Article

An Open-Source Face-Aware Capture System

Md Abdul Baset Sarker [ID], S. M. Safayet Hossain, Naveenkumar G. Venkataswamy, Stephanie Schuckers and Masudul H. Imtiaz *

Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, USA; sarkerm@clarkson.edu (M.A.B.S.); smhossa@clarkson.edu (S.M.S.H.); venkatng@clarkson.edu (N.G.V.); sschucke@clarkson.edu (S.S.)
* Correspondence: mimtiaz@clarkson.edu

Abstract: Poor-quality facial images pose challenges in biometric authentication, especially in passport photo acquisition and recognition. This study proposes a novel and open-source solution to address these issues by introducing a real-time facial image quality analysis utilizing computer vision technology on a low-power single-board computer. We present an open-source complete hardware solution that consists of a Jetson processor, a 16 MP autofocus RGB camera, a custom enclosure, and a touch sensor LCD for user interaction. To ensure the integrity and confidentiality of captured facial data, Advanced Encryption Standard (AES) is used for secure image storage. Using the pilot data collection, the system demonstrated its ability to capture high-quality images, achieving 98.98% accuracy in storing images of acceptable quality. This open-source, readily deployable, secure system offers promising potential for diverse real-time applications such as passport verification, security systems, etc.

Keywords: AES encryption; face-aware; face-quality; Jetson processor; passport; quality assessment

1. Introduction

Face recognition systems are widely used in border security [1]. Until July 2023, the U.S. Customs and Border Protection (CBP) utilized biometric facial comparison technology to handle over 300 million travelers and effectively thwarted the entry of over 1800 impostors into the U.S. [2]. Facial image reliability is paramount [3] in ensuring precise identification. Variations in pose, illumination, and expression (PIE) lead to degradation of face recognition performance [4,5] and impede acceptance of this technology. Different methods have been suggested to enhance the resilience of face recognition against various forms of degradation in face image quality [6,7]. The criteria for being a good photo for a biometric system are defined by ISO standards, which establish a uniform framework for encoding human facial data within a Common Biometric Exchange Formats Framework (CBEFF). The CBEFF-compatible data structure intended for integration within facial recognition systems involves a comprehensive analysis of various facial traits and characteristics, such as facial location, orientation, lighting, and image resolution [8]. The International Civil Aviation Organization (ICAO) also works on the specifications for Machine Readable Travel Documents (MRTDs), emphasizing the importance of the portrait printed on these documents as a crucial identifier [9].

For passport photo capture, the face quality assessment is generally performed offline [10]; this makes the system more complex and increases the possibility of introducing bad-quality images. 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 [11]. In some places, images are taken manually by officials, where good quality depends on that person's experience. Subsequently, these individuals are required to send the images by mail. This process poses a potential risk of image tampering or manipulation.

To overcome the limitations of these outdated systems, we propose to automate the system with a computer algorithm and encrypt the image at the end so that only authorized persons can use these images. We have developed computer vision algorithms for geometric, pose, and photographic analysis with real-time face capture using only open-source software and hardware solutions. The need for such a system for e-gates in airports is substantial, as many face-aware systems are employed there but not for data acquisition [1,12–15]. Aware Biometrics [16] is one such system that provides commercial biometric solutions for face-aware systems. These systems are not open-source and sometimes not customizable, so customers are dependent on the company for any modification or integration to their system.

Javier et al. [17] 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 detect the appropriateness of a given input image for the task of face recognition. Jiansheng et al. [8] 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. [18]. 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. None of these systems use open-source hardware and software solutions together for face-aware capture systems.

In facial recognition systems and other biometric security systems, camera-based solutions are widely used for different modalities [15,19–25], and low-powered single-board computers are popular for image analysis-based projects because of their smaller size, low power consumption, etc. [26–30]. In our research, we provided an open-source hardware and software solution that can run on a low-power single-board computer with a commercially available camera in a fully customizable system.

This research addresses the crucial aspect of facial image quality in passport photo capture by introducing a novel open-source face-aware capture system. Our algorithm performs the geometric, pose, and photographic tests and secures the image by AES-128 encryption [31]. The hardware design includes a Jetson processor (manufacturer NVIDIA Corporation, Santa Clara, CA, USA), a 16 MP camera, and a touchscreen display, ensuring an efficient and user-friendly interface for this system as a kiosk-based system. These components of the proposed face-aware capture system are shown in Figure 1.
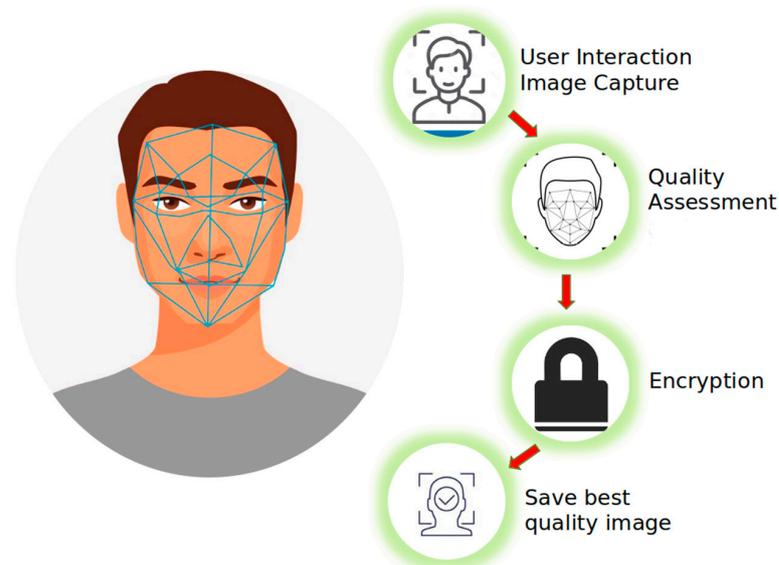

Figure 1. Components of the proposed face-aware capture system.

The overall contribution of this study can be summarized as:

(1) A novel open-source hardware solution,
(2) A software application designed for embedded processors that evaluates face quality in real-time based on ISO standards and provides a user interface for interaction,
(3) A system validation study involving live participants, with a U.S. government-certified website for passport image quality serving as the benchmark [32].

The paper is organized as follows: Section 2 discusses the system operation, and Section 3 discusses the methodology employed in the study. Section 4 presents a complete overview of the hardware design. The procedure for software installation and implementation is given in Section 5. Section 6 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 flowchart provided in Figure 2, the working steps of the proposed face-aware capture system offer both better image quality and data integrity, thereby enhancing the overall passport photo capture experience.
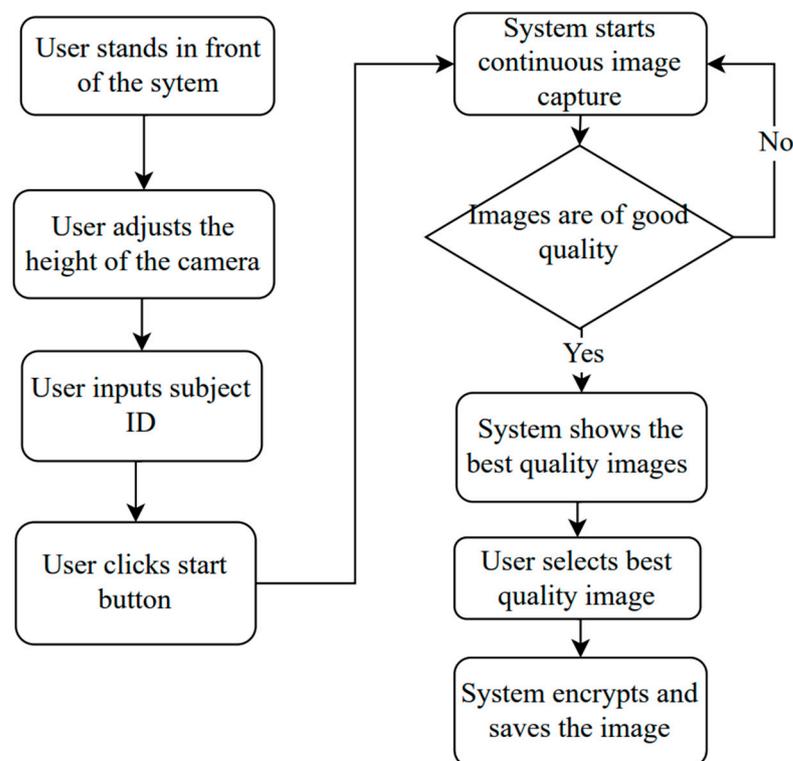

Figure 2. Working steps of the face-aware capture system.

To use the system, the user stands in front of the camera, and the 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, and 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.

3. Methodology

The flowchart of the face-aware capture system is shown in Figure 3. The face-aware capture process begins when a user approaches the system. Each participant's name or ID was provided as input to the software, generating a dedicated folder with their identity for organizing purposes only.
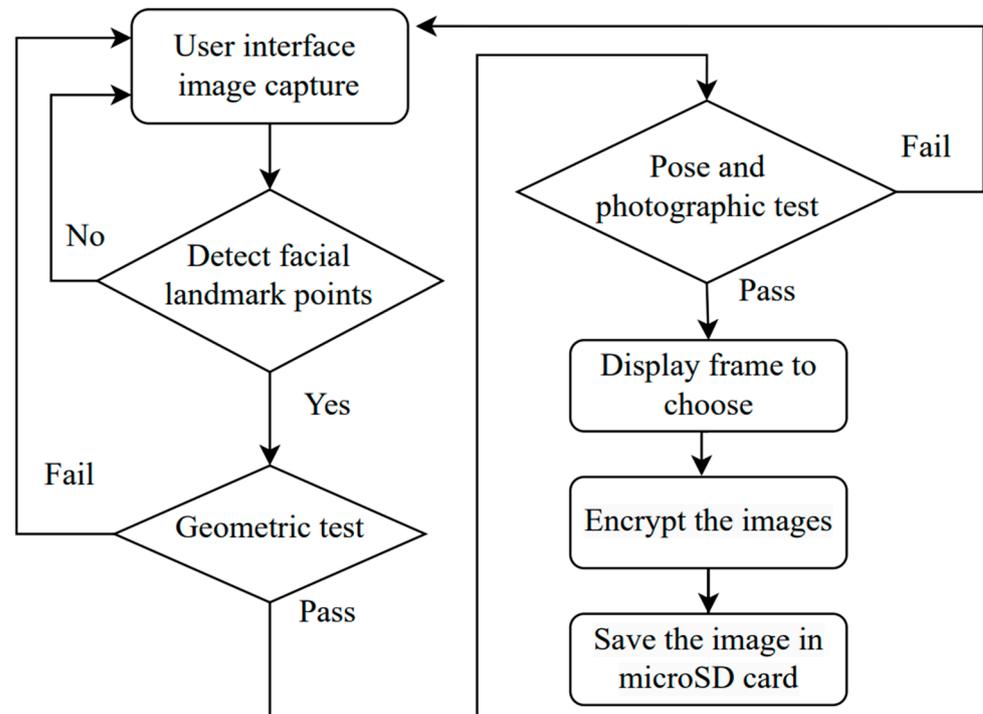
Figure 3. Overview of face-aware capture system software.

The system detects the presence of a face and proceeds to assess several criteria to determine the best facial image for capture, providing the user with feedback to move accordingly. After detecting the face, the system detects an empirical subset of facial landmark points using a facial landmark point detector [33]. After taking the landmark points, we perform geometric and photographic tests. The geometric characteristics of the full-frontal face image based on ISO/IEC-19794-5 are shown in Figure 4, and the specifications are described in Table 1. If the geometric and photographic tests are successful, that indicates a high-quality facial image. The system displays four best-quality images on a Liquid Crystal Display (LCD) to choose the desired photo to save; we provide four best-quality images to choose from. 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 or authorized person can only decrypt these images with the provided secure key generated by the system; thus, it remains secure.

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

Test	Parameters
Geometric tests	Eye distance (min 90 pixels) Vertical position (0.3 B $<$ M < 0.5 B$'$) Horizontal position (0.45 A $<$ M < 0.55 A) Head image width ratio (0.5 A $<$ CC < 0.75 A) Head image height ratio (0.6 B $<$ DD < 0.9 B$'$)

Table 1. *Cont.*

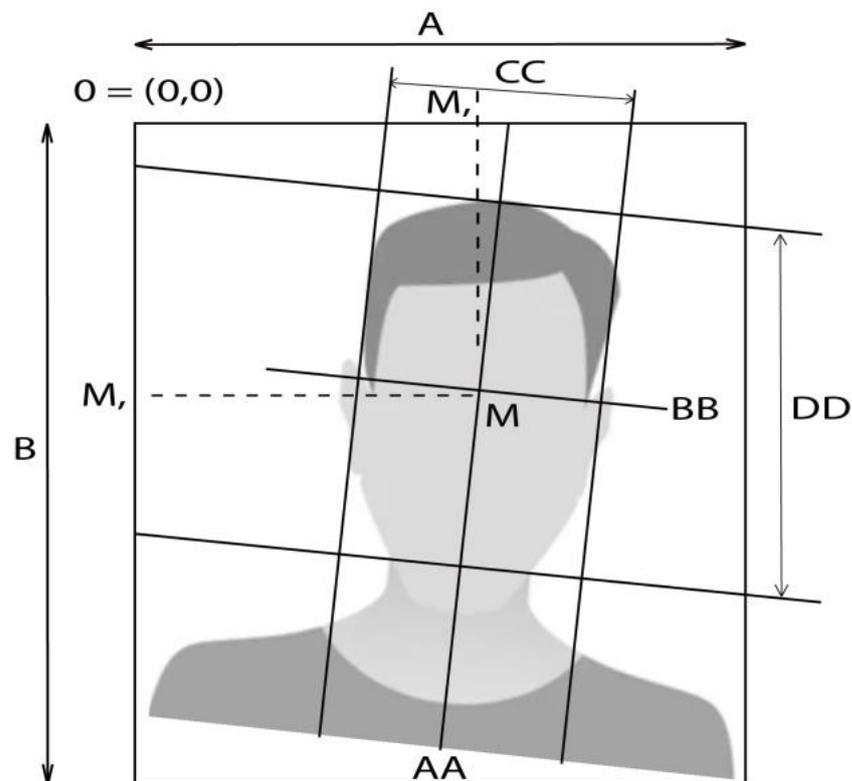| Test	Parameters
Photographic and pose-specific tests	Blurred Looking Away Unnatural Skin Tone Too Dark/Light Washed Out Pixelation Red Eyes Eyes Closed Mouth Open Varied Background Roll/Pitch Greater than 8°

Figure 4. Geometric measurements of the full-frontal face image based on ISO/IEC-19794-5 [34].

3.1. Geometric Test

After detecting the face, the system then conducts geometric measurements, including the ratio of eye distance to head position. Geometric characteristics of the full-frontal face image from the ISO/IEC 19794-5 standard are shown in Figure 4. We used the Python library dlib [33] to detect 68 landmark points and took the empirical subset of 17 landmark points, as shown in Figure 5. Eye distance is calculated by taking the Euclidean distance of points (39 and 42). Depending on ISO standards, the vertical position of the head should be between 30% and 50% of the image height, and the horizontal position of the head should be between 45% and 55% of the image width. To achieve head positioning and maintain the standard ratio shown in Table 1, we placed a bounding box on the frame, as shown in Figure 6. The horizontal and vertical position of the head is determined by the center position of the nose (center of points 28, 32, and 36) in the frame. The system feedback is shown on top to help users align their faces to the box, simplifying the process of achieving correct horizontal and vertical positioning.
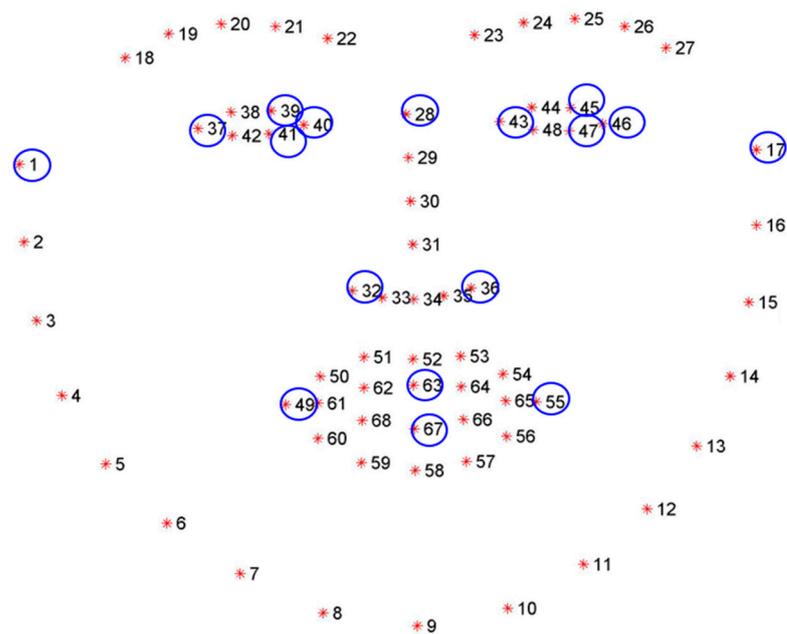
Figure 5. The empirically selected subset (circled in blue) of 68 landmark points used to analyze face quality parameters.
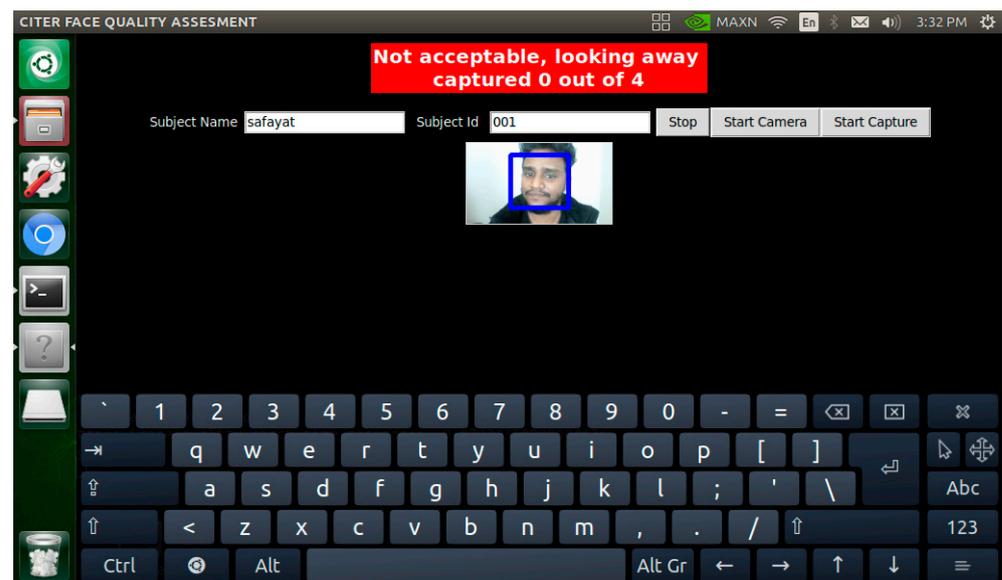

Figure 6. The user interface was developed to give feedback to the user with the bounding box (blue color) for head alignment.

3.2. Photographic and Pose-Specific Tests

After the geometric analysis (shown in 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 pitch angles represent vertical rotation around a vertical axis indicating left and right rotation of the face, roll angles indicate face rotation about its axis, and yaw angles represent 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. We have calculated pixelation by calculating horizontal and vertical mean gradients. To calculate brightness, we calculated the Euclidean norm for each pixel vector and took the average value.

Different techniques are used to detect the blurriness of an image, such as Fast Fourier Transform (FFT), Haar Wavelet Transform (HWT), Laplacian Operator (LAP), etc. [35].

Laplacian-based approaches are popular for blur detection [36,37]. We have used a variance of the Laplacian values across the entire image to detect blur values [38].

$$Variance\ of\ Laplacian\ (VarL) = \frac{1}{WH}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}\left(\nabla^2 f(x,y) - \mu\right)^2$$

where W and H are the image width and height, respectively, $\nabla^2 f(x, y)$ is the Laplacian value at pixel (x, y), and μ is the mean of the Laplacian values of the whole image. If $VarL > T$, then the image is identified as blurred.

To check if the background is white or not, we took 3% of the image from the top and checked the RGB mean intensity. The background is likely white if the average red, green, and blue are above a threshold (200 was empirically selected). Any channel below suggests the background is not fully white.

We determined if the image was washed out or not by analyzing the histogram of the image. Through the examination of this distribution of pixel intensities, the histogram exposes the washed-out appearance of the image. A washed-out image will typically show a histogram heavily skewed towards the brighter end, with fewer pixels in the darker regions. We put the high threshold at 80% and the low threshold at 10%.

Whether eyes are open or closed is detected by calculating each eye separately. Whether the left eye is open or closed is determined by the distance ratio of points (43 and 46) and (45 and 47). The state of the right eye is determined by the distance ratio of (37 and 40) and (39 and 41). To detect red eyes, the system crops the pupil area of both eyes and analyzes them for a high concentration of red pixels. Whether the mouth is open or closed is determined by the distance ratio (49 and 55) and (63 and 67). The system calculates the roll or pitch of the face by measuring the angle between an imaginary horizontal line drawn across key facial landmarks (points 1 and 17) and the horizontal axis of the image. A tilt of less than 8 degrees is considered acceptable.

3.3. Encryption

We used the Advanced Encryption Standard (AES) algorithm of the Python py-Cryptodome [39] module in the Cipher Block Chaining (CBC) mode to encrypt the image. We encrypted the data before saving it 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 U.S. Passport office. AES is a cryptographic algorithm employed for protecting electronic data. AES uses 128, 192, or 256-bit keys; here, we have used AES-128. The adoption of AES encryption adds an additional layer of assurance to our face-aware capture system. The algorithm performs multiple rounds of encryption, and the number of rounds depends on the key length. For example, a key size of 32 bytes 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 [31]. The decryption of the 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.

4. Hardware Design

The core hardware components of the prototype shown in Figure 7 include a high-resolution RGB 16 MP 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 then performs image processing and face quality assessments to identify the best possible images for further processing.

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 (manufacturer NVIDIA Corporation, USA), providing users with versatile options for interacting with the system.
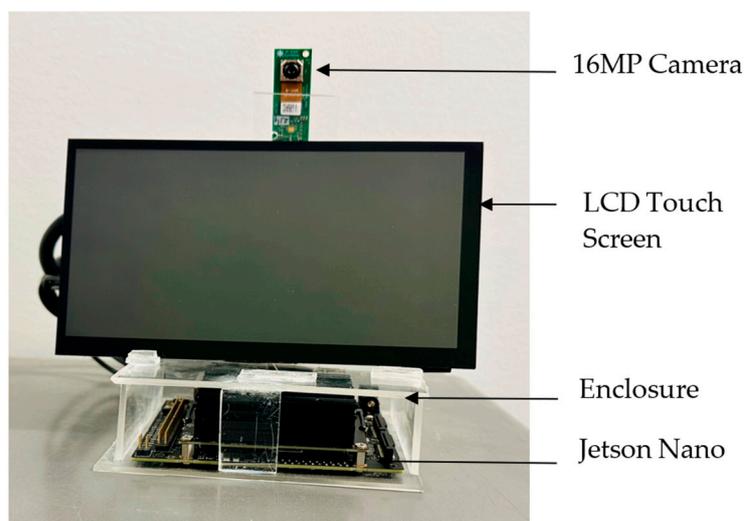

Figure 7. Components of face-aware capture system: The Jetson Nano processor, LCD touchscreen, and a 16 MP camera.

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 (Arm, Cambridge, UK) processor and 4 GB 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 on the market, such as Raspberry Pi 4 model B [40] and BeagleBone Black [41]. Compared to those boards, Jetson Nano performs better in image processing [42].

4.2. Camera

To build a face-aware capture system, the camera must have the capability to autofocus and auto-brightness control because manual brightness and focus control take time. The See3CAM_160 camera (manufacturer E-Con systems, Chennai, India), which is a 16 MP RGB camera with autofocus and USB 3.1 Gen 1 support, utilizes the 1/2.8″ IMX298 CMOS (Sony Semiconductor Manufacturing Corporation, Kumamoto, Japan) image sensor and focuses from 100 mm to Infinity [43]. This camera has auto-brightness control so that it can work in a wide range of lighting conditions.

4.3. Display

We intend to build a system that can be used as a kiosk-like system, where the user can interact with the system. Thus, our face-aware capture system is equipped with an Ingcool seven-inch HDMI LCD touchscreen IPS display featuring a resolution of 1024 × 600. The display operates on 5 V power, allowing it to be powered directly from the USB ports of the Jetson Nano.

4.4. Enclosure

The enclosure for our system measures 120 × 100 × 40 mm and is crafted from a 3 mm acrylic sheet, as depicted in Figure 8. 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 GitHub repository [44].
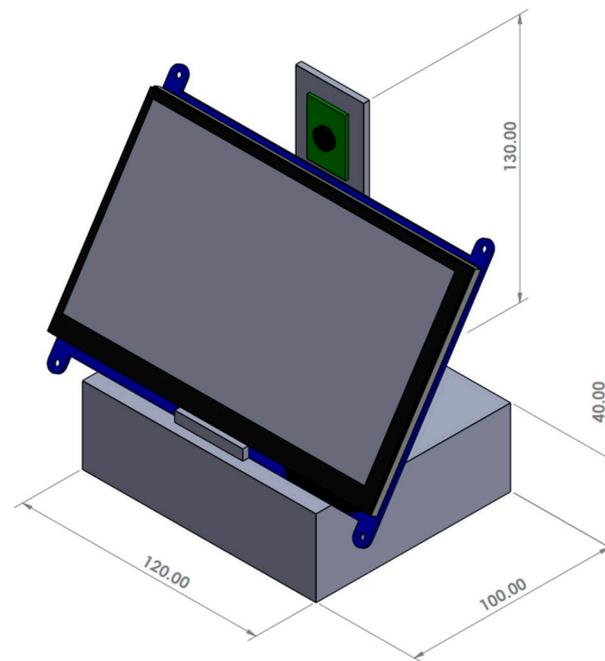

Figure 8. Three-dimensional design of face-aware capture system enclosure with measurements in millimeters (mm).

5. Software Installation and Implementation

The necessary components of the Jetson Nano Developer Kit 4 GB include a microSD card (we have used 128 GB), a compatible power supply, a keyboard, a mouse, a display (HDMI-compatible), and an internet connection. Next, we downloaded the latest version of the microSD card flash tool, BalenaEtcher [45], and the Ubuntu 18.04.5 LTS (Canonical, London, UK, modified by NVIDIA corporation, USA) image from the Nvidia website [46]. After flashing the image onto the microSD card, we inserted it into the Jetson Nano, connected the peripherals, and powered it up. We then followed the on-screen instructions to complete the initial setup, including configuring the language, network settings, and user account. The Python version was Python 3.6.9. For face detection, we have used dlib-19.21. The GitHub repository has all the instructions to install and run the software [44].

## 6. 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 U.S. Travel government passport image check website [32].

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 manually adjusted the camera's height depending on the participant's height. Table 2 summarizes demographic details about the subjects, including the distributed gender representation, ethnicities, and associated age range.

We have collected 1920 × 1080 images in the pilot study. The data collection included over 6000 images captured, with 50 images of each participant passing quality checks using our software. The rejected images were saved for further analysis. Figure 9 displays a comparison of rejected and acceptable images. The left-hand side images were rejected due to issues such as the mouth being 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.

Table 2. Subject's 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
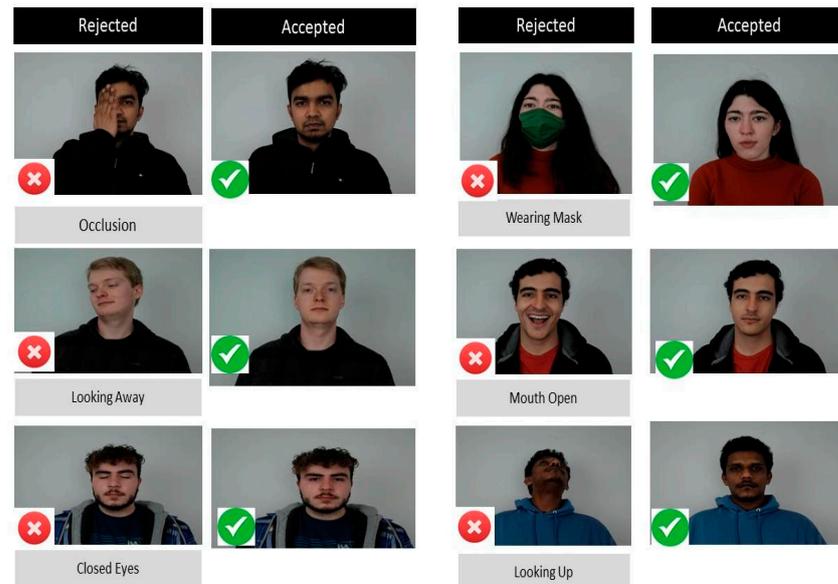
Figure 9. Examples of accepted and rejected images.

After collecting the pilot data, we conducted a rigorous comparison with the U.S. Travel government passport image check website [32]. We randomly took three images from each of our subjects and tested them there. Of the images considered acceptable by our face-aware capture system, 98.98% were accepted by the U.S. government passport image check website [32], as shown in Table 3. Only one image was rejected due to a compression issue. An example of an accepted image tested on the U.S. Travel website is shown in Figure 10. While analyzing the image we also calculated how much time it takes to process real-time analysis by the Jetson Nano. Table 4 shows the time it takes to perform a single-frame analysis. The Jetson Nano takes 0.075 s to process each frame in real-time.

While collecting pilot data, we saved both accepted and rejected images using our developed hardware and software. We then analyzed the rejected data to identify the most common reason for rejection. As shown in Figure 11, head position alignment issues were the most frequent, accounting for 45.16% of rejections. We collected the data in a controlled environment using a high-quality, fast camera. As a result, issues such as washout and blurriness were reduced.

Table 3. Test results on the U.S. government passport website.

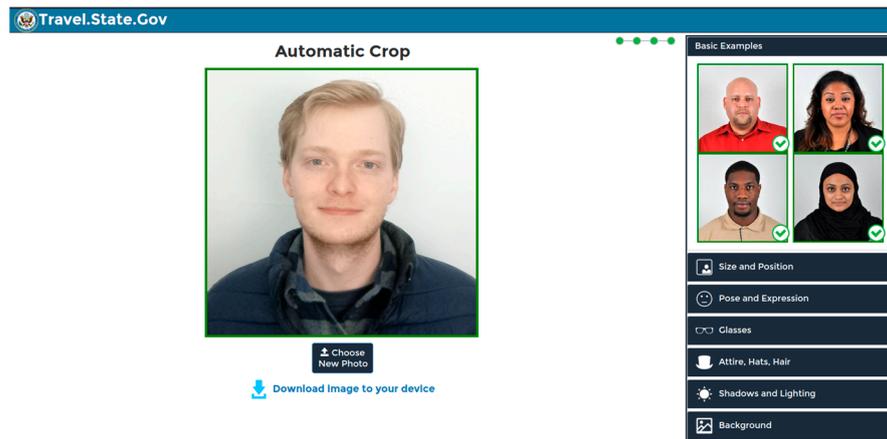| Ethnicity	No. of Subject	No. of Test Image	Accepted	Rejected	Accuracy
Caucasian	24	72	72	0	100%
Asian	11	33	32	1	96.96%
Hispanic	4	12	12	0	100%
Average					98.98%

Figure 10. Screenshot of accepted image on the U.S. Travel website.

Table 4. Type of quality checks and corresponding time taken for each task in seconds.

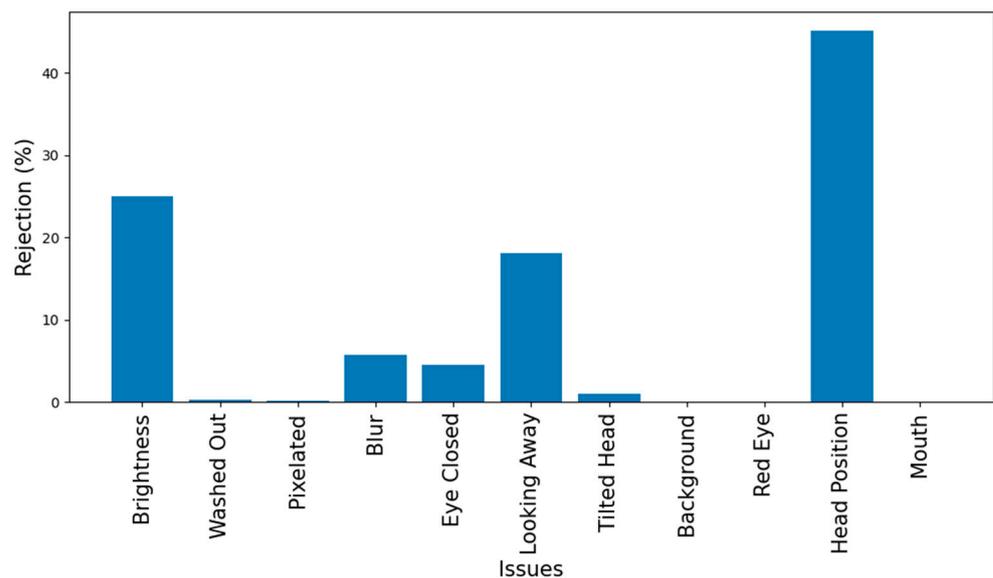| Operation	Time (s)
Brightness check	0.004549
Background color check	0.001094
Blur photo check	0.001533
Image washed-out check	0.000539
Pixelation check	0.003152
Landmark point detection	0.032035
Jaw angle time	0.000037
Eye distance	0.000312
Red-eye detector	0.000306
Mouth distance	0.000139
Total time per frame	0.075623

Figure 11. Issues with rejected images of pilot data collection.

7. Discussion

A novel open-source, 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 rate for accepted images on the U.S. Travel website.

One significant step towards enhancing the biometric 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 proactively addressed the shortcomings and ensured that only high-quality images were considered for biometric enrolment by implementing ISO standards. Integrating 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 4 GB for its processing capabilities, featuring a Quad-core ARM A57 @ 1.43 GHz processor and 4 GB 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 4 GB processor, we achieved a running speed of up to ten frames per second. Because the Jetson Nano 4 GB takes 5 to 10 watts of power, in our future research endeavors, we aim to further reduce power consumption, for example by creating our Printed Circuit Board (PCB) by taking only the necessary components that are crucial for our application.

To minimize technical issues, we employed a 16 MP camera with autofocus. Additionally, at application startup, the camera calibrates itself, effectively eliminating blurry or washed-out images. A white background was used during data collection, resulting in zero background-related rejections. While we tested the system's ability to handle red-eyed images, none were encountered during the pilot data collection phase.

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. An important variable that we did consider from the beginning in the collection of our data was the diversity of subjects. 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 did not include skin tone detection in our system. Skin tone detection would help detect spoofing attacks such as wearing a mask or artificial skin. We were not able to implement yaw detection (the angle of looking up and looking down) as we were using a 2D camera. 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 adjust the height automatically using a motorized solution.

In this project, we did not implement face tracking, as the intention was to capture a passport photo. We assumed that only one person would be in front of the camera. However, in any system where multiple people are supposed to be present and need to be identified, a tracking algorithm would need to be implemented.

To improve the processing time, we will explore other deep learning-based models, retrain the landmark point detector for a smaller number of points, and conduct hyperparameter tuning.

For detecting the background, we took a small portion of the background and checked whether it was white or not. The algorithm we used here can only detect the face, so we could not separate the background from the face using this algorithm. A better way could be to separate the background from the participant and check the background color.

The techniques we used to detect blur, pixelation, and image wash-out are not universal for every situation. These calculations are sensitive to noise, and lighting variations can be influenced by image content with sharp edges or high contrast, leading to false positives. Implementation of deep learning or machine learning-based algorithms could improve accuracy.

To improve the design, 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. Changes in the camera will be left open for future consideration.

8. Conclusions

In conclusion, this paper presented a novel open-source, face-aware capture system that utilizes real-time image quality analysis to significantly improve facial biometric authentication and image acquisition. Pilot data demonstrated a high accuracy of 98.98% in capturing good-quality images, addressing a critical challenge in this field. Determining appropriate thresholds for assessing good image quality across diverse skin tones and lighting conditions presented a significant challenge. The system prioritizes user experience with a touch-enabled interface and leverages open-source hardware, promoting ease of deployment. By adhering to ISO standards, the system ensures consistent and reliable image quality across diverse capture scenarios. This secure and portable solution has the potential to improve facial biometric enrollment in security systems that require access control and identity verification, enhancing the overall efficacy and trustworthiness of these applications in real-world settings. Further research is necessary to explore advanced algorithms for improved detection of washed-out images and blur in diverse lighting conditions. Machine learning and deep learning approaches may perform better in this area. Additionally, incorporating 3D camera technology could enhance the system's robustness by enabling accurate yaw angle detection and liveness detection.

References

1. Sanchez del Rio, J.; Moctezuma, D.; Conde, C.; Martin de Diego, I.; Cabello, E. Automated Border Control E-Gates and Facial Recognition Systems. *Comput. Secur.* **2016**, *62*, 49–72. [CrossRef]
2. Biometrics | U.S. Customs and Border Protection. Available online: https://www.cbp.gov/travel/biometrics (accessed on 28 August 2023).
3. Grother, P.; Tabassi, E. Performance of Biometric Quality Measures. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 531–543. [CrossRef] [PubMed]
4. Mahmood, Z.; Ali, T.; Khan, S.U. Effects of Pose and Image Resolution on Automatic Face Recognition. *IET Biom.* **2016**, *5*, 111–119. [CrossRef]
5. Aldrian, O.; Smith, W.A.P. Inverse Rendering of Faces with a 3D Morphable Model. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *35*, 1080–1093. [CrossRef] [PubMed]
6. Wiskott, L.; Fellous, J.-M.; Kruger, N. Face Recognition by Elastic Bunch Graph Matching. *IEEE Trans. Pattern Anal. Mach. Intell.* **1997**, *19*, 7. [CrossRef]
7. Blanz, V.; Vetter, T. Face Recognition Based on Fitting a 3D Morphable Model. *IEEE Trans. Pattern Anal. Mach. Intell.* **2003**, *25*, 1063–1074. [CrossRef]
8. Chen, J.; Deng, Y.; Bai, G.; Su, G. Face Image Quality Assessment Based on Learning to Rank. *IEEE Signal Process. Lett.* **2015**, *22*, 90–94. [CrossRef]
9. Home. Available online: https://www.icao.int/Pages/default.aspx (accessed on 7 March 2024).
10. U.S. Passports. Available online: https://travel.state.gov/content/travel/en/passports.html (accessed on 23 February 2024).
11. U.S. Passport Photos. Available online: https://travel.state.gov/content/travel/en/passports/how-apply/photos.html (accessed on 25 June 2022).
12. Labati, R.D.; Genovese, A.; Muñoz, E.; Piuri, V.; Scotti, F.; Sforza, G. Advanced Design of Automated Border Control Gates: Biometric System Techniques and Research Trends. In Proceedings of the 2015 IEEE International Symposium on Systems Engineering (ISSE), Rome, Italy, 28–30 September 2015; pp. 412–419.
13. Noori, S. Suspicious Infrastructures: Automating Border Control and the Multiplication of Mistrust through Biometric E-Gates. *Geopolitics* **2022**, *27*, 1117–1139. [CrossRef]
14. Oostveen, A.-M.; Kaufmann, M.; Krempel, E.; Grasemann, G. Automated Border Control: A Comparative Usability Study at Two European Airports 2014. In Proceedings of the 8th International Conference on Interfaces and Human Computer Interaction (IHCI 2014), Lisbon, Portugal, 14–17 July 2014.
15. Bingöl, Ö.; Ekinci, M. Stereo-Based Palmprint Recognition in Various 3D Postures. *Expert Syst. Appl.* **2017**, *78*, 74–88. [CrossRef]
16. Biometrics, A. Biometrics Simplified. Available online: https://www.aware.com/ (accessed on 21 August 2023).
17. Hernandez-Ortega, J.; Galbally, J.; Fierrez, J.; Haraksim, R.; Beslay, L. FaceQnet: Quality Assessment for Face Recognition Based on Deep Learning. In Proceedings of the 2019 International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; pp. 1–8.
18. Lijun, Z.; Xiaohu, S.; Fei, Y.; Pingling, D.; Xiangdong, Z.; Yu, S. Multi-Branch Face Quality Assessment for Face Recognition. In Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 16–19 October 2019; pp. 1659–1664.
19. Kumar, V.D.A.; Kumar, V.D.A.; Malathi, S.; Vengatesan, K.; Ramakrishnan, M. Facial Recognition System for Suspect Identification Using a Surveillance Camera. *Pattern Recognit. Image Anal.* **2018**, *28*, 410–420. [CrossRef]
20. Kleihorst, R.; Reuvers, M.; Krose, B.; Broers, H. A Smart Camera for Face Recognition. In Proceedings of the 2004 International Conference on Image Processing, 2004. ICIP '04, Singapore, 24–27 October 2004; Volume 5, pp. 2849–2852.
21. Al-Faris, M.; Chiverton, J.; Ndzi, D.; Ahmed, A.I. A Review on Computer Vision-Based Methods for Human Action Recognition. *J. Imaging* **2020**, *6*, 46. [CrossRef]
22. Iancu, C.; Corcoran, P.; Costache, G. A Review of Face Recognition Techniques for In-Camera Applications. In Proceedings of the 2007 International Symposium on Signals, Circuits and Systems, Iasi, Romania, 13–14 July 2007; Volume 1, pp. 1–4.
23. Suryowinoto, A.; Herlambang, T.; Tsusanto, R.; Susanto, F.A. Prototype of an Automatic Entrance Gate Security System Using a Facial Recognition Camera Based on The Haarcascade Method. *J. Phys. Conf. Ser.* **2021**, *2117*, 012015. [CrossRef]
24. Innovative Contactless Palmprint Recognition System Based on Dual-Camera Alignment | IEEE Journals & Magazine | IEEE Xplore. Available online: https://ieeexplore.ieee.org/abstract/document/9707646 (accessed on 17 January 2024).
25. Chowdhury, A.M.M.; Hossain, S.M.S.; Sarker, M.A.B.; Imtiaz, M.H. Automatic Generation of Synthetic Palm Images. In Proceedings of the Interdisciplinary Conference on Mechanics, Computers and Electrics, Barcelona, Spain, 6–7 October 2022.
26. Sarker, M.A.B.; Sola-Thomas, E.; Jamieson, C.; Imtiaz, M.H. Autonomous Movement of Wheelchair by Cameras and YOLOv7. *Eng. Proc.* **2023**, *31*, 60. [CrossRef]
27. Lindner, T.; Wyrwał, D.; Białek, M.; Nowak, P. Face Recognition System Based on a Single-Board Computer. In Proceedings of the 2020 International Conference Mechatronic Systems and Materials (MSM), Bialystok, Poland, 1–3 July 2020; pp. 1–6.
28. Caracciolo, M.V.; Casciotti, O.; Lloyd, C.D.; Sola-Thomas, E.; Weaver, M.; Bielby, K.; Sarker, M.A.B.; Imtiaz, M.H. Autonomous Navigation System from Simultaneous Localization and Mapping. In Proceedings of the 2022 IEEE Microelectronics Design Test Symposium (MDTS), Albany, NY, USA, 23–26 May 2022.

29. Sola-Thomas, E.; Sarker, M.A.B.; Caracciolo, M.V.; Casciotti, O.; Lloyd, C.D.; Imtiaz, M.H. Design of a Low-Cost, Lightweight Smart Wheelchair. In Proceedings of the 2021 IEEE Microelectronics Design & Test Symposium (MDTS), Albany, NY, USA; 2021; pp. 1–7. [CrossRef]

30. Sarker, M.A.B.; Sola, P.S.T.; Jones, A.; Laing, E.; Sola-Thomas, E.; Imtiaz, M. Vision Controlled Sensorized Prosthetic Hand. In Proceedings of the Interdisciplinary Conference on Mechanics, Computers and Electrics (ICMECE 2022), Barcelona, Spain, 6–7 October 2022.

31. Dworkin, M.J. *Advanced Encryption Standard (AES)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023; p. NIST FIPS 197-upd1.

32. Photo-Tool. Available online: https://tsg.phototool.state.gov/photo (accessed on 18 August 2023).

33. Davisking/Dlib: A Toolkit for Making Real World Machine Learning and Data Analysis Applications in C++. Available online: https://github.com/davisking/dlib/tree/master (accessed on 18 August 2023).

34. Ferrara, M.; Franco, A.; Maio, D.; Maltoni, D. Face Image Conformance to ISO/ICAO Standards in Machine Readable Travel Documents. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1204–1213.

35. Pagaduan, R.A.; Aragon, R.; Medina, R.P. iBlurDetect: Image Blur Detection Techniques Assessment and Evaluation Study. In Proceedings of the International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies, Virtual, 17–18 September 2020; SCITEPRESS—Science and Technology Publications: Medan, Indonesia, 2020; pp. 286–291.

36. Aravinth, S.S.; Gopi, A.; Chowdary, G.L.; Bhagavath, K.; Srinivas, D.R. Implementation of Blur Image to Sharp Image Conversion Using Laplacian Approach. In Proceedings of the 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 20–22 October 2022; pp. 339–345.

37. Bianchi, D.; Buccini, A.; Donatelli, M.; Randazzo, E. Graph Laplacian for Image Deblurring 2021. *arXiv* **2021**, arXiv:2102.10327.

38. Gonzalez, R.C.; Woods, R.E. *Digital Image Processing*, 4th ed.; Pearson: New York, NY, USA, 2018; ISBN 978-0-13-335672-4.

39. Eijs, H. Pycryptodome: Cryptographic Library for Python. Available online: https://www.pycryptodome.org (accessed on 5 March 2024).

40. Raspberry Pi 4 Model B. Available online: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/ (accessed on 29 August 2023).

41. BeagleBone®Black. BeagleBoard. Available online: https://www.beagleboard.org/boards/beaglebone-black (accessed on 19 August 2023).

42. Crazy Engineer. Nvidia Jetson Nano vs Raspberry Pi 4 Benchmark. Arnab Kumar Das 2021. Available online: https://www.arnabkumardas.com/topics/benchmark/nvidia-jetson-nano-vs-raspberry-pi-4-benchmark/ (accessed on 29 August 2023).

43. See3CAM_160—16MP (4K) Autofocus USB 3.1 Gen 1 Camera Board (Color). Available online: https://www.e-consystems.com/usb-cameras/16mp-sony-imx298-autofocus-usb-camera.asp (accessed on 16 August 2023).

44. Sarker, M.A.B. Baset-Sarker/Face-Aware-Capture 2024. Available online: https://github.com/baset-sarker/face-aware-capture (accessed on 1 March 2024).

45. balenaEtcher—Flash OS Images to SD Cards & USB Drives. Available online: https://etcher.balena.io/ (accessed on 27 February 2024).

46. Get Started with Jetson Nano Developer Kit. Available online: https://developer.nvidia.com/embedded/learn/get-started-jetson-nano-devkit (accessed on 27 February 2024).