

Article

Not peer-reviewed version

---

# An Open-Source Face-Aware Capture System

---

[Md Abdul Baset Sarker](#)<sup>\*</sup>, SM Safayet Hossain, [Naveenkumar G Venkataswamy](#), Stephanie Schuckers, [Masudul H Imtiaz](#)

Posted Date: 8 December 2023

doi: 10.20944/preprints202312.0617.v1

Keywords: <span>Face-aware; Face Quality; Jetson processor; AES encryption; Quality assessment; Passport</span>



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

# An Open-Source Face-Aware Capture System

Md Abdul Baset Sarker, SM Safayet Hossain, Naveenkumar G Venkataswamy,  
Stephanie Schuckers and Masudul H Imtiaz \*

Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, USA

\* Correspondence: mimitiaz@clarkson.edu

**Abstract:** This work introduces a novel facial image capture system that utilizes computer vision technology and artificial intelligence for real-time detecting, tracking, and capturing of human faces. The objective of this study is to address the challenges posed by poor-quality facial images in biometric authentication, especially in passport photo acquisition and recognition. By combining face-aware capture technology with AES encryption for secure image storage, we present a completely open-source hardware solution that consists of a Jetson processor, a 16MP autofocus RGB camera, a custom enclosure, and a touch sensor LCD for user interaction. Pilot data collection demonstrates the system's ability to capture high-quality images, achieving a 98.98% accuracy in storing images of acceptable quality. The integration of AES encryption ensures data security, making the proposed system suitable for real-time applications in other domains beyond identity verification in passport applications, such as security systems, video conferencing, etc.

**Keywords:** face-aware; jetson processor; AES encryption; quality assessment

---

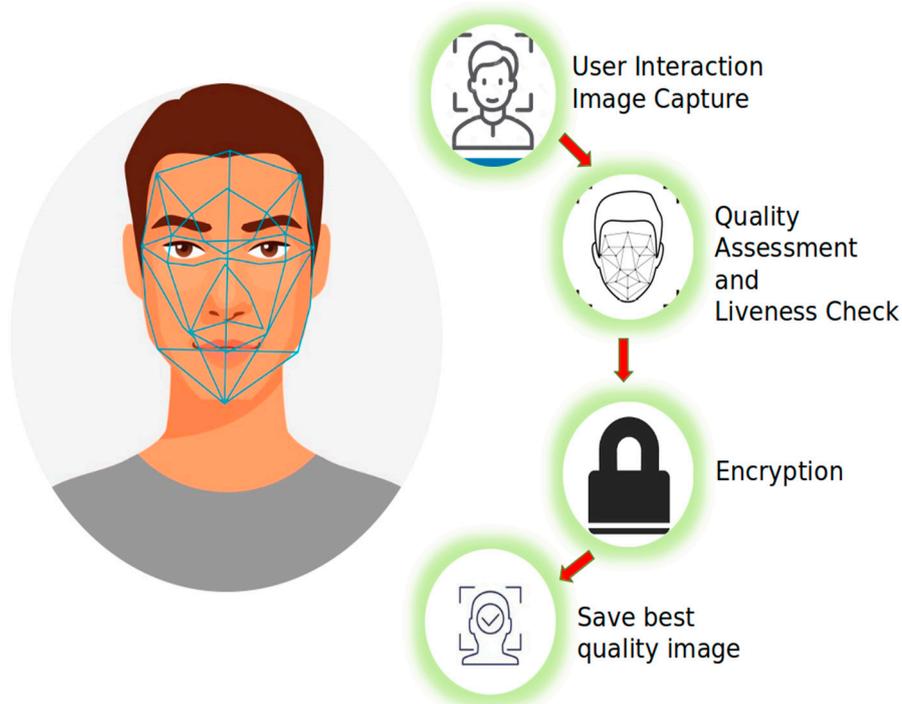
## 1. Introduction

Face recognition systems are widely used in border security. Till July 2023, the U.S. Customs and Border Protection (CBP) has utilized biometric facial comparison technology to handle over 300 million travelers and has effectively thwarted the entry of over 1,800 impostors into the U.S. [1]. Facial image reliability is paramount [2] in ensuring their precise identification. Variations in pose, illumination, and expression (PIE) lead to degradation of face recognition performance [3], [4] and acceptance of this technology. Numerous methods have been suggested to enhance the resilience of face recognition against various forms of degradation in face image quality [5], [6]. To ensure suitability, a face quality assessment is commonly performed. This involves a comprehensive analysis of various facial traits and characteristics, such as facial location, orientation, lighting, and image resolution [7]. For passport photo capture, the face quality assessment is performed offline.

Certain locations for passport photo capture still rely on outdated systems, where individuals either take their own photos or have them captured by authorized organizations. Subsequently, these individuals are required to send the images by mail. This process poses a potential risk of image tampering or manipulation. To overcome these limitations, state-of-the-art computer vision algorithms and geometric analysis are implemented in this research with real-time tracking of faces. In some places, images are taken manually by officials, where good quality depends on that person's experience. We wanted to automate this system with a computer algorithm and encrypt the image at the end so that only authorized persons can use these images.

According to our preliminary analysis, we found very few complete solutions regarding face-aware capture systems. Companies such as Aware Biometrics [8] provide commercial biometric solutions for face-aware systems. These systems are not open-source and sometimes not customizable, and customers need to be dependent on them for any modification or integration to their own system. In our research, we provided an open-source hardware and software-based solution that can run on a low-power single-board computer, and this is fully customizable.

This research addresses the crucial aspect of facial image quality in passport photo capture by introducing a novel face-aware capture system. The primary objective of our face-aware capture system is to determine whether an image meets the necessary criteria for effective use in biometric systems. For a system that requires a passport photo for verification, such as border security and immigration offices, it is important to have a high-quality image of the person's face. This research addresses the crucial aspect of facial image quality in passport photo capture by introducing a novel face-aware capture system. To ensure secure image storage, the proposed system integrates AES encryption [9], a reliable and effective technique for safeguarding sensitive data. The hardware design includes a Jetson processor, a 16MP camera, and a touchscreen display, ensuring an efficient and user-friendly interface for this system as a kiosk-based system. The demonstration of components of the face-aware capture system is shown in Figure 1.



**Figure 1.** Components of the proposed face-aware capture system.

The contribution of this study is 1) the presentation of a novel open-source hardware solution, 2) the development of an algorithm depending on ISO standards for face quality assessment, and 3) system validation through a pilot study and a US government-approved passport image quality website [10].

The paper is organized as follows: Section 2 discusses the methodology employed in the study. Section 3 presents a complete overview of the hardware design. Section 4 explains the details of the hardware used in the system. The procedure for software installation and implementation is given in Section 5. Section 6 describes the encryption part of the system. Section 8 explains the process for the pilot study. Finally, the paper concludes with a discussion and suggestions for future study.

## 2. System Overview

By following the methodical flowchart provided in Figure 2, the proposed face-aware capture system offers both better image quality and data integrity, thereby enhancing the overall passport photo capture experience. To using the system, the user stands in front of the camera; height is adjusted manually to ensure proper facial alignment within the capture area. Upon inputting their unique subject ID, the user starts the capture process by clicking the designated start button in the User Interface (UI). The integrated camera will start capturing the image; by the system, an automated quality check assesses each captured image based on predefined criteria, ensuring that

only high-quality images are considered for further review. The best quality images passing the quality check are displayed on the system's interface, allowing the user to select the most suitable photo for their passport. Once the user makes their choice, the selected image is encrypted and securely saved, along with the corresponding subject ID. These encrypted images can only be decrypted by the given key, which will only be available to authorized personnel.

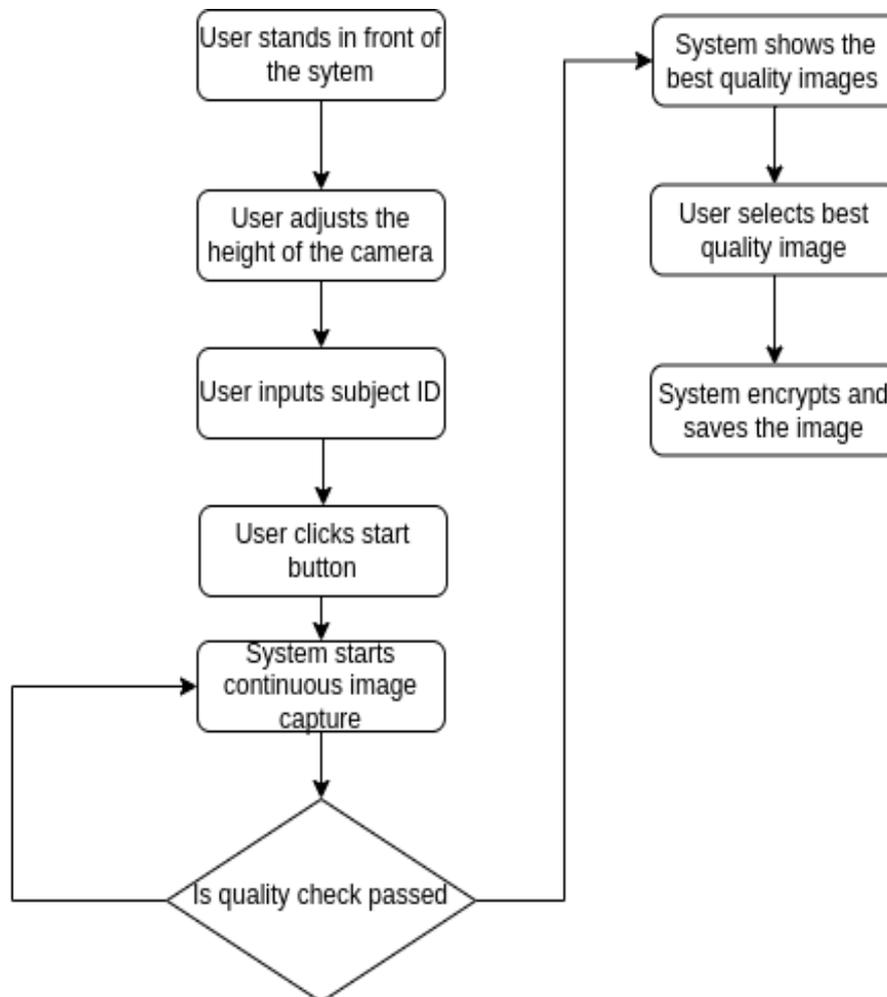


Figure 2. Flowchart of the system operation.

### 3. State-of-the-Art

The primary design objective of the proposed system was to ensure optimal performance and swift processing of user feedback, leading to an efficient and user-friendly system. A touch sensor LCD was integrated to facilitate seamless interaction with the system. Each participant's name and ID were provided as input to the software, generating a dedicated folder with their identity for organizing purposes only. During each capture, the image quality test was conducted with varying parameters based on the ISO standards, including face positions in the camera frame, eyes open/closed, face angles, and background conditions, among others, as shown in Table 1. Commonly abbreviated as ISO/IEC 19794-5 [11], face image data constitutes the fifth segment among the eight components of the ISO/IEC 19794 standard published in 2005. ISO/IEC 19794-5's purpose is to establish a uniform framework for encoding human facial data within a Common Biometric Exchange Formats Framework (CBEFF) compatible data structure intended for integration within facial recognition systems [11].

**Table 1.** Geometric and Photographic compliance check for ISO/IEC-19794-5.

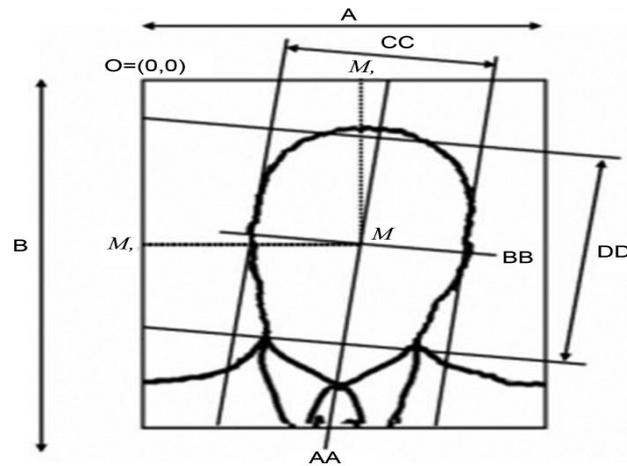
Test	Parameters
Geometric tests	Eye distance (min 90 pixels)
	Vertical position ( $0.3B < M < 0.5B'$ )
	Horizontal position ( $0.45A < M < 0.55A$ )
	Head image width ratio ( $0.5A < CC < 0.75A$ )
	Head image height ratio ( $0.6B < DD < 0.9B'$ )
Photographic and pose-specific tests	Blurred
	Looking Away
	Unnatural Skin Tone
	Too Dark/Light
	Washed Out
	Pixelation
	Red Eyes
	Eyes Closed
	Mouth Open
	Varied Background
Roll/Pitch Greater than $8^\circ$	

Javier et al. [12] proposed a deep-learning-based technique for evaluating the quality of face recognition. The approach involves employing a Convolutional Neural Network named FaceQnet, designed to forecast the appropriateness of a given input image for the task of face recognition. Jiansheng et al. [7] introduce a framework designed for assessing the quality of face images, incorporating both feature fusion and learning-to-rank techniques. The fusion method is also used by Zhang et al. [13]. They introduce the multi-branch face quality assessment (MFQA) algorithm for assessing face image quality, leveraging a lightweight CNN to extract features. Multiple factors, including alignment, visibility, deflection, and clarity, are evaluated through the algorithm's multi-branch layers. These individual scores are fused using a score fusion module to yield a final comprehensive quality confidence measure for subsequent recognition tasks.

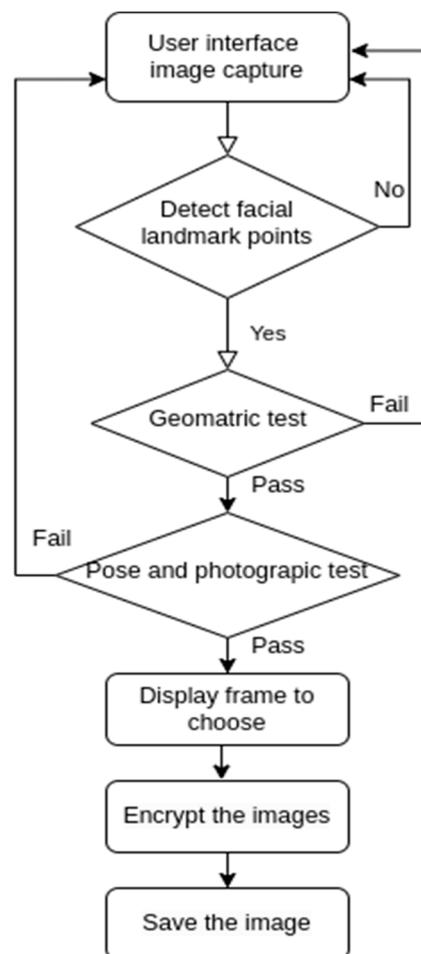
The face-aware capture process begins when a user approaches the system. The system promptly detects the presence of a face and proceeds to assess several criteria to determine the best facial image for capture. After detecting the face, the system detects a subset of facial landmark points using a custom facial landmark point detector [14]. The system then conducts geometric tests. The geometric test includes eye distance, head position and ratio, etc. After the geometric analysis (Table 1), the captured image undergoes further tests for pose and photographic quality. These tests include checking for blur, appropriate lighting, mouth open, closed eyes, and other relevant factors. The system also calculates pitch angles, which represent vertical rotation around a vertical axis indicating left and right rotation of the face, roll angles indicating face rotation about its axis, and yaw angles representing horizontal rotation like looking up and down. Additionally, pixelation refers to the emergence of indistinct, square-shaped blocks that become noticeable when an image is excessively enlarged. A comprehensive list of geometric and photographic tests is provided in Table 1.

If the geometric and photographic tests are successful, indicating a high-quality facial image, the system displays the best-quality images on the touch sensor LCD display. The user is then given the option to choose the desired photo for saving.

To ensure data security, the selected facial image is encrypted before being stored in the system's memory. For this purpose, AES encryption, a reliable and effective technique for safeguarding sensitive data, is implemented. After encryption, the passport office can only decrypt these images with the provided secure key generated by the system thus, it remains secure.



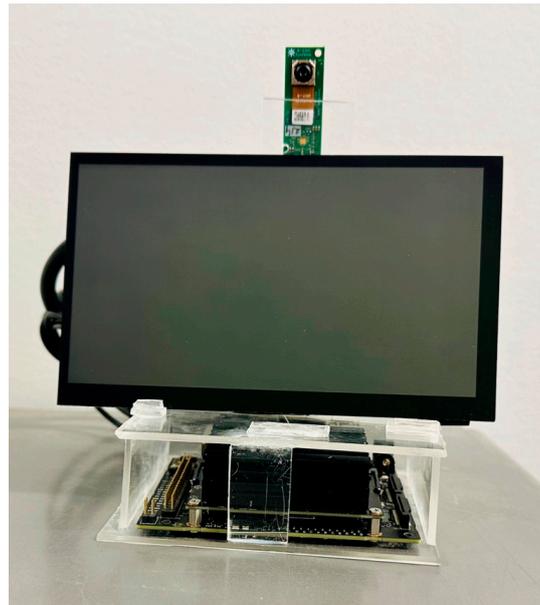
**Figure 3.** Geometric characteristics of the full-frontal face image ISO/IEC-19794-5.



**Figure 4.** Flow chart showing the steps of the face-aware capture system.

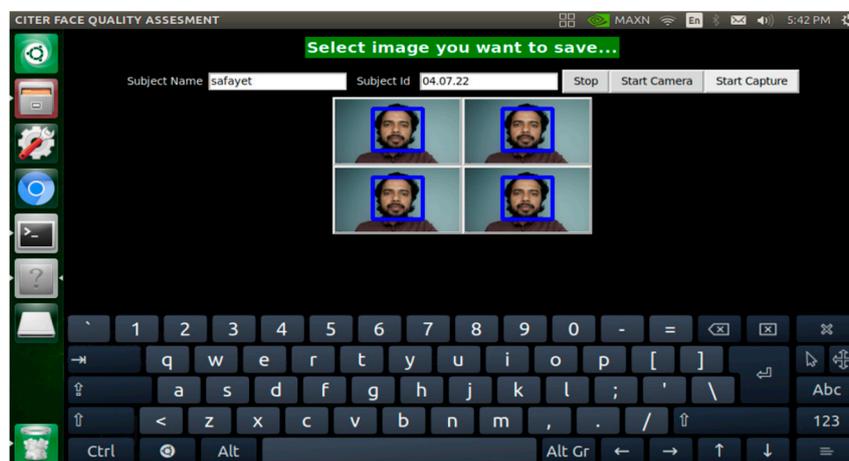
#### 4. Hardware Design

The core hardware components of the prototype (shown in Figure 5) include a high-resolution RGB 16MP camera responsible for capturing images and transmitting frames to the processor hosted on a Jetson Nano development board. Within the processor, the face-aware capture system detects faces and performs image processing and face quality assessments to identify the best possible images for further processing.



**Figure 5.** Components of Face-Aware Capture System: The Jetson Nano processor, LCD touchscreen, and a 16MP camera.

To facilitate user interaction, the touchscreen LCD is connected to the Jetson Nano board. This intuitive user interface, as shown in Figure 6, allows for convenient operations, such as starting or stopping the camera and selecting the optimal image for saving on the local drive. External input devices like a mouse and keyboard can also be connected to the Jetson Nano, providing users with versatile options for interacting with the system.



**Figure 6.** Graphical user interface (GUI) for inputting required information with process controls.

#### 4.1. NVIDIA Jetson Nano

The NVIDIA Jetson Nano developer kit is a compact yet powerful computer system. It has a Quad-core ARM A57 @ 1.43 GHz processor and 4GB of RAM. The Jetson Nano is equipped with an array of essential features, including four USB 3.0 ports for connecting peripherals, HDMI and DisplayPort connectors, a Micro-USB port for power supply, an Ethernet port for network connectivity, and a barrel jack socket to provide additional power for intensive computations. These comprehensive hardware specifications make the Jetson Nano an ideal choice for this application. There are similar single-board computers in the market, such as Raspberry Pi 4 model B [15], and BeagleBone Black [16]. Compared to those boards, Jetson Nano performs better on image processing, which is why we chose this board [17].

#### 4.2. Camera

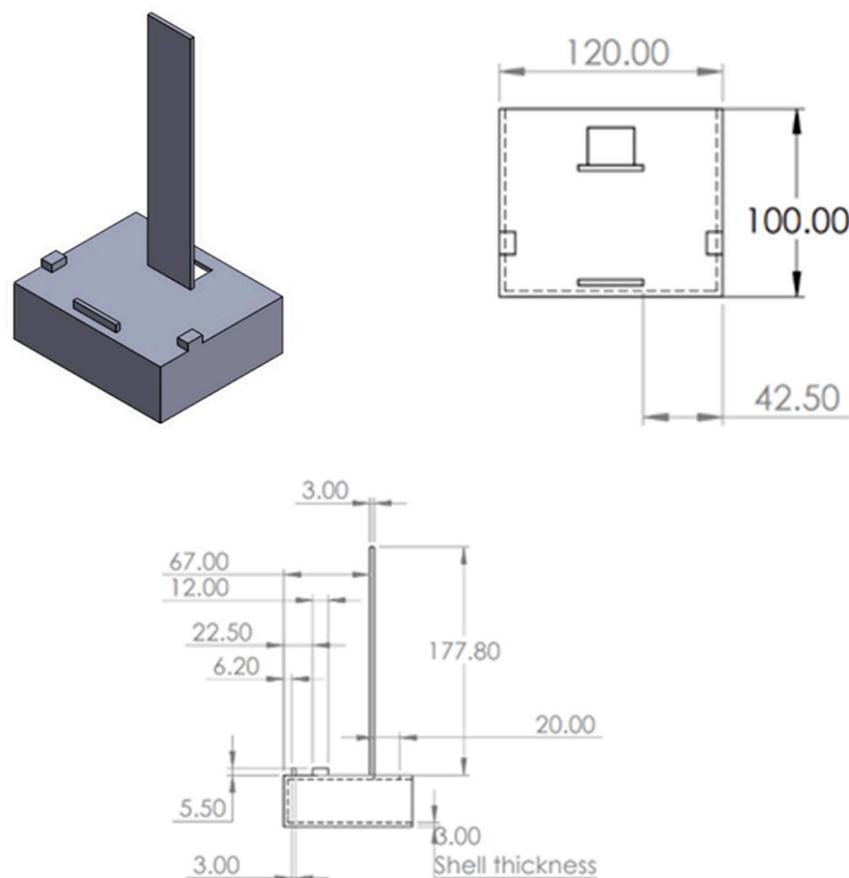
To build a face-aware capture system, we need a camera that has the capability to autofocus and auto brightness control. Because manual brightness and focus control take a good amount of time. So we used a See3CAM\_160 camera, which is a 16MP RGB camera with autofocus and USB 3.1 Gen 1 support, utilizing the 1/2.8" IMX298 CMOS image sensor, the focus distance is 100mm to Infinity [18]. This camera has auto-brightness control so that it can work in a wide range of lighting conditions.

#### 4.3. Display

Our intention is to build a system that can be used as a kiosk-like system, and the user can interact with the system. So our face-aware capture system is equipped with an Ingcool seven-inch HDMI LCD touchscreen IPS display featuring a resolution of 1024x600. The display operates on 5V power, allowing it to be powered directly from the USB ports of the Jetson Nano.

#### 4.4. Enclosure

The enclosure for our system measures 120X100X76 mm and is crafted from a 3mm acrylic sheet, as depicted in Figure 7. This designed enclosure serves as a secure enclosure for both the Jetson Nano and the LCD components. The design also prioritizes proper ventilation, ensuring optimal cooling for the Jetson Nano and LCD during operation. The design is also available in the repository [19].



**Figure 7.** System Enclosure with measurements in millimeters (mm). The top figure is the 3D model of the enclosure. The left-bottom Figure shows the measurements of the bottom plate, while the right-bottom Figure represents the complete enclosure measurements.

## 5. Software installation and implementation:

During the hardware installation process, we connected an external MicroSD card to the Jetson Nano Developer Kit. The operating system install was Ubuntu 18.04.5 LTS, and the Python version was Python 3.6.9. All the codes and installation instructions are available in the GitHub repository [19].

## 6. Encryption:

We used the Advanced Encryption Standard (AES) algorithm of the Python pyCryptodome module in the Cipher Block Chaining (CBC) Mode to encrypt the image. We have encrypted before saving the data so that the data becomes secure and less prone to spoofing. The encrypted images can only be decrypted using the private key provided to the Passport office. AES is a cryptographic algorithm employed for protecting electronic data. The adoption of AES encryption adds an additional layer of assurance to our face-aware capture system. AES is a 128-bit block cipher that supports 16, 24, or 32-byte independent key sizes. The algorithm performs multiple rounds of encryption, and the number of rounds depends on the key length. For example, we used a key size of 32 bytes that required 14 rounds. CBC mode starts by XOR-ing the first plaintext block with an initialization vector of 16 bytes. Then, AES encryption is applied to the resulting block using a key. In the next step, before performing encryption with the key, each subsequent plaintext blockchain is XOR-ed with the previous block [9].

The Decryption of CBC mode with AES is performed by XOR-ing the output block obtained from the decryption algorithm using the key to the previous ciphertext block.

The encryption and decryption process is shown in Figure 8, where IV is the Initial vector,  $P_i$  is the  $i$ th plain text block, and  $C_i$  is the  $i$ th Ciphertext block.

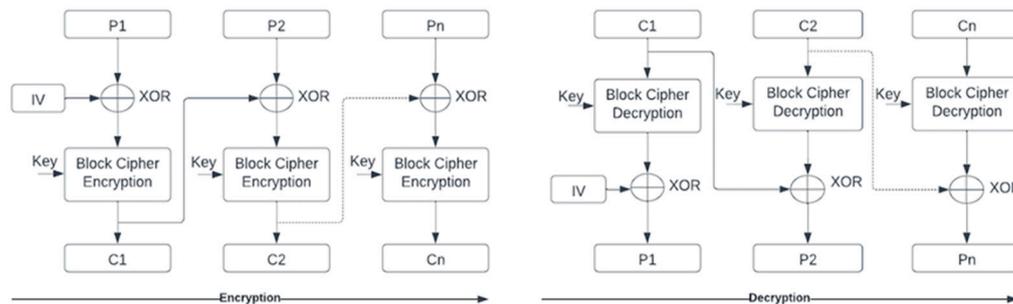


Figure 8. CBC mode of AES encryption and decryption.

## 7. Validation Study and Performance Analysis

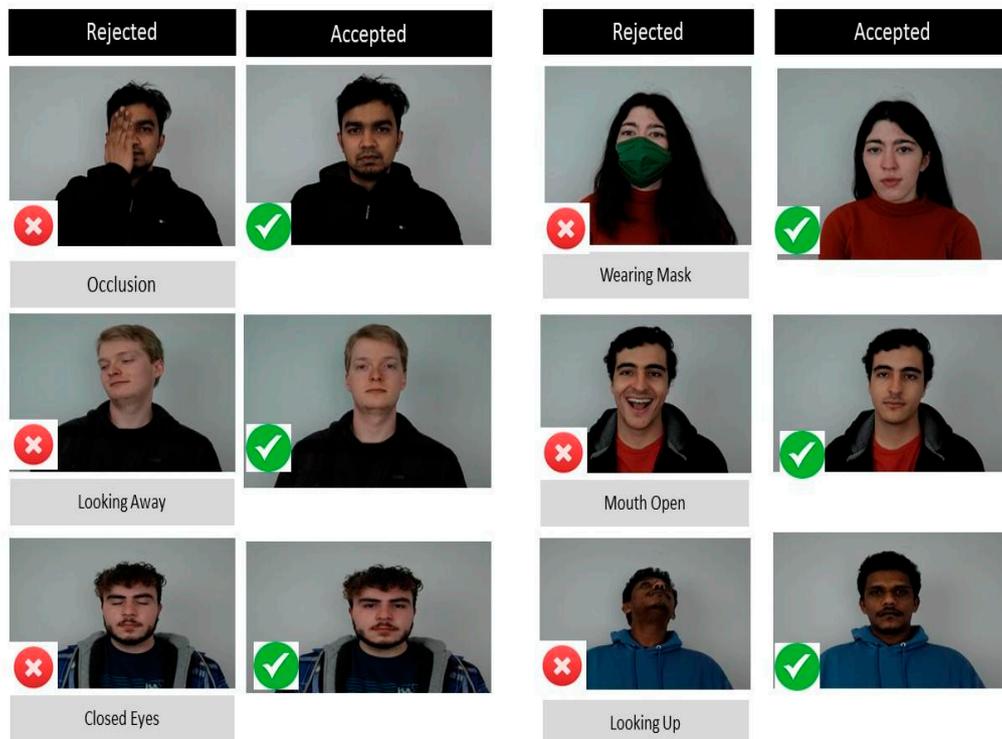
To verify our face-aware capture system's capability, we collected face image data using our system and verified it on the US Travel government passport image check website [10]. Throughout a span of three months, multiple continuous captures were conducted for 39 participants, consisting of 29 males and 10 females. The dataset included Caucasians, Asians, and Hispanics. The ages ranged from 6 to 60 years. In terms of height, the participants varied from a minimum of 138 cm to a maximum of 201 cm. We used a tripod and adjusted the height of the camera depending on the participant's height. We have adjusted the height of the tripod depending on the participants' height.

Table 2 summarizes demographic details about the subjects, including the distributed gender representation, ethnicities, and associated age range.

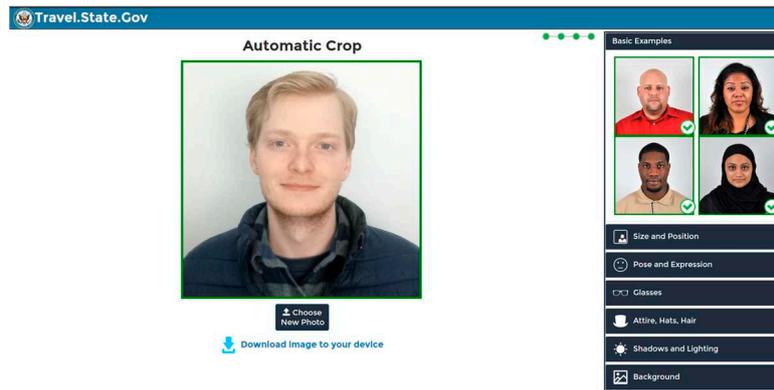
**Table 2.** Subject demographic details in the validation study.

Demographic details	Type	Count
Ethnicity	Caucasian	24
	Asian	11
	Hispanic	4
Age range	6 to 17 years	2
	18 to 25 years	24
	26 to 40 years	11
	Above 40 years	1

The data collection comprised over 6,000 images captured. Figure 9 displays a comparison of rejected and acceptable images. The left-hand side images were rejected due to issues with the mouth open, looking away, eyes closed, etc. The right-hand side images were acceptable because they satisfy all the predefined criteria for a high-quality image.

**Figure 9.** Examples of accepted and rejected images.

After collecting the pilot data, we conducted a rigorous comparison with the US Travel government passport image check website [10]. We randomly took three images from each subject and tested them there. Of the images that are determined as acceptable images from our face-aware capture system, 98.98% of them were accepted by the US Travel government passport image check website [10], as shown in Table 4. Only one image was rejected due to a compression issue. An example of an accepted image is shown in Figure 10, tested on the US Travel website. Table 3 shows the timing information of the system. The system takes 0.085 seconds to process each image.



**Figure 10.** Example of the accepted image on the website.

**Table 3.** Type of Quality Checks and Corresponding Time Taken for Each Task in Seconds.

Operation	Time (s)
Brightness check	0.0078
Background color check	0.0015
Blur photo check	0.0027
Landmark point detection	0.0376
Jaw angle time	.0000724
Eye distance time	0.00011
red eye detector	0.00029
Mouth distance	0.00015
Total time per frame	0.085

**Table 4.** Test results on US passport website.

Ethnicity	No of Subject	No of Test Image	Accepted	Rejected	Accuracy
Caucasian	24	72	72	72	100%
Asian	11	33	32	1	96.96%
Hispanic	4	12	12	12	100%
Average					98.98%

## 8. Discussion

A novel face-aware capture system is proposed to facilitate efficient and user-friendly image capture. The facial recognition system's performance is generally influenced by the quality of the acquired raw face data. With the facial recognition system we developed, we achieved a 98.98% accuracy of accepted images on the US Travel website. This approach allowed us to minimize potential issues arising from inaccuracies and improve the overall reliability of the system.

One significant step towards enhancing the system's performance was the implementation of real-time quality assessment during facial data capture. By continuously evaluating the quality of facial images during acquisition, we could proactively address shortcomings and ensure that only high-quality images were considered for biometric enrolment by implementing ISO standards. The integration of AES encryption further ensures data security, making the system suitable for real-time applications in various domains, such as security systems, video conferencing, and identity verification in passport applications.

In this proposed system, we opted to utilize the Jetson Nano 4GB for its processing capabilities, featuring a Quad-core ARM A57 @ 1.43 GHz processor and 4GB of RAM. The base version of the Jetson Nano was not selected due to our requirement for faster processing, and the Jetson Xavier series (with a 2.2 GHz processor) was not chosen, considering its higher cost. Using the Jetson Nano 4GB processor, we achieved a running speed of up to ten frames per second. Usually, Jetson Nano 4GB takes 5 to 10 watts of power. During this research phase, our primary focus was not on power consumption concerns. However, in future research endeavors, we intend to address power consumption issues. Creating our own PCB by taking only the necessary components that are crucial for our application will reduce power consumption and cost.

During the data collection phase, we encountered various challenges and insights. The process of gathering high-quality facial data required careful attention to lighting conditions, camera settings, and participant cooperation. We found that participants' movements or expressions during image capture could affect data quality. Additionally, varying environmental factors influenced the outcome of facial recognition accuracy. Understanding these factors deepened our appreciation for the importance of meticulous data collection in producing reliable results. While collecting data, we tried to consider the diversity in subjects. Diversity in the dataset becomes essential when analyzing and comprehending the overall diversity within our study's population groups. Diversity helps in evaluating how system performance varies across demographics.

Despite the system's advantages, it also has some limitations. The effectiveness of real-time quality assessment depends on the effectiveness of the assessment algorithms, and some artifacts, such as skin tone, might still go undetected. We were not able to implement Yaw detection (the angle of looking up and looking down) as we were using a 2D camera. And we did not include skin tone detection in our system. Skin tone detection would be helpful in detecting spoofing attacks such as wearing a mask or artificial skin. Additionally, while we exercised strict control over data quality during collection, external factors beyond our control could still influence the overall quality of acquired facial data.

Another limitation of this system is that the participant needs to manually adjust the camera height by controlling the tripod heights. In our future design, we plan to make the height adjust automatically using a motorized solution.

To improve the design further, we could explore advanced preprocessing techniques to handle challenging lighting conditions and facial variations better. Incorporating machine learning or deep learning algorithms to control the optimum brightness dynamically could improve the system. The camera we used here worked well, and we believe it will also work with young children as well. This is left open for the future.

## 9. Conclusion

The face-aware capture system presented in this research will contribute significantly to advancing technology in facial biometric enrolment systems. The system ensures reliable and secure face image capture and authentication by providing a portable, open-source hardware and software solution. With its potential applications in security systems, access control, and identity verification, the face-aware capture system aims to enhance the overall efficacy and trustworthiness of biometric authentication systems in diverse real-world scenarios.

## References

1. "Biometrics | U.S. Customs and Border Protection." Accessed: Aug. 28, 2023. [Online]. Available: <https://www.cbp.gov/travel/biometrics>
2. P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 531–543, Apr. 2007, doi: 10.1109/TPAMI.2007.1019.
3. Z. Mahmood, T. Ali, and S. U. Khan, "Effects of pose and image resolution on automatic face recognition," *IET Biom.*, vol. 5, no. 2, pp. 111–119, 2016, doi: 10.1049/iet-bmt.2015.0008.
4. O. Aldrian and W. A. P. Smith, "Inverse Rendering of Faces with a 3D Morphable Model," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 5, pp. 1080–1093, May 2013, doi: 10.1109/TPAMI.2012.206.

5. L. Wiskott, J.-M. Fellous, and N. Kruger, "Face Recognition by Elastic Bunch Graph Matching".
6. V. Blanz and T. Vetter, "Face recognition based on fitting a 3D morphable model," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1063–1074, Sep. 2003, doi: 10.1109/TPAMI.2003.1227983.
7. J. Chen, Y. Deng, G. Bai, and G. Su, "Face Image Quality Assessment Based on Learning to Rank," *IEEE Signal Process. Lett.*, vol. 22, no. 1, pp. 90–94, Jan. 2015, doi: 10.1109/LSP.2014.2347419.
8. A. Biometrics, "Biometrics Simplified," Aware. Accessed: Aug. 21, 2023. [Online]. Available: <https://www.aware.com/>
9. M. J. Dworkin, "Advanced Encryption Standard (AES)," National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 197-upd1, 2023. doi: 10.6028/NIST.FIPS.197-upd1.
10. "Photo-tool." Accessed: Aug. 18, 2023. [Online]. Available: <https://tsg.phototool.state.gov/photo>
11. 14:00-17:00, "ISO/IEC 19794-5:2011," ISO. Accessed: Aug. 29, 2023. [Online]. Available: <https://www.iso.org/standard/50867.html>
12. J. Hernandez-Ortega, J. Galbally, J. Fierrez, R. Haraksim, and L. Beslay, "FaceQnet: Quality Assessment for Face Recognition based on Deep Learning," in *2019 International Conference on Biometrics (ICB)*, Jun. 2019, pp. 1–8. doi: 10.1109/ICB45273.2019.8987255.
13. Z. Lijun, S. Xiaohu, Y. Fei, D. Pingling, Z. Xiangdong, and S. Yu, "Multi-branch Face Quality Assessment for Face Recognition," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, Oct. 2019, pp. 1659–1664. doi: 10.1109/ICCT46805.2019.8947255.
14. "davisking/dlib: A toolkit for making real world machine learning and data analysis applications in C++." Accessed: Aug. 18, 2023. [Online]. Available: <https://github.com/davisking/dlib/tree/master>
15. R. P. Ltd., "Buy a Raspberry Pi 4 Model B," Raspberry Pi. Accessed: Aug. 29, 2023. [Online]. Available: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>
16. "BeagleBone® Black," BeagleBoard. Accessed: Aug. 29, 2023. [Online]. Available: <https://www.beagleboard.org/boards/beaglebone-black>
17. C. Engineer, "Nvidia Jetson Nano vs Raspberry Pi 4 Benchmark," Arnab Kumar Das. Accessed: Aug. 29, 2023. [Online]. Available: <https://www.arnabkumardas.com/topics/benchmark/nvidia-jetson-nano-vs-raspberry-pi-4-benchmark/>
18. "See3CAM\_160 - 16MP (4K) Autofocus USB 3.1 Gen 1 Camera Board (Color)," e-con Systems. Accessed: Aug. 16, 2023. [Online]. Available: <https://www.e-consystems.com/usb-cameras/16mp-sony-imx298-autofocus-usb-camera.asp>
19. M. A. B. Sarker, "for jetson nano, python 3.6." Jan. 21, 2022. Accessed: Aug. 16, 2023. [Online]. Available: <https://github.com/baset-sarker/face-aware-gui>

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.