

Fingerprint-sensing Keycap: A Novel Concept with Verified Image Quality for Notebook Applications

Hsiang-Hung Hsu,¹ Yi-Pin Hsu,^{2*} and Kuo-Chun Wei¹

¹Department of Computer Science and Information Engineering, National Taipei University of Technology,
No. 1, Sec. 3, Zhongxiao E. Rd., Taipei 11608, Taiwan

²Department of Electrical Engineering, Chinese Culture University,
No. 55, Hwa-Kang Rd., Yang-Ming-Shan, Taipei 11114, Taiwan

(Received September 1, 2025; accepted October 24, 2025)

Keywords: fingerprint image quality, NFIQ 2, fingerprint-sensing keycap, notebook

Traditionally, the notebook fingerprint application design has been limited to specific areas, such as the power key or touchpad. Additionally, its low-frequency usage has not been promoted for real-time protection and enhanced economic effects. In this paper, we propose an innovative system that creates a functional fingerprint-sensing keycap in notebooks. To verify that the concept is workable in the overall system, a mainboard controller and a host application program are implemented. An international score indicator metric is also for an objective comparison of the quality of acquired fingerprint images. The use of the fingerprint verification competition (FVC) open database results to verify the score accuracy constitutes a good and acceptable choice. From the results of the comparison of the verification scores from open databases and the proposed captured fingerprint images, the proposed fingerprint-sensing keycap system was found to yield excellent responses. Findings show that the resulting fingerprint image quality score of about 24.29, assessed on the basis of the National Institute of Standards and Technology fingerprint image quality (NFIQ) 2 score, is very close to those of images available in the FVC 2000 database 2 and FVC 2002 database 3, about 26.15 and 25.85, respectively. It is demonstrated that the innovative system is functional and the captured fingerprint image quality is acceptable. In the future, it is envisaged that this innovative concept and implemented system will enable the development of notebooks and the evolution of other industrial applications.

1. Introduction

Artificial intelligence and the Internet of Things have developed tremendously. The efficient protection of personal privacy becomes an important goal. Some devices, including notebooks, keyboards, smartphones, and smart cards, still possess touch functionality to facilitate human interactions. Indeed, fingerprints constitute the best solution for touch action procedures in biometric technology applications. Biometric recognition is one of the promising authentication systems worldwide for personal and commercial applications. It uses a verification process that

*Corresponding author: e-mail: xyb@ulive.pccu.edu.tw
<https://doi.org/10.18494/SAM5884>

involves biological features, such as the face, fingerprints, hand veins, iris, retina, and others.⁽¹⁾ Practically, fingerprint identification and verification are extensively used in biometric techniques owing to their simplicity, distinctiveness, and lifetime properties. Recently, in the development or formulation of strategies for fingerprint recognition algorithms, minutiae-based techniques have become popular fingerprint-matching algorithms, including phase and skeleton topology matching or image correlation.^(2–6) In some instances, the noise present in the image during the scanning of biometric data distorts the recognition results.⁽⁷⁾

Therefore, fingerprint identification systems are still slow and often produce incorrect results. To overcome these problems, possible approaches include the development of a more accurate algorithm based on parametric adjustments and the enhancement of the image quality produced by the entire fingerprint-sensing system or at the sensor level only.

The performance in terms of the fingerprint recognition rate depends on many factors, such as the fingerprint acquisition systems (from the sensor level to the overall system construction), the quality of fingerprint images obtained using the sensor, and the physical attributes of the electronic device connection. The types of sensor used in fingerprint scanners are optical, capacitive, ultrasound, and thermal.^(8,9) The fingerprint recognition rate of optical sensors degrades considerably in cases of low-quality fingerprint images compared with those of capacitive sensors. Many factors that affect the quality of the images, including the complexity of the image background or finger touch time, sensing equipment distortions (such as those caused by the coating procedure), camera quality (only for optical images), and individual subject's artefacts for specified applications, hinder the process of authentication, as well as compute resources of embedded systems.^(8,10) Furthermore, poor image quality reduces the extractability of fingerprint features and the sensor's capabilities.⁽¹¹⁾ This results in higher false rejection rates (FRRs), leading to lower fingerprint authentication system performances, resulting in unsatisfactory user experiences.⁽¹²⁾ Furthermore, fingerprint systems (at the sensor and image-acquisition levels) were explored in a new study using images of the entire range of fingerprints, including plain, latent, partial, and contactless two-dimensional and three-dimensional images under a common framework,⁽¹³⁾ and new application fields were proposed, including those that use smartphones, webcams, prototypical hardware, Raspberry Pi, and digital cameras. Ordinary sensor applications have been proposed and have only been used for dedicated research studies and industrial development owing to the use of conventional sensor-oriented systems.

The fingerprint is a very important and suitable choice among all biometric features for user applications, such as the identification of humans or data encryption. Traditionally, humans are expected to use the touch functionality as the main input to replace original hardware devices such as the keyboard. Nowadays, every notebook still uses the keyboard as an input device. The main reason is that the up–down keycap feedback can provide users with a direct response to prepare for subsequent actions, such as typing or screen switching. In current commercial or consumer notebook products, the fingerprint function is only used for locking and unlocking the “Windows Hello” applications, and the fingerprint's hardware design is located in the power-button key or specified locations. Windows Hello is a feature in Windows that allows users to log into the device securely using facial recognition, fingerprints, or a personal digital

identification number. Even if the company Apple uses fingerprints to implement more application functions, such as payments, the fingerprint-sensing keycap is still required to input specified locations without having extra functionality. Notebooks are very popular devices nowadays for daily work, entertainment, telecommunications, online trades, and other tasks. Personal identification is associated with the identities of individuals, which is the requirement set by our society to ensure the safety of processes. However, identifying users and giving convenient access to them are ongoing topics. Owing to the rapid growth of information technology, people are more connected electronically to technology, which requires accurate, fast, and automatic individual identification. Because of personal privacy, fingerprint recognition is the best solution and is typically used as a biometric technology compared with face recognition, especially in notebook devices.

In this paper, we present a novel fingerprint-sensing keycap system. The key contributions and innovations of this work are summarized as follows. First, we propose a novel hardware design that integrates fingerprint sensors directly into standard keyboard keycaps, demonstrating the feasibility of fingerprint sensing through regular keys without requiring a dedicated fingerprint module. Second, we validate the proposed system using the standard metric and achieved results comparable to those obtained from representative open datasets. Finally, the performance obtained on the representative open datasets is employed as an indirect indicator of the proposed system's potential for practical fingerprint recognition applications.

2. Description of Fingerprint-sensing Keycap System

Herein, the innovative concept of the fingerprint-sensing keycap is proposed on the basis of the descriptions listed above. To construct and realize this concept, both hardware and software design considerations are essential. First, the design of a new keycap hardware architecture for sensor insertion is necessary according to the selected notebook keyboard specifications. The fundamental information of the capacitive sensor used includes a resolution of 160×160 pixels, operation using 8-bit datatypes, and a keycap size of $8 \times 8 \text{ mm}^2$. Second, the design of the software framework is expected to be functional and smooth; this framework is used to receive fingerprint data from the sensor connected to the keyboard controller via a serial peripheral interface protocol. The ARM-based M4-series microcontroller unit (MCU)⁽¹⁴⁾ is used and operated in conjunction with the keyboard controller to control the sensor and receive fingerprint data.

Additionally, the MCU is connected simultaneously to the host to transmit fingerprint data. Finally, the implementation of a software fingerprint-data-collection framework requires an application program (AP) to run on the Windows platform to receive real-time fingerprint data from the keyboard controller via the universal asynchronous receiver/transmitter or inter-integrated circuit protocols. The AP's functional contributions are twofold: one is to store fingerprint data and the other is to display images on the notebook screen (see Fig. 1). Typically, the overall processing in the system can be summarized in two stages, namely, the initial and working stages. During the initial stage, the keyboard controller arranges parameters correctly for the sensor and AP. During the working stage, the AP simultaneously displays the received

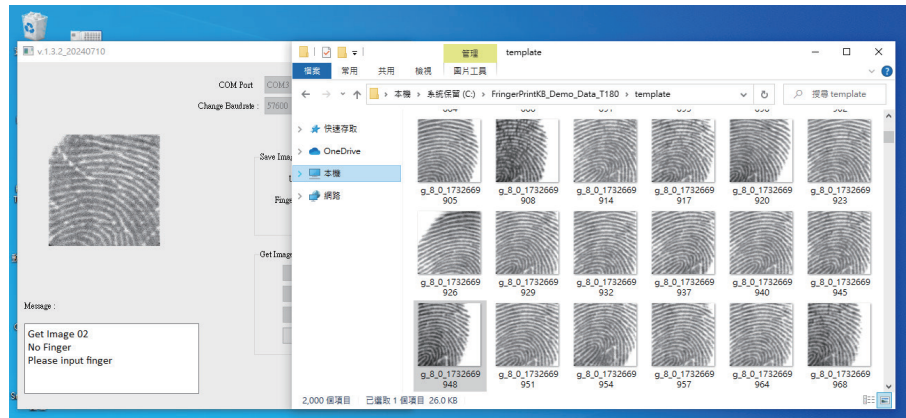


Fig. 1. (Color online) Depiction of the user interface in a notebook screen showing AP (left) and stored file folder (right).

fingerprint data on the screen when the user places their finger on the fingerprint-sensing keycap. The decomposition of the sensor's connection layout in actual notebooks is shown in Fig. 2.

Finally, schematic and actual views of the entire fingerprint-sensing keycap system are depicted in Fig. 3. This figure shows in detail the fingerprint-sensing keycap keyboard of the notebook and the structure of the fingerprint-sensing keycap (left). This fingerprint-sensing keycap includes a coating, a glass, a sensor, and the hardware keycap. Additionally, the implementation and installation of the fingerprint-sensing keycap sensor are shown in detail (upper right side). Finally, the software framework of the fingerprint dataflow and its operation are also shown (bottom right).

3. Presentation and Analysis of Captured Fingerprint and Open Database Images

Before setting up the fingerprint data collection process, all six participants were instructed to place their fingers in the fingerprint-sensing keycap. In this study, we recruited three additional volunteers in addition to the three authors due to personal privacy and the difficulty in obtaining real private fingerprints. Before the fingerprint collection process, the subjects were clearly informed and their consent was obtained. These fingerprint images will only be used for the presentation of this paper and will not be used for any other purpose. Four fingers, namely, the index and middle fingers of the left and right hands of each participant, were placed on the keycap because these are the fingers most often used during typing. Figure 4 shows all 24 fingerprint images of the four fingers of the six participants.

A fingerprint consists of ridge and valley patterns known as furrows. An important requirement for the fingerprint sensor is that the ridge should be analyzed smartly, irrespective of whether a male or female presses their fingers on the sensor. Participants 1, 2, and 3 were male, and the others were female. In the cases of participants 1, 2, and 5, the ridge gaps of the fingerprints were larger than those of the other participants. Typically, a large ridge gap is a feature associated with males and a small gap is usually associated with females. Moreover, the

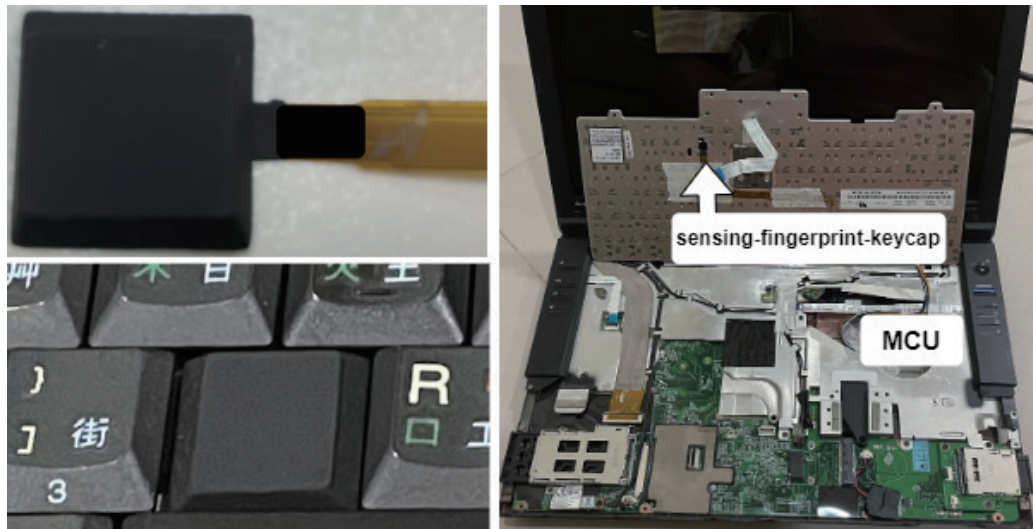


Fig. 2. (Color online) Display of the hardware system, including the (upper left) fingerprint-sensing keycap, (lower left) fingerprint-sensing keycap in the notebook's keyboard, and (right) MCU and its connection to the fingerprint-sensing keycap.

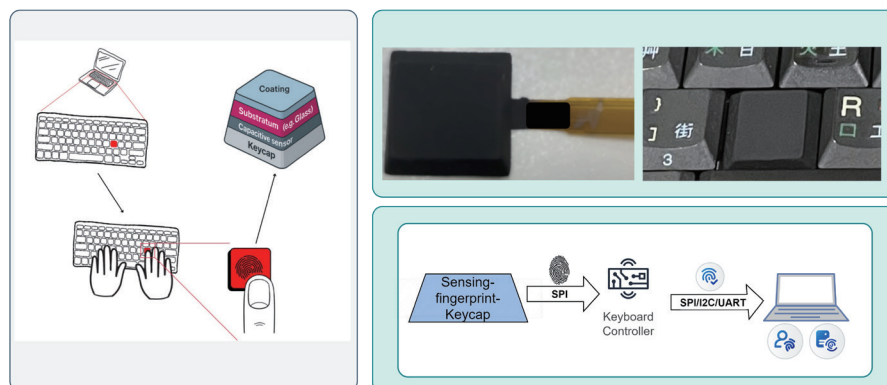


Fig. 3. (Color online) Entire view of the sensor and keycap (ranging from the physical concept of the fingerprint-sensing keycap system to the actual hardware implementation). The software framework of the fingerprint-sensing dataflow is presented in detail on the right side of the figure.

ridges and relative minutiae features, such as the bifurcation and crossover, are adequately visible. Figure 4 shows that the sensor's plug-in keycap has the proper fingerprint-sensing keycap functionality. For an objective comparison, two large open databases from the fingerprint verification competition (FVC) were used first, namely, FVC2000 and FVC2002.^(15,16) Two subset database images (FVC2000_DB2 and FVC2002_DB3) were selected arbitrarily and are presented in Fig. 5.

To ensure an objective comparison, the original images were cropped to have sizes of 160×160 pixels. Specifically, FVC2000_DB2 and FVC2002_DB3 belong to capacitive sensors. Twenty years ago, FVC2000 started the first international competition for fingerprint verification algorithms, and a shared open database was made available for downloading for



Fig. 4. Fingerprint images of four fingers including the index and middle fingers (left to right) of the six study participants (top to bottom).

research or other useful applications. Moreover, the first evaluation session was held in August 2000. The results of different algorithms that used the same database were presented at the 15th International Conference on Pattern Recognition, demonstrating excellent recognition rate outcomes (up to 99%). The fingerprint image quality in these databases was deemed adequate and acceptable. On the basis of these results, an objective and valuable reference point was identified and recommended. Without considering the influence of different recognition

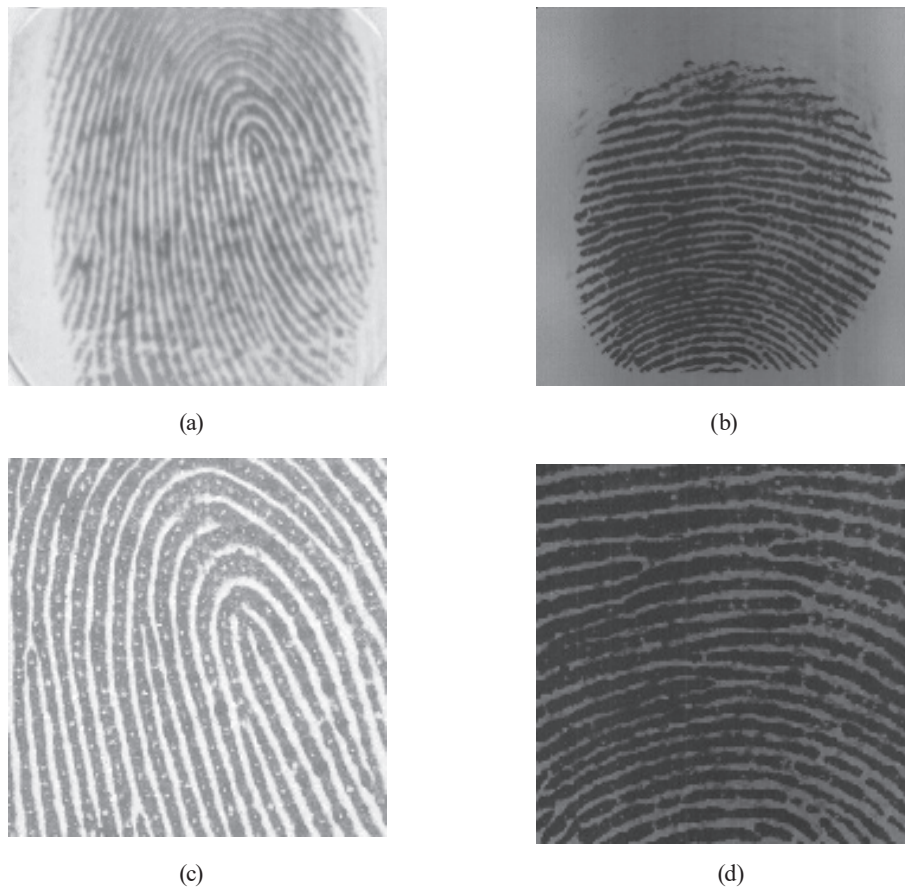


Fig. 5. (a) and (b) Selection of two different fingerprint images based on the image index codified as 3-1 in the FVC2000_DB2 dataset and 101-5 in the FVC2002_DB3 dataset, respectively. (c) and (d) are resized and cropped versions of (a) and (b), respectively, with the original resolutions of 300×300 pixels reduced to 160×160 pixels.

algorithms, the newly captured fingerprint image (with a quality equal to or almost equal to that of the FVC) should be accepted for fingerprint applications. Even if the above observations were visually distinguishable, an analytical strategy should be adopted to perform quantitative analyses.

4. Selection of an Objective Score Evaluation Metric for Fingerprint Image Quality Assessments

Image quality assessed by previous approaches has been discussed extensively.^(17–24) Two types of distortion and self-content estimation have been used. First, the distortion estimation focuses on the measurement error of the original and processed images, also known as the peak signal-to-noise ratio. Second, the core concept involves the estimation of the current image quality without any reference image. The second type uses a fingerprint image quality metric that is more suitable for accurate measurements related to the proposed work. Few objective fingerprint image quality algorithms have been proposed; these can be summarized into feature- and geometry-based frameworks.⁽¹⁷⁾ The feature-based framework applies quality metrics that

include the orientation certainty level, local orientation, and symmetry features, whereas the ridge direction has been typically used in parameter-adjustment algorithms. Typically, the ratio of the area of directional blocks to that of the entire image is used for feature extraction. For example, Shen *et al.* proposed an algorithm that employed an 8-directional Gabor filter to extract the fingerprint's feature.⁽¹⁸⁾ Quality was quantified according to the feature data and corresponding weights. However, parametric thresholding was involved during this process, which was an easy strategy and led to increased image quality variability.

The advanced feature-based framework involves the merging of several existing quality assessment approaches. This technique was further extended to solve the quality issue on the basis of classification approaches, such as the use of support vector machines or random forests. For example, the National Institute of Standards and Technology (NIST)—an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness—formulated a fingerprint score evaluation software called NIST fingerprint image quality (NFIQ). NFIQ⁽¹⁹⁾ classifies fingerprints into five levels using a trained neural network. All 11-dimensional feature sets⁽¹⁹⁾ and 36-dimensional feature sets^(20,21) are then utilized to estimate a matching score. However, prior dataset knowledge is required for NFIQ to work efficiently during the training process. The differences between the matched and nonmatched distributions of a given fingerprint determine the image quality. Although excellent performance was achieved in previous studies,^(21–24) they focused on only the generalized nature or human scenes. To achieve an objective comparison, NFIQ⁽¹⁹⁾ constitutes a recommended solution.

Two different versions of NFIQ (1 and 2) have been proposed. NFIQ was developed in 2004 to produce a quality marker extracted from a fingerprint image that was directly predictive of the expected matching performance (named NFIQ 1). Moreover, for the industry to improve core finger image quality assessment technology, NFIQ 2 was established on the basis of lessons learned from recent deployments of quality assessment algorithms (including NFIQ) in large-scale identity management applications. Thus, NFIQ 2 was considered suitable for fingerprint image quality assessments. As NFIQ can collect large fingerprint data (from the image to feature level), this facilitated the development of an efficient and visible score evaluation approach.

Table 1 lists the NFIQ 2 scores of different image databases obtained from FVC and the sensing keycap tests of our proposed system. A clearly excellent result was obtained, which showed that the score of the sensing keycap was very close to the score from the FVC database. This shows that the proposed keycap system can be used directly for fingerprint recognition applications.

Table 2 shows that the false nonmatch rate (*FNMR*) of fingerprint recognition was approximately 1% for the top three participant algorithms in FVC2000_DB2 and FVC2002_DB3 datasets. In the FVC2000_DB2 case, the fingerprint recognition rate and the image quality score are higher than those obtained in the FVC2002_DB3 case. This means that the recognition rate correlates with the evaluated score. On the basis of the reference guideline of the evaluated score of 25 and the achieved recognition rate of 99% in FVC2002_DB3, it can be inferred that the captured fingerprint image quality from our proposed system is acceptable. Moreover,

Table 1

Comparison of NFIQ 2 scores of FVC2000 DB2, FVC2002 DB3, and actual sensing keycap.

Database	FVC 2002 DB2	FVC 2002 DB3	Sensing keycap
NFIQ 2 score	26.15	25.85	24.29

Table 2

Summary of best *FRR* results associated with two open databases and different conditions. *FNMR* is also referred to as *FRR*.

<i>FNMR (FRR)</i>	FVC 2002 DB2			FVC 2002 DB3		
	Sag1 (%)	Sag2 (%)	Cspn (%)	PA15 (%)	P101 (%)	P097 (%)
FMR100 (<i>FAR</i> < 0.1%)	0.005	0.008	0.006	0.32	3.86	5.54
FMR1000 (<i>FAR</i> < 1%)	0.02	0.04	0.08	0.61	9.25	9.75

increasing the sensor's score is possible when the precision of the hardware assembly and installation increases. Thus, from the findings in Tables 1 and 2, our proposed system is considered functional and achieves an adequate fingerprint image for recognition in real-time typing.

5. Conclusions

In this study, two important results were obtained. First, an innovative fingerprint-sensing keycap system was proposed. The successful implementation and functionality of the system parts, including the inner sensor keycap, mainboard controller construction, and host AP framework, were demonstrated. To test reliability, six participants and up to 1200 images were involved in image quality evaluation tests. From the results of direct visual field tests, it was determined that the image quality and context (such as the fingerprint ridge and valley) were acceptable. Second, to achieve an objective image quality comparison without enhancement and recognition algorithm influences, the fingerprint quality of the proposed system was verified on the basis of NFIQ 2. In this step, a reasonable image quality reference score was obtained and used for the assessment of all the test fingerprint images.

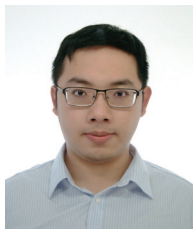
In the future, multiple systems, including the fingerprint-sensing keycap, should be constructed to enhance the capabilities of the sensor and system and the reliability of tests. Although in this study we have verified that the image quality is workable according to FVC comparisons and the score indicator is a feasible metric for different sensors, the transfer from the current to a new hardware system is necessary. The new score measurement method can also provide another marker for the verification of the acquired fingerprint images.

References

- 1 H. Hasan and S. Abdul-Kareem: Neural Comput. Appl. **23** (2013) 1605. <https://doi.org/10.1007/s00521-012-1113-0>
- 2 K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li: Future Gener. Comput. Syst. **110** (2020) 758. <https://doi.org/10.1016/j.future.2019.10.019>
- 3 A. Nur-A-Alam, M. Ahsan, M. A. Based, J. Haider, and M. Kowalski: Comput. Electr. Eng. **95** (2021) 107387. <https://doi.org/10.1016/j.compeleceng.2021.107387>

- 4 N. R. Pradeep, D. V. Manjunatha, A. Napolean, A. Arjun, and R. S.: Eng. Res. Express **7** (2025) 015226. <https://doi.org/10.1088/2631-8695/ada667>
- 5 R. Garg, G. Singh, A. Singh, and M. P. Singh: Syst. Soft Comput. **6** (2024) 200106. <https://doi.org/10.1016/j.sasc.2024.200106>
- 6 D. Kothadiya, C. Bhatt, D. Soni, K. Gadhe, S. Patel, A. Bruno, and P. L. Mazzeo: J. Imaging **9** (2023) 158. <https://doi.org/10.3390/jimaging9080158>
- 7 M. Nazarkevych, O. Riznyk, V. Samoty, and U. Dzelendzyak: East.-Eur. J. Enterp. Technol. **1** (2019) 57. <https://doi.org/10.15587/1729-4061.2019.154862>
- 8 S. Prabhakar, A. Ivanisov, and A. Jain: IEEE Instrum. Meas. Mag. **14** (2011) 10. <https://doi.org/10.1109/MIM.2011.5773529>
- 9 D. Zhang, F. Liu, Q. Zhao, G. Lu, and N. Luo: IEEE Trans. Instrum. Meas. **60** (2011) 863. <https://doi.org/10.1109/TIM.2010.2062610>
- 10 F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun: IEEE Trans. Inf. Forensics Security **2** (2007) 734. <https://doi.org/10.1109/TIFS.2007.908228>
- 11 Y. Chen, S. C. Dass, and A. K. Jain: Proc. Int. Conf. Audio- and Video-Based Biometric Person Authentication (Springer, Berlin, 2005) 160. https://doi.org/10.1007/11527923_17
- 12 D. Valdes-Ramirez, M. A. Medina-Pérez, R. Monroy, O. Loyola-González, J. Rodríguez, A. Morales, and F. Herrera: IEEE Access **7** (2019) 48484. <https://doi.org/10.1109/ACCESS.2019.2909497>
- 13 A. J. M. A. Cader and V. J. Banks Chandran: Sensors **23** (2023) 6591. <https://doi.org/10.3390/s23146591>
- 14 STMicroelectronics: <https://www.st.com/en/microcontrollers-microprocessors/stm32f4-series.html> (accessed August 2025).
- 15 D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain: Proc. 2002 Int. Conf. Pattern Recognition (IEEE, Quebec City, 2002) 811. <https://doi.org/10.1109/ICPR.2002.1048144>
- 16 D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain: IEEE Trans. Pattern Anal. Mach. Intell. **24** (2002) 402. <https://doi.org/10.1109/34.990140>
- 17 Z. Yao, J.-M. Le Bars, C. Charrier, and C. Rosenberger: IET Biometrics **5** (2016) 243. <https://doi.org/10.1049/iet-bmt.2015.0027>
- 18 L. Shen, A. Kot, and W. Koo: Proc. Int. Conf. Audio- and Video-Based Biometric Person Authentication (Springer, Berlin, 2001) 266. https://doi.org/10.1007/3-540-45344-X_39
- 19 M. Garriss, C. Watson, R. McCabe, and C. Wilson: NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD (2000). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151534
- 20 A. Mittal, R. Soundararajan, and A. C. Bovik: IEEE Signal Process. Lett. **22** (2013) 209. <https://doi.org/10.1109/LSP.2012.2227726>
- 21 A. Mittal, A. K. Moorthy, and A. C. Bovik: IEEE Trans. Image Process. **21** (2012) 4695. <https://doi.org/10.1109/TIP.2012.2214050>
- 22 R. Zhou, G. Jiang, L. Zhu, Y. Cui, and T. Luo: IEEE Signal Process. Lett. **32** (2025) 711. <https://doi.org/10.1109/LSP.2025.3531209>
- 23 S. Mishra, M. Jha, and A. C. Bovik: IEEE Trans. Image Process. **34** (2024) 140. <https://doi.org/10.1109/TIP.2024.3512376>
- 24 Y. Zhang, L. Wan, D. Liu, X. Zhou, P. An, and C. Shan: IEEE Trans. Instrum. Meas. **73** (2024) 1. <https://doi.org/10.1109/TIM.2024.3485447>

About the Authors



Hsiang-Hung Hsu received his B.S. degree from National Taiwan Ocean University, Taiwan, in 2018 and his M.S. degree from the Advanced Intelligence Control Laboratory, Graduate Institute of Automation Technology, National Taipei University of Technology, Taipei, in 2020. He is currently a research assistant at National Taipei University of Technology, Taiwan. His main research interests include computer vision, sensor sensing, and machine learning. (jkyounl98@gmail.com)



Yi-Pin Hsu received his B.S. degree in electrical engineering from Chinese Culture University, Taipei, Taiwan, in 2003. He received his M.S. degree from the Graduate Institute of Mechanical and Electrical Engineering, National Taiwan Normal University, Taipei, Taiwan, in 2005. He received his Ph.D. degree in electrical control engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2012. He is currently an assistant professor in the Department of Electrical Engineering of Chinese Culture University, Taipei, Taiwan. His research interests are in fingerprint and sensor applications, video processing, and other related areas. (xyb@ulive.pccu.edu.tw)



Kuo-Chun Wei received his M.S. degree from the Department of Communication Engineering, National Central University, Taiwan, in 2017. He is currently a research assistant at National Taipei University of Technology, Taiwan. His main research interests include computer vision, sensor sensing, and pattern recognition. (wei08957@gmail.com)

