College of Science and Technology, University of London, U.K., in 1988. Since December 2006, he has been a Professor of computer science and informatics with the Department of Information Technology, Institute of Graduate Studies and Research (IGSR), Alexandria University. From August 2008 to July 2012, he was the Head of the Department of Information Technology, IGSR, Alexandria University. From August 2015 to August 2017, he was the Vice Dean for the Institute of Graduate Studies and Research (IGSR). He supervised approximately 80 M.Sc. and Ph.D. scholars. He has authored or coauthored more than 80 articles publications in prestigious journals and top international conferences and received several citations. His research interests include computer networks, information security, wireless sensor networks, intelligent decision support systems, image processing, optimization techniques, and databases. He is an Editorial Board Member of the *International Journal of Software Reuse*. He was a Reviewer of the *International Journal of Remote Sensing* (Taylor & Francis, U.K.), *International Journal of Computer Applications in Technology*, and *Alexandria Engineering Journal* (AEJ).