Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REAL-TIME HUMAN FACE ANONYMIZATION SYSTEM FOR SERVICE ROBOTS

[1]GERMAN ROJAS, [2]JASON MARTÌNEZ, [3]FREDY MARTÍNEZ
Facultad Tecnológica, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia
E-mail: [1]garojass@correo.udistrital.edu.co, [2]jarmartinezg@correo.udistrital.edu.co, [3]fhmartinezs@udistrital.edu.co

ABSTRACT

Like any other computer system, robots are susceptible to security problems that could lead to unauthorized disclosure of private information. While it is true that these systems in critical applications (industrial or medical level for example) can result in great damage to equipment and people, in addition to the costs involved with data leakage, domestic applications, in particular service robots, cannot be left aside. A security breach in a system that stores private information puts the security of all individuals in a family group at risk. The communication capabilities of these systems can make them targets for attacks that can seriously compromise the privacy and security of their users. As a sensor system for human environments, it is normal for these robots to incorporate cameras as an important element of their interaction system, similar to the way human eyes do. This research presents an anonymization strategy for all video signals captured by a home service robot as a way to reduce unnecessary personal information captured by these cameras and to increase the confidence of use by users. We propose the use of an algorithm capable of identifying and distorting faces in real-time from the video input of the robot. This process is performed with the original video signal ensuring that no human face is digitized by the robot. The algorithm was evaluated on the ARMOS TurtleBot platform for different operating conditions, demonstrating more than sufficient performance for general robot applications. This strategy will be combined in the future with other systems under investigation by the research group related to source encryption protocols.

Keywords: *Anonymization, Human face, Personal information, Privacy, Real-time, Service robots*

1. INTRODUCTION

Robots are designed to support humans in performing tasks [1, 2, 3]. These systems must operate in human environments, and interact with humans, so it is common for them to be equipped with sensing, actuation, and processing capabilities equivalent to those of humans [4, 5]. Human environments present by design certain restrictions that suggest specific characteristics for robots [6, 7]. For example, for indoor applications, bipedal locomotion systems are considered instead of wheeled or tracked systems, since the robot may have to avoid elements on the floor or use a ladder. Something similar happens with the interaction of the robot, it is coherent to think that the most convenient way to identify a door, a ball, or a person is using an optical sensor equivalent to the human eye [8, 9, 10]. This is why many service robots (which generally support people in indoor environments) have one or more cameras as their main sensor. These cameras not only collect information necessary for their operation but also collect sensitive personal information.

According to its function, and as a performance requirement, it is normal that these cameras, as well as other sensors, are continuously collecting information from the environment [11]. The robot continuously performs many activities related to relative localization, global localization, identification of the user's needs, navigation tasks, etc. The information collected by its sensors is sometimes filtered and discarded, but at other times it is stored for further processing and/or communication [12, 13, 14]. The user is aware of this every time he recognizes that the robot (or any other system) has a camera. Unless the robot is using user information to improve its task performance (e.g., identifying emotional states from the face), visual information from users (particularly children) is irrelevant to its operation [15]. However, the storage and communication of such information may be subject to security issues if unauthorized persons or systems gain access to the storage or communication.

In general, users' greatest concern about service robots relates to the potential physical harm that these robots may cause to users, other individuals, or their property [16, 17]. This is true given that robots are found operating in a wide variety of environments, from autonomous cleaning systems to complex systems that perform surgery on patients, to military and industrial applications. However, a less obvious problem is the potential exposure of users' privacy if the information these robots have access to is accessed in an unauthorized manner [18, 19]. Home service robots have access to sensitive personal information, including that related to children. Private images of children as well as other household members may be stored on these systems, information that can be compromised if accessed by criminals.

In terms of information security, threats to an artificial system can be classified into at least one of three types: confidentiality, integrity, and availability of information [20, 21]. The confidentiality threat is related to the leakage of private data without the authorization of the owner of such information. The integrity threat is related to the modification of information without the owner's authorization, and the availability threat refers to the loss of information. Threats of privacy, authentication, and authorization also appear in an assistive robot [22]. These threats do not neglect the possible physical damage caused by any of them.

Service robots are rapidly spreading to a wide variety of applications [23, 24, 25]. It is now common to find them in homes as well as in commercial spaces. Typical applications of these robots are welcome and information assistants in hotels, banks, shopping malls, etc., electronic pets and interactive toys, intelligent audio players, or even household appliances such as refrigerators and clothes washers. The location and interaction of these robots with humans cause them to collect a large amount of personal information that in many cases exceeds their requirement for the development of a task [9, 26, 27]. It is probably important for a robot dog to identify the position and movement of a child, but it doesn't need to record and memorize the child's face. Other sensitive information such as age, weight, consumption habits, schedules, etc. also constitutes private data that although not focused on in this research as a primary problem, are part of the overall problem and should be attacked simultaneously [28].

The leakage of private information is something that has already been detected in commercial systems. Perhaps the most documented case is that of the Cayla doll (Vivid Toy Group), which has been banned and ordered to be destroyed by the German Federal Network after an investigation showed that it was possible to access its Bluetooth communication device in an unauthorized way and come into direct contact with children [29, 30]. Although this doll is only a proven case, the fact is that there are multiple commercial systems and robots on the market that could lead to similar situations. Service robots present a unique concern in this regard, since in addition to cameras they interact directly with users, and are capable of collecting a lot of private and confidential information that can be illegally accessed for commercial or criminal gain [31, 32].

2. PROBLEM STATEMENT

Automated electronic systems, and in particular, service robots, are highly integrated into today's everyday life. For their integration with human beings, these systems tend to be equipped with sensing, processing, and communication systems that in many cases exceed the minimum amount of information required for their operation, and easily manipulate the personal data of their users, whose privacy can be compromised causing serious security problems.

Among the sensors that cause the greatest concern in terms of potential privacy problems are digital cameras. Through them, an autonomous robotic system can continuously record the privacy of a home or office, including access to images of minors [33]. If it is taken into account that these robots have extensive communication capabilities that would allow the leakage of information, it is clear that a guarantee is required to provide security to the user regarding the use of these robots.

We propose the development of a system capable of avoiding such information leakage by preventing sensitive information from being obtained first by the robot. As a strategy to minimize the severity of these concerns, it is proposed to establish a digital image processing protocol as the first pre-processing stage for any visual capture system installed on a service robot. In this sense, such a system should take the video signal directly from the sensor, and process it to eliminate personal information that could lead to explicitly identify the users. This protocol must identify and distort in real-time the face of any person registered by the robot.

Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. METHODS

The strategy selected to process the video signal captured by the camera corresponds to a facial blur. Our robotic platform, ARMOS TurtleBot has an embedded system based on Arrow's DragonBoard 410c board with Linux Debian operating system. Python and OpenCV have been implemented on this platform as working tools. The objective is to identify and pixelate any face found in the camera images. Fig. 1 shows the general scheme proposed as a solution.

The video is imported directly from the camera with the help of OpenCV. Variables were created that allow adjusting the number of frames per second, capture resolution, and the maximum number of frames for recording. These parameters are not accessible to the end-user, but allow evaluating the performance of the system for different operating conditions. A deep neural network is used to identify the faces in the images, to propagate the data in this network the images are scaled to 224x224 pixels, this does not affect the image quality delivered to the central control unit of the robot.

For face detection, we use the MobileNet-SSD model with pre-trained weights, which corresponds to a Single-Shot multibox Detection (SSD) network trained for this purpose. The model is in the Caffe framework format, which is imported from OpenCV. From there, the regions to be pixelated (location and size) in each frame are identified, the RGB matrices that compose the frame are resized, and the cycle for pixelating each detected face is started.

This process starts with the definition of a frame where a face is presumed to be located. Then, the values of the frame resolution and the values of each step are pre-set to establish the pixel size [34]. A face count variable is also initialized to allow a new detection cycle. The pixelation process of the frame where the face was located is performed by creating a matrix of average values between the three RGB matrices obtained from the face frame. This process is carried out using three cycles, two of them in charge of creating the rows and columns of the pixel matrix, and the third one is in charge of generating the size of each pixel. Once the pixel matrix is built, the matrix is saved in a variable that has the same resolution as the face frame. Finally, the section of the face frame is replaced in the initial frame by the pixelated matrix.

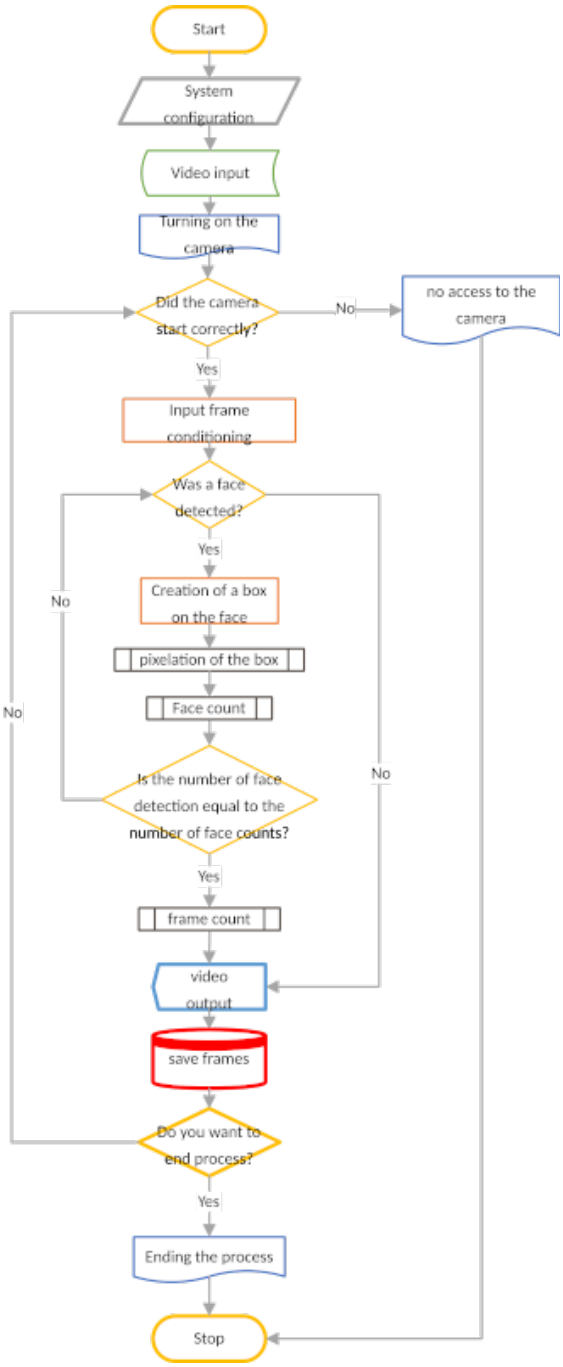

Figure 1: Face pixelation algorithm for service robot

The next step of the process corresponds to the frame counting and sending of the filtered image to the central control unit of the robot. The frame counting is done by measuring the time before processing and after pixelization of the image, a process that has a resolution of up to one microsecond. As for the sending of the processed image, the values obtained corresponding to the number of frames and number of detected faces are

printed on the processed frame. These results are also stored for system performance evaluation.

4. RESULTS

The evaluation of the strategy was performed on the hardware of our ARMOS TurtleBot platform (Fig. 2). Our robot is a caterpillar tracked platform with high payload capacity, designed to transport in indoor human environments other robotic modules on top of it, as user interfaces (in our case, the digital camera) [35].

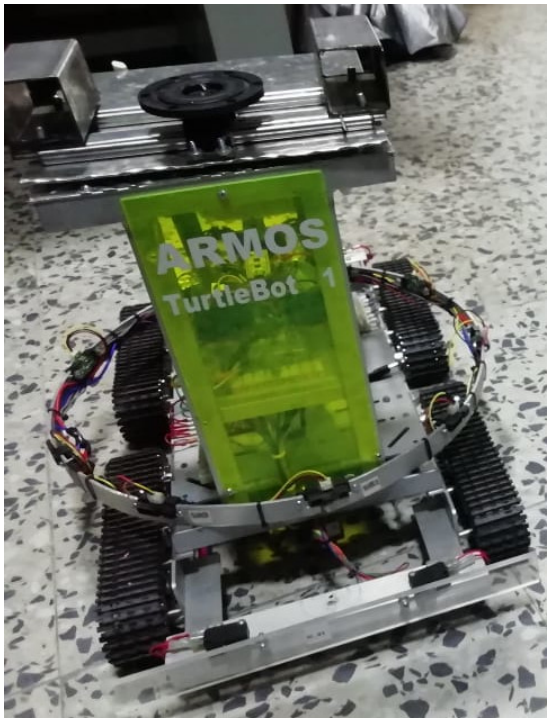

Figure 2: ARMOS TurtleBot

We evaluated the performance of our system for multiple operating options. First, tests were conducted to determine the ability to discriminate human faces when only one user appears in the range of the robot's camera, for different user conditions. Then the number of faces, occlusion levels, position, and types of faces were increased. According to the results, a strong occlusion of the face is needed to prevent the algorithm from recognizing it, showing that it is unable to recognize it only when there is no face to identify in the image.

Figs. 3 to 7 show some of the cases evaluated on the prototype for a single user (face) captured by the camera. The first case shows a test with a distance to the camera of about 0.6 meters, with a strong occlusion of the eyes, forehead, and part of the nose of the user. The purpose is to remove the user's eyes from the image, one of the most important features in recognition algorithms, and to see if it is possible to disorient the algorithm in this way. As can be seen, the scheme not only recognizes the face, but it also eliminates from the pixelated image what does not correspond to it, that is to say, the cutting matrix processes a smaller field excluding the element that hides the eyes. This behavior of the system not only guarantees the identification and pixelation of sensitive information but also reduces the processing capacity required by the system, since it adjusts the processing frame only to the user's personal information, leaving unprocessed information that is not relevant.

Figure 3: Face with large sports glasses

In the next two cases (Figs. 4 to 7) a similar exercise is performed, but trying to occlude the user's mouth. Lenses are also included to try to avoid eye recognition. When the face is facing the camera, the system can identify and pixelate the face, but with a smaller number of frames, so more processing is required to achieve identification, and the response is slower. When the user is in profile (side view) it is observed that the system does not check the contours so that it can identify and pixelate the face (no identification). In these times of global pandemic, it is essential to have surgical masks for health care, even more so if it is for patient care assistance. This is a fundamental reason to be analyzed in our tests, this is a feature that can remain in our society in an undefined way, and the algorithm should be able to identify and anonymize the faces when it is possible to identify the user. From the results it is observed that the system performs the complete cut on the face, achieving a total pixelation. However, this only occurs when the user's eyes are uncovered.

One of the problems of robotic systems is the ability to make decisions when their sensors are

occluded, and therefore the information is not sufficient for decision making. This is true for digital camera-based schemes in tasks such as route planning, tracking, monitoring, multi-agent coordination, and human interaction, among others. Schemes have been proposed in which the robot uses different viewpoints to reconstruct information, or historical data to estimate future behaviors. Our algorithm proposes an alternative solution, in which recognition is performed from partial information. This strategy has proved to be highly efficient and, thanks to the neural model, very reliable.

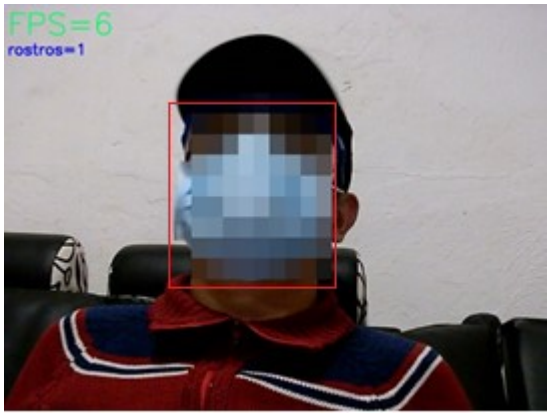

Figure 4: Face with working glasses, cap, and surgical mask

Figure 5: Face with working glasses, cap, and surgical mask, side view

When there is no identifiable information from a human face, the algorithm does not perform any pixel processing. The categorization model does not identify a person with a completely covered face as a person, which reduces unnecessary processing.

Figure 6: Face with sports glasses and surgical mask

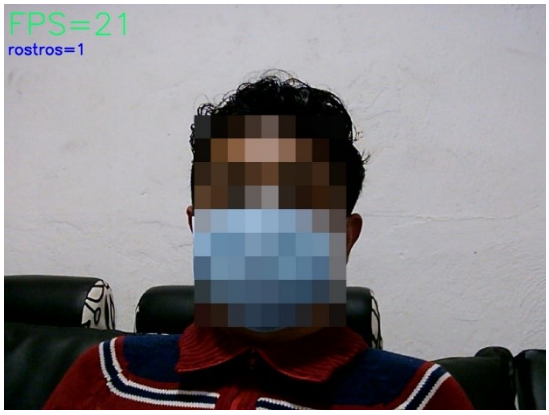

Figure 7: Face with a surgical mask

When there is information in the image that can lead to the identification of a person, regardless of whether part of the face is covered, the scheme chooses to pixelate the relevant information. It is possible to identify a person from their eyes or face shape; in these cases, it is necessary to remove such information from the images.

The following figures show the result of our system with more than one user in the image under different conditions, in particular with different levels of occlusion of the face. Fig. 8 and 9 show two users in front of the robot. In the first case, the two users are at a similar distance in front of the camera, and the only extraneous element is eyeglasses on one of the faces. In the second case, one of the users is asked to completely cover his face with his hand. However, in both cases, the algorithm easily identifies and pixelates the two users.

Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 8: Two faces without strong occlusion of features

Figure 9: Two faces, one with strong occlusion of features

The next pair of tests (Figs. 10 and 11) sought to evaluate the behavior of the system for two users located at different distances, one main user and one in the background of the image. In Fig. 10 the first user was placed at 0.6 m from the robot, while the second user was detected in the background at 1.5 m. In both cases, the algorithm was able to correctly identify the face area and pixelate it with a very high FPS (without excessive computational cost). In Fig. 11 a similar exercise is done, but in this case, the distance of the user in the background is increased, the first user is again located at 0.6 m, while the second user in the background is located at 2.5 m from the robot. Although with a lower FPS the algorithm can correctly detect both users, and correctly perform the anonymization. In principle, the number of faces does not increase the computational cost considerably, but this is something that is evaluated in the following cases.

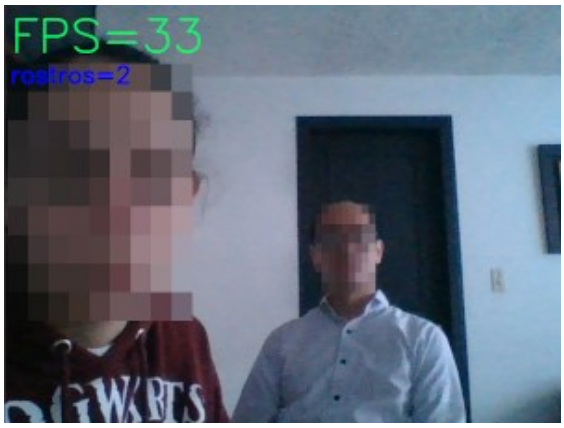

Figure 10: Two faces with a difference in depth

Figure 11: Two faces with a strong difference in depth

The last set of tests was aimed at determining the performance of the system under more demanding conditions, such as a larger number of faces, smaller faces from photographs, minors, and even the presence of pets. In Fig. 12 it can be seen that in the scene there are four people at distances between 1 and 2 m from the robot. This particular test was performed with people of different ages and genders to determine any possible system failures. The system correctly identifies each of the users without considerably computational cost.

Figure 12: Four faces without strong feature occlusion

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 13 shows the behavior of the system in front of a larger number of faces, including the case of faces captured from photographs, which are of smaller size, different lighting, and normally found in the home from pictures on walls and furniture. A total of six faces are found, one of them belonging to the user. Again, the system identifies all the faces and applies frame and distortion to each of them correctly with a good video frequency.

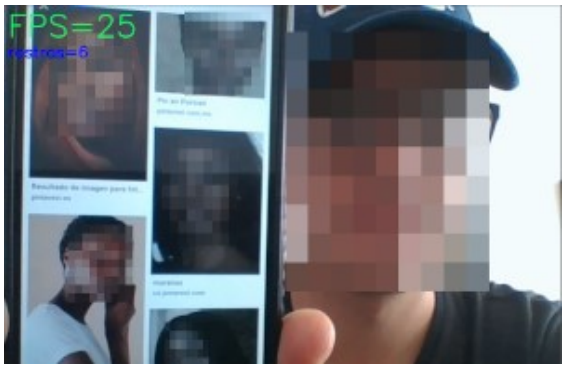

Figure 13: Multiple faces, user and from external sources

A much more extreme case is shown in the test in Fig. 14. The objective of this test was to check the maximum capacity of the algorithm to identify and process faces. For this purpose, an image is presented with a total of 117 faces of which the system manages to identify and anonymize an average of 105 (in some cases, depending on the position, the number increases or decreases, but always around this value). In this case, the computational cost of the algorithm was higher, and the FPS dropped to only 8. Under these conditions, performance reduction was observed, which should be addressed in eventual system improvements.

Figure 14: Multiple faces from external sources

One of the most important objectives of this system is to ensure the privacy of images and videos that include minors. This is perhaps the biggest concern for the average user, to ensure that children in the home are safe. The system must identify and process children's faces efficiently. Fig. 15 shows how the system effectively identifies a child from a photograph (more complex case), establishes the frame, and applies the pixelation correctly, and with very low computational cost. In this sense, the algorithm and the processing strategy can guarantee the complete anonymity of these images.

Figure 15: Two faces, adult and minor

The last test presented illustrates an unintended effect of the system, but demonstrates its ability to identify and process faces. Due to the high capacity of the neural network to categorize elements, in this case, faces, the system is even able to identify and process faces of some pets, in general, those that share general characteristics with the human face. Fig. 15 shows the case of a pet next to the user, a case that can be very common for a service robot. The image shows that it identifies the two faces and processes them without making any distinction between them. However, the FPS drops to 7, indicating that the identification of this pet and its processing turns out to be more computationally expensive than the case of human faces. These performance issues should be considered in future improvements of the system.

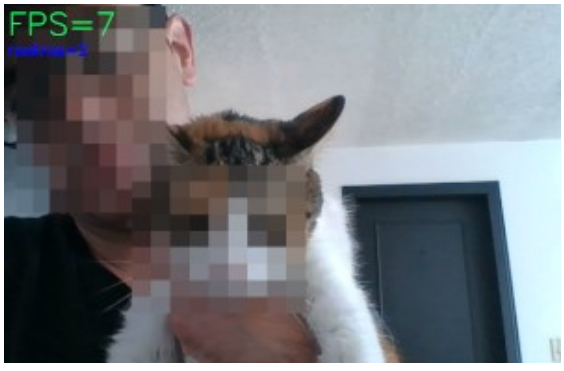

Figure 16: Two faces, adult and feline

The results show a high performance of the system, both in characterizing faces and in pixel-imaging and transmitting them in real-time. The correct identification of faces works very well, the system can identify them despite the existence of partial occlusion, both in eyes, hair and mouth, and even other regions. This is achieved thanks to the identification system based on a neural network, a scheme that in principle shows a high performance and we believe it should be maintained with few modifications in future improvements of the system. On the other hand, the digital image processing with OpenCV is also very good, although performance problems were detected in some specific cases (some types of occlusion, number of faces, and type of faces, such as pets). This part can be intervened in the future to increase the overall performance of the system.

6. CONCLUSION

This paper shows an anonymization system developed as the initial interface of a video capture system for a service robot. The purpose of this system is to guarantee the private identity of robot users, in particular children under the care of the robots, against possible information leaks given the processing and communication capabilities that are being included in these robotic systems. The objective is to prevent the robot's central unit from receiving information that includes people's faces, particularly those of minors. In principle, this personal information is not required for most of the activities of these robots, but it has been proposed that in the future if the user wishes, the anonymization system can be deactivated by the user to allow the operation of personal integration algorithms. The proposed system works from an object identification system (faces), and then a digital pixelation process by image processing. The identification of faces is performed by a pre-trained deep neural network, whose model is loaded and propagated from OpenCV. The result corresponds to the location and size of the faces in each video frame, which is processed one by one by OpenCV. According to the location information, a frame is drawn around each face and then pixelated using the color information of the region. The video is reconstructed and transmitted to the central control unit of the robot. Such a scheme has been implemented on an embedded system with Linux and Python and evaluated in real operation on our ARMOS TurtleBot robotic platform. The laboratory results confirm the performance of the system and its capacity for real use. These results show a high identification capability, even with strong occlusion of the face. It is also observed a large capacity to work with a high number of faces simultaneously, although it is observed that this considerably reduces the video processing speed. To date, the authors are not aware of a similar system, with the same or greater capacity and performance, used in service robots. Future work on the system is aimed at increasing these performance constraints.

7. LIMITATIONS AND FUTURE RESEARCH

Despite the good performance of the system, it is desirable to increase the number of FPS and size of the images processed by the robot. In this sense, it is suggested to upgrade the DragonBoard 410c card in search of higher performance. It is also suggested to increase the storage capacity of the system as a strategy for possible changes in filtered images (modification of historical images). Other alternatives to be explored to increase system performance include moving the coding from Python to Julia, as well as optimizing the processing code. A limitation of the current system is that it does not consider the possible deactivation of the pixel processing using some command to allow some kind of operation on the assistive robot. Many schemes augment their interaction with the user by interpreting animic states, particularly from the face, processes that are limited by the anonymization scheme.

As a short-term development of the research project, it is proposed to explore algorithms based on different methods for face detection, which can mitigate the impact of the processing of this section in each of the frames, and thus obtain greater fluidity in the anonymization of the output video. Another path of research is the incorporation of an algorithm that allows the classification of faces that do not belong to the users (faces detected in photographs or videos, or of animals) so that the system can avoid the consumption of resources generated by processing this information, which in most cases is unnecessary. It is also proposed to advance more performance tests in real conditions on the ARMOS TurtleBot robot.

8. ACKNOWLEDGMENT

This work was supported by the Universidad Distrital Francisco José de Caldas, in part through CIDC, and partly by the Facultad Tecnológica. The

views expressed in this paper are not necessarily endorsed by Universidad Distrital. The authors thank the research group ARMOS for the evaluation carried out on prototypes of ideas and strategies.

REFRENCES

[1] S. Chakraborty, S. Dutta, and J. Timoney. The Cyborg Philharmonic: Synchronizing interactive musical performances between humans and machines. Humanities and Social Sciences Communications, 8(1), 2021. doi: 10.1057/s41599-021-00751-8.

[2] A. Kotov, L. Zaidelman, A. Zinina, N. Arinkin, A. Filatov, and K. Kivva. Conceptual processing system for a companion robot. Cognitive Systems Research, 67:28–32, 2021. doi: 10.1016/j.cogsys.2020.12.007.

[3] W.Q. Koh, S.A. Felding, E. Toomey, and D. Casey. Barriers and facilitators to the implementation of social robots for older adults and people with dementia: A scoping review protocol. Systematic Reviews, 10(1), 2021. doi: 10.1186/s13643-021-01598-5.

[4] H. Liu and L. Wang. Gesture recognition for human-robot collaboration: A review. International Journal of Industrial Ergonomics, 68:355–367, 2018. ISSN 01698141. doi: 10.1016/j.ergon.2017.02.004.

[5] J. Medina-Catzin, A. Martin-Gonzalez, C. Brito-Loeza, and V. Uc-Cetina. Body Gestures Recognition System to Control a Service Robot. International Journal of Information Technology and Computer Science, 9(1):69–76, 2017. ISSN 20749007, 20749015. doi: 10.5815/ijitcs.2017.09.07.

[6] Z.-T. Liu, A. Rehman, M. Wu, W.-H. Cao, and M. Hao. Speech emotion recognition based on formant characteristics feature extraction and phoneme type convergence. Information Sciences, 563:309–325, 2021. doi: 10.1016/j.ins.2021.02.016.

[7] K. Shima, A. Mutoh, K. Moriyama, and N. Inuzuka. Human motion analysis using expressions of non-separated accelerometer values as character strings. Artificial Life and Robotics, 26(2):202–209, 2021. doi: 10.1007/s10015-020-00668-6.

[8] A.A. Oliva, P.R. Giordano, and F. Chaumette. A General Visual-Impedance Framework for Effectively Combining Vision and Force Sensing in Feature Space. IEEE Robotics and Automation Letters, 6(3):4441–4448, 2021. doi: 10.1109/LRA.2021.3068911.

[9] T.-P. Liang, L. Robert, S. Sarker, C.M.K. Cheung, C. Matt, M. Trenz, and O. Turel. Artificial intelligence and robots in individuals' lives: How to align technological possibilities and ethical issues. Internet Research, 31(1):1–10, 2021. doi: 10.1108/INTR-11-2020-0668.

[10] A. Rendón. Operational amplifier performance practices in linear applications. Tekhnê, 16(1):57–68, 2019. ISSN 1692-8407.

[11] G. Chen, H. Cao, J. Conradt, H. Tang, F. Rohrbein, and A. Knoll. Event-Based Neuromorphic Vision for Autonomous Driving: A Paradigm Shift for Bio-Inspired Visual Sensing and Perception. IEEE Signal Processing Magazine, 37(4):34–49, 2020. ISSN 1558-0792. doi: 10.1109/MSP.2020.2985815.

[12] S. Habibian, M. Dadvar, B. Peykari, A. Hosseini, M.H. Salehzadeh, A.H.M. Hosseini, and F. Najafi. Design and implementation of a maxi-sized mobile robot (Karo) for rescue missions. ROBOMECH Journal, 8(1), 2021. doi: 10.1186/s40648-020-00188-9.

[13] R.A. Søraa and M.E. Fostervold. Social domestication of service robots: The secret lives of Automated Guided Vehicles (AGVs) at a Norwegian hospital. International Journal of Human Computer Studies, 152, 2021. doi: 10.1016/j.ijhcs.2021.102627.

[14] A. Rendón. Design and evaluation of Volume Unit (VU) meter from operational amplifiers. Tekhnê, 16(2):31–40, 2019. ISSN 1692-8407.

[15] F. Martínez, E. Jacinto, and F. Martínez. Obstacle detection for autonomous systems using stereoscopic images and bacterial behaviour. International Journal of Electrical and Computer Engineering (IJECE), 10(2):2164, 2020. ISSN 2088-8708, 2088-8708. doi: 10.11591/ijece.v10i2.pp2164-2172.

[16] P. Fratczak, Y.M. Goh, P. Kinnell, L. Justham, and A. Soltoggio. Robot apology as a post-accident trust-recovery control strategy in industrial human-robot interaction. International Journal of Industrial Ergonomics, 82, 2021. doi: 10.1016/j.ergon.2020.103078.

[17] A.Y. Alhaddad, J.-J. Cabibihan, A. Hayek, and A. Bonarini. Influence of the shape and mass of a small robot when thrown to a dummy human head. SN Applied Sciences, 1(11), 2019. doi: 10.1007/s42452-019-1447-7.

[18] M. Leal, F. Pisani, and M. Endler. A blockchain-based service for inviolable presence registration of mobile entities. Journal of the Brazilian Computer Society, 27(1), 2021. doi: 10.1186/s13173-021-00104-y.

[19] M. Nikooghadam, H. Amintoosi, S.H. Islam, and M.F. Moghadam. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. Journal of Systems Architecture, 115, 2021. doi: 10.1016/j.sysarc.2020.101955.

[20] R. Jaichandran, S. Muthuselvan, S. Rajaprakash, C. Vibin, J. Joel, and A.S. Gopan. Biometric based user authentication and privacy preserving in cloud environment. Turkish Journal of Computer and Mathematics Education, 12(2):347–350, 2021. doi: 10.17762/turcomat.v12i2.801.

[21] S. Srinivasan, S.K. Mandal, L. Kumar, C. Menaka, and A.A. Menon. A structured protective cohesive health care information system using security and storage mechanism in cloud. SSRG International Journal of Engineering Trends and Technology, 69(3):29–33, 2021. doi: 10.14445/22315381/IJETT-V69I3P206.

[22] M.P. Manuel and K. Daimi. Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications. SN Applied Sciences, 3(4), 2021. doi: 10.1007/s42452-021-04377-y.

[23] A. Tuomi, I.P. Tussyadiah, and J. Stienmetz. Applications and Implications of Service Robots in Hospitality. Cornell Hospitality Quarterly, 62(2):232–247, 2021. doi: 10.1177/1938965520923961.

[24] R. Pozharliev, M. De Angelis, D. Rossi, S. Romani, W. Verbeke, and P. Cherubino. Attachment styles moderate customer responses to frontline service robots: Evidence from affective, attitudinal, and behavioral measures. Psychology and Marketing, 38(5):881–895, 2021. doi: 10.1002/mar.21475.

[25] F. Martínez, D. Acero, and M. Castiblanco. Robótica autónoma: acercamiento a algunos problemas centrales. UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE, Colombia, 1st edition edition, January 2013. ISBN 978-958-8897-56-1.

[26] J. Mizuno, D. Saito, K. Sadohara, M. Nihei, S. Ohnaka, J. Suzurikawa, and T. Inoue. Effect of the information support robot on the daily activity of older people living alone in actual living environment. International Journal of Environmental Research and Public Health, 18(5):1–13, 2021. doi: 10.3390/ijerph18052498.

[27] C. Russo, K. Madani, and A.M. Rinaldi. An Unsupervised Approach for Knowledge Construction Applied to Personal Robots. IEEE Transactions on Cognitive and Developmental Systems, 13(1):6–15, 2021. doi: 10.1109/TCDS.2020.2983406.

[28] E. Jacinto, F. Martínez, and F. Martínez. Learning strategies for cryptography using embedded systems. Smart Innovation, Systems and Technologies, 59(1):495–505, 2016. ISSN 2190-3018. doi: 10.1007/978-3-319-39690-3.

[29] J. Haynes, M. Ramirez, T. Hayajneh, and M. Bhuiyan. A Framework for Preventing the Exploitation of IoT Smart Toys for Reconnaissance and Exfiltration. In G. Wang, Mohammed Atiquzzaman, Zheng Yan, and Kim-Kwang Raymond Choo, editors, Security, Privacy, and Anonymity in Computation, Communication, and Storage, Lecture Notes in Computer Science, pages 581–592, Cham, 2017. Springer International Publishing. ISBN 978-3-319-72395-2. doi: 10.1007/978-3-319-72395-2_53.

[30] S. Druga, R. Williams, H. Park, and C. Breazeal. How smart are the smart toys? children and parents' agent interaction and intelligence attribution. In Proceedings of the 17th ACM Conference on Interaction Design and Children, IDC '18, pages 231–240, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 978-1-4503-5152-2. doi: 10.1145/3202185.3202741.

[31] L. Villamar and J. Miura. Ontology-based knowledge management with verbal interaction for command interpretation and execution by home service robots. Robotics and Autonomous Systems, 140, 2021. doi: 10.1016/j.robot.2021.103763.

[32] A. Brunete, E. Gambao, M. Hernando, and R. Cedazo. Smart assistive architecture for the integration of IoT devices, robotic systems, and multimodal interfaces in healthcare environments. Sensors, 21(6):1–25, 2021. doi: 10.3390/s21062212.

[33] F. Martínez, E. Jacinto, and F. Martínez. Using bacterial interaction and stereoscopic images for the location of obstacles on autonomous robots. Bulletin of Electrical Engineering and Informatics, 9(3):906-913, 2020. doi: doi.org/10.11591/eei.v9i3.2012.

[34] A. Barrero, M. Robayo, and E. Jacinto. Board navigation algorithm in controlled environments based on image processing. Tekhnê, 12(2):23-34, 2015. ISSN 1692-8407.

[35] L. Hicapié, and E. Garavito. Modeling and design of DC/DC converters. Tekhnê, 15(1):21-26, 2018. ISSN 1692-8407.