People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

University of Mohamed El Bachir El Ibrahimi of Bordj Bou Arréridj

Faculty of Mathematics and Computer Science

Computer Science department

Master’s thesis

Presented for graduation

IT master

Specialty: Network and multimedia / Information and communication technologies

THEME

Inmates Tracking Based on Face and Visual Markers

Presented by :

DRICI ADEM

HAMIDOUCHE SALAH

In front of a committee composed of :

Examiner :

- BELHADJ Foudil
- Belazzoug Mouhoub

Supervisor:

- Mostefai Messaoud

2024/2023

Dedications

To my family, whose steadfast help has been the bedrock of my journey, to my parents, for his or her boundless love and encouragement and for their sage recommendation and steering, to my brothers, for his or her steady companionship and support, And to my instructors, for their beneficial concept and expertise to all my pals and those who expensive to me.

Thank you for being my source of power and motivation.

Thanks

I am honored to present this work and extend my sincere thanks to Professor Mustafa Masoud from Mohamed Bashir Al-Ibrahimi University. His dedicated supervision and guidance during the research period, as well as his assistance in finalizing this document, were greatly appreciated.

Sincerely.

Summary

The proposed project presents a pioneering system for identifying and monitoring inmates in correctional centers. Traditional strategies along with RFID, wristbands and fingerprinting are recognized to be fallacious and useless. To conquer those shortcomings, the mission combines facial technology with ArUco tag generation embedded in prisoner uniforms. Each prisoner is assigned a unique ArUco tag ID, making sure correct identity even when facial recognition is impaired. Strategic placement of cameras in important areas including entrances, corridors and relevant courtyards ensures constant surveillance and will increase prisoner detection rates.This revolutionary gadget promises to noticeably enhance safety and operational efficiency inside correctional facilities.

Abstract

Traditional prison identification methods, such as RFID, wristbands, and fingerprinting, have many defects and shortcomings. For this reason, we propose a new system that uses facial recognition and ArUco marker technologies, adapted to prisoner uniforms. Each prisoner is given a unique ArUco marker ID that enables accurate identification even if the face is obstructed. Our system will help track prisoners throughout the prison by placing cameras at strategic locations, entrances, corridors, and jail squares, ensuring constant surveillance and optimizing detection capability. This idea gives better security with improved efficiency and reliability and can completely revolutionize prison surveillance.

ملخص

يقدم المشروع المقترح نظاما لتحديد ومراقبة النزلاء في المراكز الإصلاحية. من المعروف أن الاستراتيجيات التقليدية مثل RFID وأساور المعصم وبصمات الأصابع غير مجدية. وللتغلب على هذه العيوب، تجمع المهمة بين تقنية الوجه مع إنشاء علامة ArUco المضمنة في زي السجناء. يتم تخصيص معرف علامة ArUco فريد لكل سجين، مما يضمن الهوية الصحيحة حتى عند ضعف التعرف على الوجه. يضمن الوضع الاستراتيجي للكاميرات في المناطق المهمة بما في ذلك المداخل والممرات والساحات . مراقبة مستمرة وسيزيد من معدلات اكتشاف السجناء. تعد هذه الأداة بتعزيز السلامة والكفاءة التشغيلية بشكل ملحوظ داخل المرافق الإصلاحية.

Contents :

List of Figures

List of Tables:

I. Chapter I: Methods of monitoring prisoners

I.1 General Introduction

In our time, security at prisons is of concern, and inmate monitoring is one aspect of prison administration that assures security inside and outside the prison, prevents prison escapes, and contributes to discipline. Effective prisoner monitoring also leads to the rehabilitation of prisoners through behavior monitoring and their facilitation in education or treatment programs. We, therefore, need to develop security, monitoring, and personnel management systems. A promising solution for the improvement in monitoring and management of prison inmates is the use of information technology, including facial recognition and visual signs, as monitoring systems have developed in recent times.

I.2 Traditional methods of monitoring prisoners:

I.2.1 Visual Inspection and Direct Inspection:

One of the most used ways and the longest is video control. Where the prison guards are regularly patrolling in different areas of prison, including annihilation, corridors and common areas, to monitor the imprisonment and prevent potential abuse between them. This system allowed guards to monitor the behavior of prisoners directly, interfere with disputes, and impose prison rules.

I.2.2 Frequent communication between officers:

Playing communication between officers is an important role in the nursery of traditional prisoners. The guards used radio phones and devices to provide information about guest movements and what was happening in prison. The documents were issued to transfer prisoners from one area to another, so that only those who have good reasons can be transferred to prison. In addition to, the blackboard or handwritten signs are used to track the guests. This data revealed the time and sites of the prisoners ’move, allowing the guards to track and monitor the place of the prisoners all the time

I.2.3 Video Surveillance:

Video surveillance technology is much more sophisticated compared to direct contact; it has, however, turned out to be one of the traditional means of surveillance. Video cameras have been installed in all the facilities to monitor inmates. They capture images and videos that can be replayed for further analysis. Video surveillance is important in the sense that it improves security by providing successive information concerning prisoners' behavior; this is imperative in ensuring that incidents that take place within the prisoners are investigated.

There has been development of a strong system for prison safety. Combining human control, effective communication, and technological support makes it possible to monitor the behavior of prisoners more precisely; it reduces the chance of escape, violence, and other crimes.

I.3 Effective Methods for Prisoner Monitoring

Contemporary conditions require innovative strategies to monitor guests in reform facilities. The use of technically advanced methods to track the inmate helps reduce errors such as accidental versions, medical supervision and poor credit.

I.3.1 Biometric Systems:

I.3.1.1 Introduction to Biometrics

Biometric authentication is a security measure based on matching the user's biometric features, seeking access to a given device or system. Only when the parameters match will the system be opened for that particular user, using his stored data in the database. Based on features those are either physiological, like fingerprints, iris, face, voice, or even DNA.[29]

I.3.1.2 Tools Based on Physical Characteristics:

I.3.1.2.1 Fingerprints:

These systems examine the particular patterns fashioned by the ridges and valleys at the hands. They are broadly used because of their ease of acquisition and problem in falsifying them. Fingerprints are collected the use of numerous techniques together with ink-primarily based techniques or digital scanners. The ensuing fingerprint pictures are then as compared towards a database for identity and verification purposes. The reliability and accuracy of fingerprint structures cause them to a cornerstone within the field of biometrics.

Figure 1 Fingerprint Scanning

I.3.1.2.2 Iris:

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance. The discriminating powers of all biometric technologies depend on the amount of entropy they are able to encode and use in matching. Iris recognition is exceptional in this regard, enabling the avoidance of collisions even in cross-comparisons across massive populations. Its major limitation is that image acquisition from distances greater than a meter or two, or without cooperation, can be very difficult.

I.3.1.2.3 Face:

A biometric identity technique called facial recognition makes it smooth to confirm someone's identity. Artificial intelligence-based software then quantifies the distinct functions of the face and its expressions. For example, the separation of the eyes, the gap among the mouth and the forehead, , the form of the cheekbones, and the define of the lips, ears, and chin.

Simplifying the identity and authentication procedures is the intention. For this cause, the adoption of facial recognition technology is developing. And that is applicable to a broad range of uses.

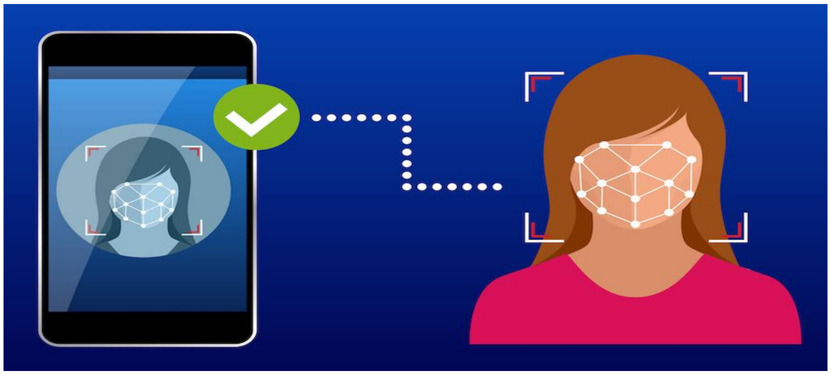


Figure 2 Face recognition

I.3.1.2.4 Retina:

Scanning the retina examines the intricate patterns of blood vessels at the rear of the eye, which is highly not possible to imitate. The process involves the individual's looking through a device that captures an image of the retina. Since these patterns are unique and remain quite stable over time, this approach achieves very high levels of accuracy about identity verification and is mainly used in high-risk and secure environments.

Figure 3 Retina Scan

I.3.1.3 Tools Based on Behavioral Characteristics:

I.3.1.3.1 Typing Dynamics:

This tool measures how a person kinds on a keyboard, including speed and rhythm. The specific sample of keystrokes may be analyzed to authenticate a user. Typing dynamics take into account elements like typing velocity, pressure. This technique is useful for non-stop authentication in cyber protection programs and fraud detection.

I.3.1.3.2 Signature:

Signature biometrics analyzes how a person signs, including the pressure applied and the movement of the pen. Signature recognition is conventionally used to record the unique way one writes his or her signature, which is not easily forgeable. Signature recognition systems are used at financial institutions, legal documents, and access control systems to verify identity.

I.3.1.3.3 Voice:

The voice of people is decided by studying the precise characteristics of their voices. This includes studying various speech functions, inclusive of pitch and intonation. Voice may be used to safely get right of entry to communications systems, banking offerings, and voice-activated devices. But it has the downside of a person's voice changing due to illness. [29]

I.4 Biometric Inmate Tracking System :

The Biometric Inmate Tracking System (BITS) was created to replace the old manual system with a computerized one, and then updated to include biometrics. During this change, the designers had to find the best way of using biometrics to track inmates at Charleston prison. They also developed software capable of identifying and verifying inmates on the basis of their biometric characteristics. The software had to be easy to use for prison officers with little computer experience **[21]**.

Over a three-twelve months period, various biometric strategies have been examined, along with iris, facial, retinal, finger and hand geometry, voice, and fingerprint reputation. Each approach had its advantages and downsides. Facial reputation produced too many false positives, on the equal time as iris recognition grow to be correct however too sluggish for a jail setting. Ultimately, the fingerprint recognition technique, used along facet hand geometry, proved to be the amazing desire. It provided correct and reliable suits at a decrease cost than different strategies and facilitated faster inmate motion through protection gates.

During the next section of inmate tracking, the manual dry-erase board and paper system have been replaced with a automatic tracking machine. In this device, a vital server stored all facts associated with inmate movements. Brig personnel ought to get entry to this information from various locations, which include housing gadgets, the manage center, and the enrollment vicinity. To enhance security, biometric scanners have been included into the gadget.

Here's how the modern-day gadget operates: When an inmate movements in the brig, the pc machine identifies a biometric match, confirms the person's identification, and verifies their authorization to move from one part of the power to another. Additionally, the pc sends a notification to the subsequent safety put up alongside the authorized course, informing them that the prisoner is en course. Notably, there may be no need for physical escorts or paper facts due to the fact the laptop meticulously logs all prisoner actions among safety checkpoints at some stage in the facility. If a prisoner fails to appear within an exact time, an alarm is precipitated, alerting workforce that the inmate is out of place.

This superior monitoring device ensures efficient and secure inmate movement inside the facility, minimizing risks and improving standard protection

I.4.1.1 Radio-Frequency Identification (RFID):

Radio Frequency Identification technology deals with the use of removable tags that emit signals in communication with RFID sensors, receivers, and monitors in almost real time, thereby ensuring better control and integration of inmates and staff into workplaces. These wearable devices improve safety by preventing criminal behavior through constant monitoring, helping quickly to respond to unauthorized travel, and reduce reliance on potentially disturbing

Witness reports. Secondly, RFID systems enhance efficiency in management since they increase alerts against tampering, ease investigations and retrieval of stored data, in addition to reducing chances of hijacking and breaches, hence cutting down on costs of staff overtime, medical care, and legal costs. Robustness of the technology and tamper alert capabilities make it even more potent. The high cost of RFID systems, however calls for independent evaluation and critical review about its cost-effectiveness and long-term effectiveness in the operations of correctional institutions. [1]

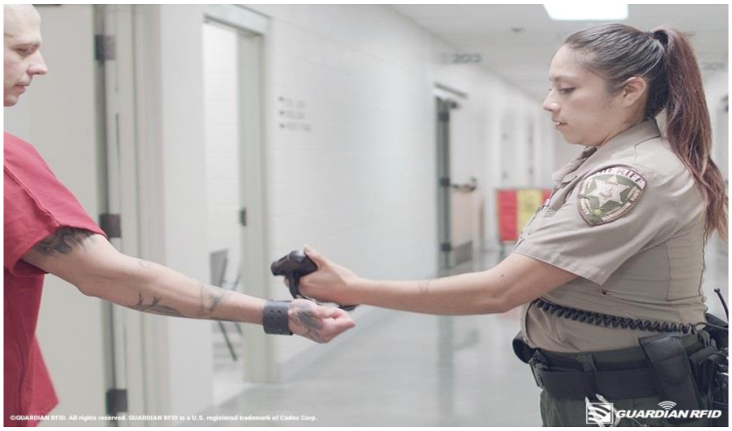

©GUARDIAN RFID. All rights reserved. GUARDIAN RFID is a U.S. registered trademark of Codex Corp.
GUARDIAN RFID

Figure 4 Tracking Inmates using (RFID)

I.4.1.2 Challenges and Limitations of RFID Technology in Correctional Facilities:

The most common problem staff at both Ross and NEPRC encounter with RFID technology is false alarms. These are common because the RFID wristband signal is picked up on a different floor, often when an inmate is sitting, which interferes with the signal between floors. The signal can also be blocked, which is prominently the case with inmates under metal-roofed pavilions at NEPRC. To alleviate this problem, the vendor installed additional detection units. Other cases of signal blockage occur when a male inmate sleeps with his hand against the wall or when a female inmate rests her ankle on the ground. Also, there are practical problems with the size of RFID wristbands. In this case, at Ross, the bracelets can't be resized, and because inmates are gaining or losing weight, the bracelets do not fit properly. The tight bracelets make the inmate feel uncomfortable and require adjustments, while loose ones generate inmate missing alerts, which are a more significant problem. Although this happened a lot at the beginning, these alerts are less frequent now that the correctional officers have become more accustomed to the technology. Other bracelet-related problems include battery life, which, when lost, an alert is triggered saying inmate missing, and cleaning and maintenance, which take considerable time for correctional officers. Finally, there is an additional problem at Ross because the software is perceived not to be user-friendly enough and may not be used to the best of its ability by the correctional officers. When a prison guard has to check RFID wristbands to record prisoner activities such as meal passes, razor passes, court transports, med passes, and work release programs, it presents a significant risk. During these checks, the guard and prisoner are so close that the likelihood of the inmate attacking the guard is very high, as there will not be a buffer zone between the guard and the prisoner.

I.5 Conclusion:

In conclusion, the challenges and limitations posed to the staff in correctional facilities by RFID technology are big challenges to them in terms of efficiently and effectively managing inmates. The realization of the false alert problem and blocking of signals, sizing problems, and questions of the usability of software raise concerns and issues towards finding alternative means of improving operational effectiveness.

The proposed solution of facial recognition integrated with ArUco markers printed on prisoner suits offers a promising approach to solve such challenges. By combining these technologies, correctional facilities can be assured of a more reliable, accurate manner in which inmate identification and tracking can be enhanced. In a nutshell, the comprehensive system provides a backup mechanism in situations where facial recognition may be hindered, ensuring continuous monitoring of inmate activities. Such a measure will not only improve the security measures but also ease operational processes, thus easing the load off the correctional staff and improving the general management of the facility. Through the applications of novel technologies and reconfigurations to the particularities of the correctional environment, the facilities will not only go beyond the limitations of RFID technology but also other techniques mentioned above to create the next level of inmate management within a correctional facility.

II. Chapter 02: Facial recognition

II.1 Introduction:

The face is an important composition of humans that is used to convey identity and emotions; hence, face recognition is an important field widely applied by law enforcers, banks, security systems, and personal identification. The paper researches three main stages: face representation, feature extraction, and classification. Face representation is modeling facial features to allow the detection and recognition algorithms. Feature extraction is the isolation of relevant facial features for recognition. The classification procedure matches the facial image against the stored data for identification. Facial expression is a natural and spontaneous way of expressing feelings and intentions; this is why face recognition is an important activity in human social interactions and in authentication procedures in modern societies.

II.2 History of facial recognition:

The history of face recognition goes back to 1964 when Woodrow Bledsoe, Helen Chan, and Charles Bisson started work on programming computers to recognize faces[7]. Their semi-automatic method required an operator to enter about 20 measurements, such as the size of the mouth or eyes, into the computer. Starting with the rise of deep learning in 2011, facial recognition saw a significant acceleration in that the computer can now choose which points to compare, which means that the better the computer is fed images, the better its learning.

II.3 Advantages and limitations of facial recognition in prisoner monitoring:

Facial recognition in inmate tracking is provided with advantages in terms of increased security and speed of data processing, very necessary in the correctional environment. Its disadvantages, however, lie in the risks of infringement of individual freedoms and the possibility of errors due to technological flaws, bad camera angles, lack of enough light, or poor image quality. Further, major challenges with regard to the adoption of this technology in prisoner monitoring include privacy concerns and algorithmic bias that could result in discrimination. These limitations must be considered in implementing facial recognition systems so that fundamental rights are respected and the technology is used ethically and responsibly.[31]

II.4 How facial recognition technology works:

Facial recognition technology is the complex device designed for the identification or verification of individuals mainly based on their face capabilities, using superior algorithms and photograph processing strategies.[32]

II.4.1 Face detection:

The first step is face detection within an image or video feed. With the use of sophisticated cameras and complex image processing algorithms, facial recognition systems can accurately pinpoint faces in very different environments, whether one is facing the camera, in profile, or partially obscured by objects or other people. These systems have been continuously refined to the extent that they will have improved the accuracy and speed of the task, now possible in real time and in any scenario, from surveillance systems to mobile devices.

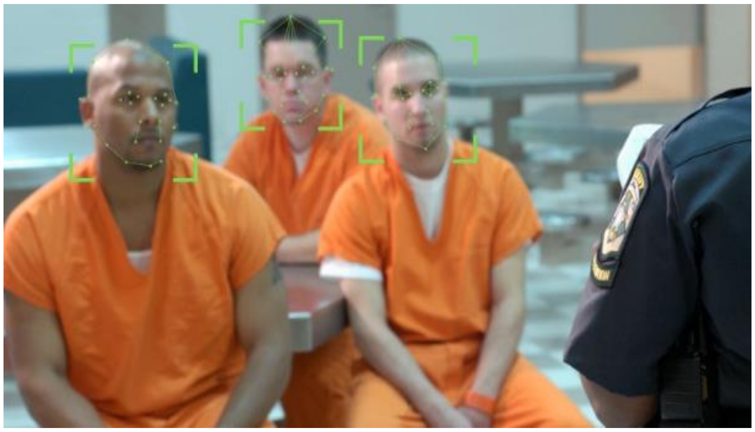


Figure 5 Inmates Face Detection

II.4.2 Face Analysis:

Once a face is detected, the system takes an image and goes on to do an in-depth analysis. While the earlier versions mostly used 2D image processing, modern facial recognition systems incorporate innovative 3D modeling and depth-sensing technologies in the quest to achieve higher accuracy. The software carefully analyzes the geometry of the face, taking into consideration key landmarks such as the distance between the eyes, the depression of the eye sockets, the shape of the nose, and the outline of the jawline. The higher level of scrutiny in facial geometry guarantees the achievement of strong facial feature extraction, hence better identification and verification. Most significantly, however, some advanced face analysis methods also consider additional factors, such as facial expression, skin texture, and aging effects, which bring about high recognition performance and robustness to variations in appearance.

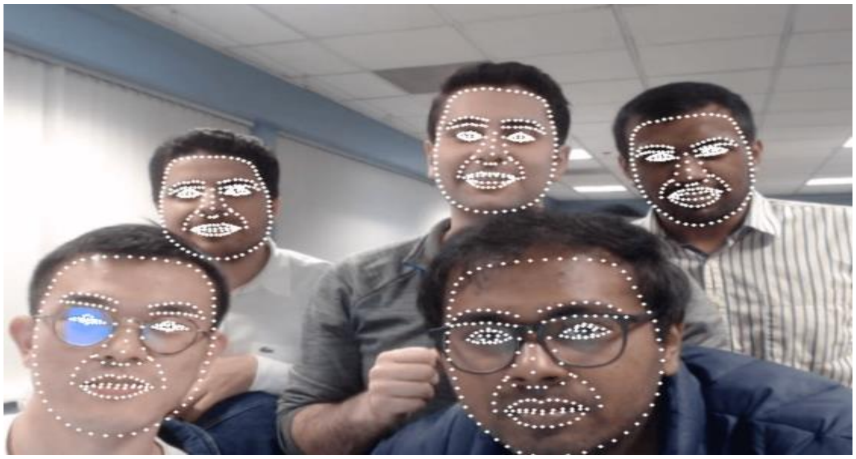


Figure 6 Face Analysis

II.4.3 Converting image to data:

Following face analysis, the facial photo undergoes conversion into a virtual dataset. This pivotal step entails the transformation of extracted facial features into a mathematical illustration or virtual code, generally called a facial template or facial print. Analogous to fingerprints, every facial print is inherently unique to a man or woman, encapsulating the extraordinary traits in their facial structure and composition. The conversion manner employs sophisticated algorithms to encode facial features in a compact yet discriminative format, allowing garage, retrieval, and contrast all through subsequent reputation obligations.

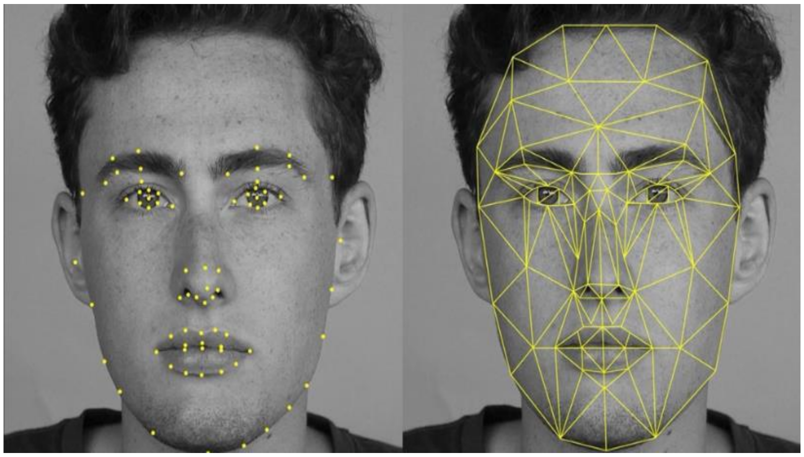


Figure 7 Depict the extracted facial features

II.4.4 Comparison and identification:

The finalized facial print is in the end compared in opposition to a database of pre-present facial templates to check a fit. In scenarios concerning verification, the system cross-references the facial print with the only previously enrolled for the individual, validating their identity based on a predetermined threshold of similarity. For identity purposes, the generation conducts a comprehensive search across the whole database, looking for the closest healthy to the supplied facial print. This iterative system allows speedy and accurate identification of individuals within numerous populations, facilitating various programs starting from get entry to control and safety surveillance to regulation enforcement and border control.

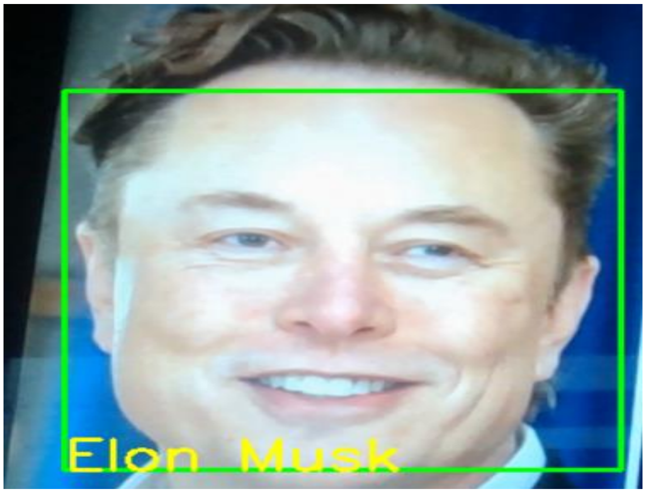


Figure 8 Comparaison and identification

II.5 Face detection methods:

II.5.1 Facial Detection Using Knowledge-Based Approach:

This technique is based totally on know-how human nature. We realize that the face should be in a sure position and that the nose, eyes and mouth ought to be in a sure role relative to each other. The trouble with this approach is setting the proper guidelines. The device could be excellent if the policies have been too general or too specific. However, this doesn't follow to all skin sorts and relies upon on lighting situations that could exchange the actual pores and skin tone of the person inside the photo.[33]

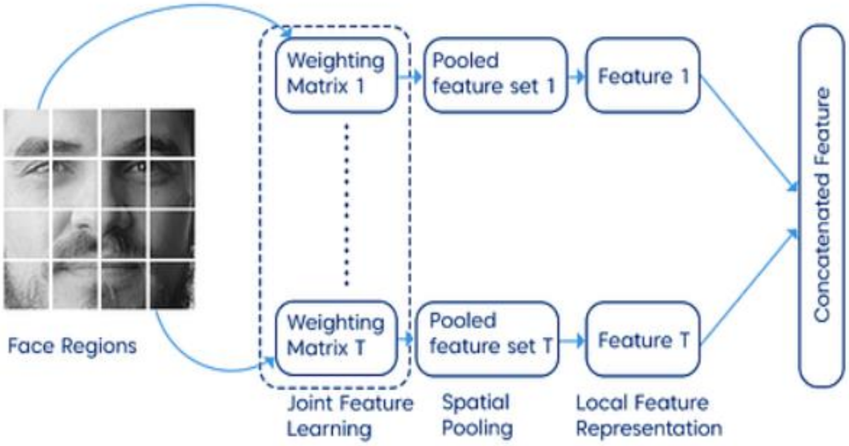


Figure 9 Facial Detection Using Knowledge-Based Approach

II.5.2 Pattern matching:

Pattern matching uses a face or a preset face parameter set to modify the spatial relationship between the model and the input image, ensuring accurate coordination. Face models are created from edges detected using methods like the Canny edge detector, Sobel operator, or Laplacian of Gaussian (LoG). These edge detection techniques identify contours of facial features such as eyes, nose, and mouth. The face parameter preset includes key measurements and characteristics defining typical facial structures. This process is essential for applications like facial recognition, image tagging, and biometric verification, where accurate face detection and analysis are required.

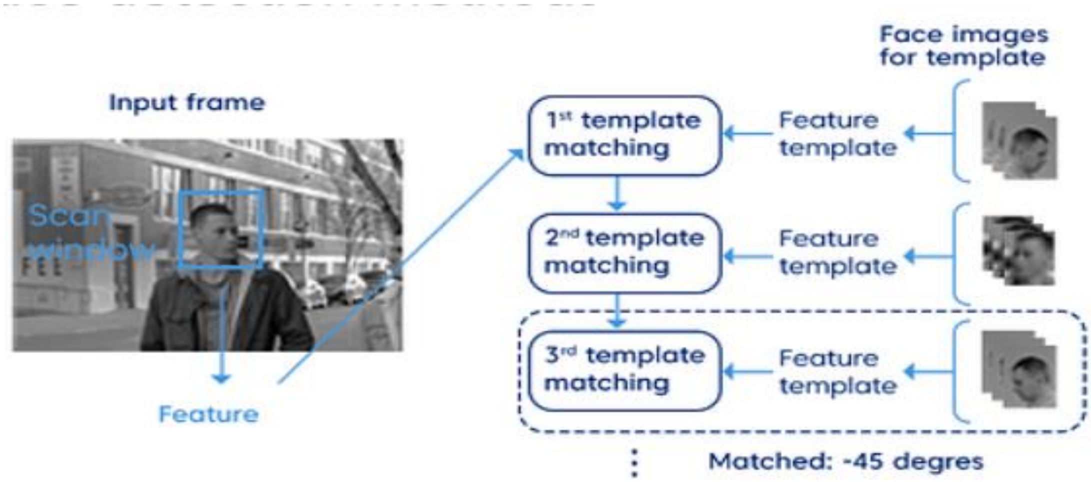
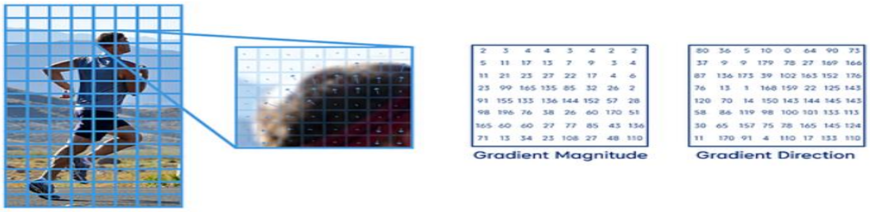


Figure 10 Pattern matching

II.5.3 Facial Detection Based on Features:

This method relies on feature extraction, using a trained reference to identify and distinguish facial regions. It involves detecting specific facial features, such as eyes, nose, and mouth, by analyzing distinctive attributes. One example is color-based image matching, which identifies normal skin tones and facial features within an image. This technique is effective for distinguishing faces in various lighting conditions and backgrounds. By focusing on unique facial features and skin color, this method enhances the accuracy and reliability of facial detection for applications like image recognition and biometric verification.



2	3	4	4	3	4	2	2
5	11	17	13	7	9	3	4
11	21	23	27	22	17	4	6
23	99	165	135	85	32	26	2
91	155	133	136	144	152	57	28
98	196	76	38	26	60	170	51
165	60	60	27	77	85	43	136
71	13	34	23	108	27	48	110

Gradient Magnitude

80	36	5	10	0	64	90	73
37	9	9	179	78	27	169	166
87	136	173	39	102	163	152	176
76	13	1	168	159	22	125	143
120	70	14	150	143	144	145	143
58	86	119	98	100	101	133	113
30	65	157	75	78	165	145	124
11	170	91	4	110	17	133	110

Gradient Direction

Figure 11 shows the detection Based on Features

II.5.4 Facial Detection Based on Appearance:

Facial Detection Based on Appearance includes state-of-the-art methodologies in face-based training for facial recognition. Utilizing advanced techniques in machine learning and statistical analysis, this approach aims to detect significant features within facial images and extract them for further analysis. By employing a multifaceted approach, Facial Detection Based on Appearance integrates various algorithms to enhance its effectiveness and reliability in recognizing and detecting faces. These algorithms work in tandem to analyses complex facial details, such as contours, textures, and delicate structural variations, enabling accurate identification even in the midst of varying environmental conditions and facial expressions. Through detailed analysis and processing, this method strives to encapsulate the diverse array of facial features that contribute to individual identity. By integrating cutting-edge technologies and methodologies, Facial Detection Based on Appearance stands as a powerful solution in the realm of facial recognition, Providing to a numerous of applications ranging from security systems to biometric authentication and beyond.

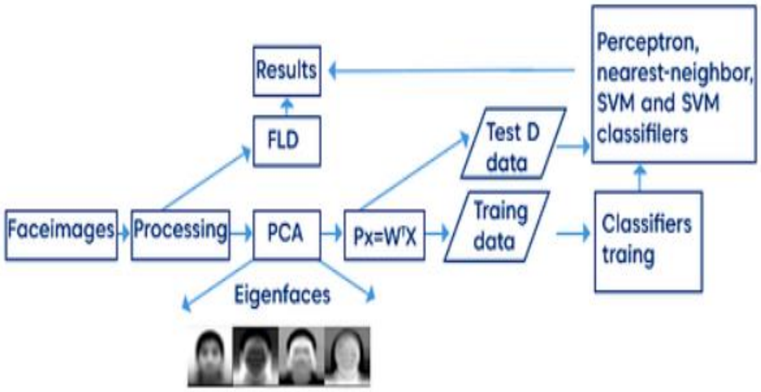


Figure 12 Detection Based on Appearance

II.5.5 Face Detection Based on Motion:

Face Detection Based on Motion utilizes dynamic motion analysis techniques to identify and track faces within video clips, treating the tour as a reference guide. By recognizing specific facial movements, like blinks, the software determines underlying facial expressions. It analyzes motion patterns within the video clips, comparing them to predefined templates of typical facial expressions to accurately categorize observed expressions. This approach enables real-time face detection and expression recognition, applicable in domains such as emotion detection, video surveillance, and human-computer interaction. Leveraging motion-based cues enhances the adaptability of face detection systems, facilitating accurate analysis of facial dynamics across diverse scenarios

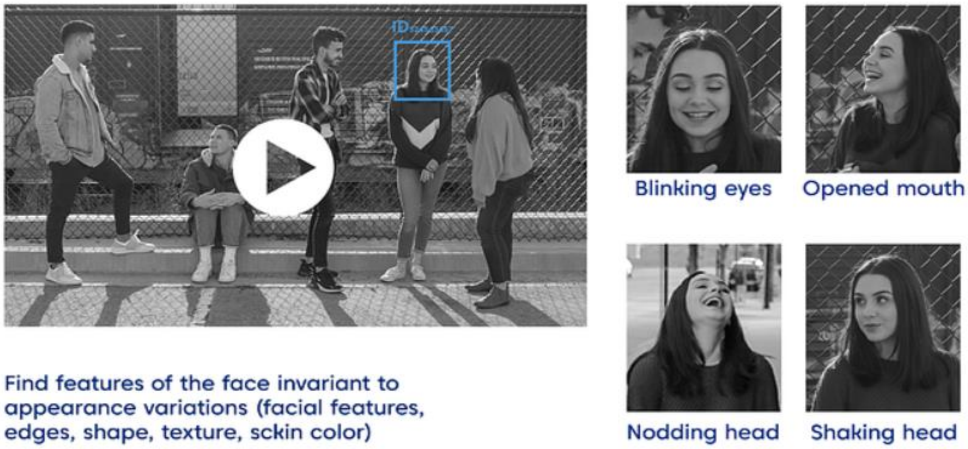

Blinking eyes
Opened mouth
Find features of the face invariant to appearance variations (facial features, edges, shape, texture, sckin color)
Nodding head
Shaking head

Figure 13 Face Detection Based on Motion

II.5.6 Utilizing MTCNN for Face Detection:

Face detection is so important for face recognition, but there are a lot of challenges such as occlusions, pose variations, and lighting conditions make these tasks hard to apply them. The Viola-Jones detector [22], that uses Haar-like features and AdaBoost, performs well in controlled settings but faces difficulties with real-world variations [23, 24, 25], Deformable Part Models (DPM) [26, 27, 28] offer better performance at a high computational cost. Recent advances in convolutional neural networks (CNNs) have improved face detection and recognition; however, CNN-based methods can be very slow and often ignore the relationship between detection and landmark localization. Existing joint approaches have limitations, such as reliance on handcrafted features or weak initial detectors .Effective hard sample mining is crucial for training robust detectors but increases manual effort. We introduce a new framework that combines face detection and alignment using cascaded CNNs with multi-task learning, and this work through these three steps: a shallow CNN for generating candidate windows, a more complex CNN for refining these windows, and a powerful CNN for final refinement and landmark localization. This approach improves performance through online hard sample mining and demonstrates significant advancements over existing methods, contributing a lightweight CNN architecture for real-time performance, an effective online hard sample mining method, and extensive benchmark testing showing great results.

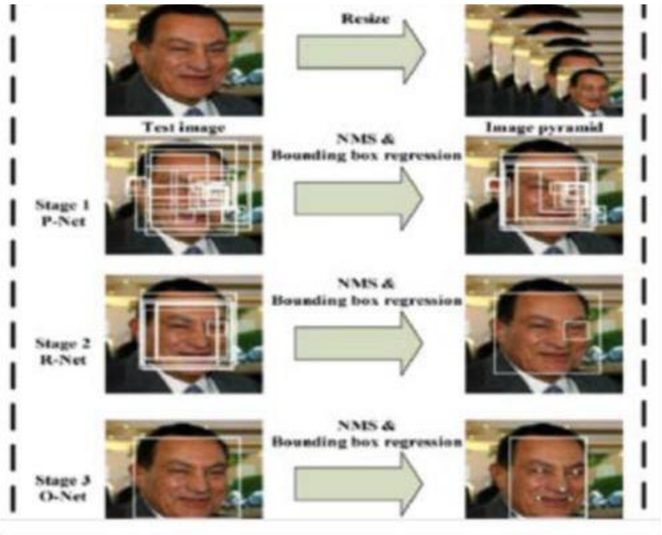


Figure 14 Face recognition using MTCNN

II.5.7 Face Detection with Haar Cascade Algorithm:

Haar-like features, named for their resemblance to Haar waves, are integral to object recognition systems due to their computational efficiency, akin to traditional methods. In the Viola-Jones framework, these features are computed across the input image within a sliding window, with thresholds separating objects from background based on the calculated differences.[12] While individual Haar features may offer weak classification, combining them in a cascade enhances overall accuracy. Notably, Haar features boast rapid computation, thanks to integral images, ensuring consistent processing speed regardless of image size. These features, including variants like 2-rectangle, 3-rectangle, and 4-rectangle structures, capture distinct aspects of images, such as light and dark areas, facilitating comprehensive analysis. This efficiency significantly reduces computation time, typically requiring only four checks per calculation. Despite efforts to enhance detection by introducing rotated Haar features at a 45° angle, practical limitations, including calculation errors in low-quality images, hinder widespread adoption of this extension.[13] Consequently, while mathematically elegant, such Haar-like elements remain sparingly utilized in practical applications.

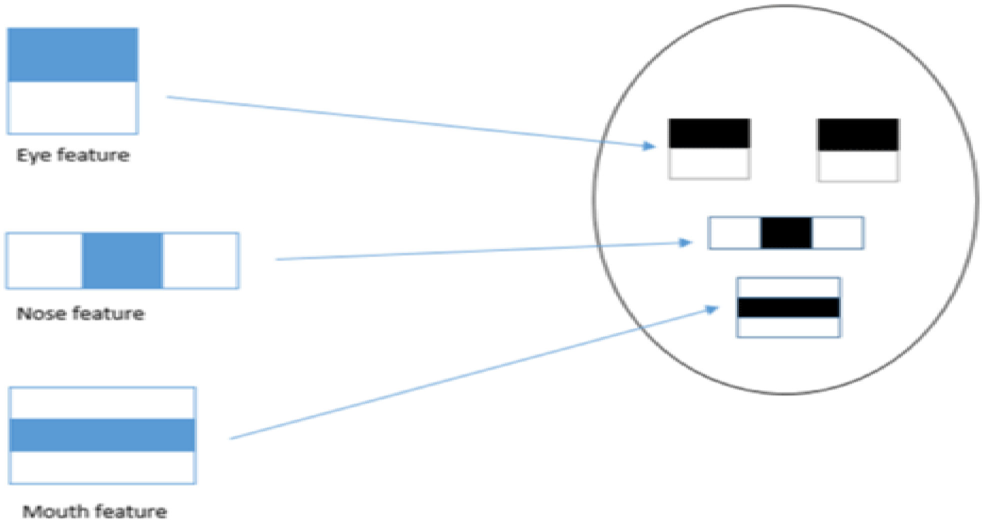


Figure 15 Haar-like features

II.5.8 Eigen faces using Principal Component Analysis:

The face recognition algorithm utilizing Eigenfaces and Principal Component Analysis (PCA) is an effective tool for identifying faces in images. PCA significantly reduces the data size of facial images by changing their shape, capturing substantial facial variations. Each facial image is then represented as a line intersecting this Eigen plane, simplifying the data while preserving crucial features. Recognition is accomplished by projecting facial images onto this Eigen plane and comparing the resultant coefficient vectors. Moreover, the incorporation of Fisher Discriminant Analysis (FDA) enhances the distribution structure of variance classes. This integrated approach enables more precise and reliable identification, rendering it applicable across various domains such as security systems, biometric authentication, and access control. Combining both PCA and FDA, this method yields accurate and dependable results, offering a comprehensive solution to the facial recognition challenge [34]

II.6 Face recognition Local Binary Patterns:

Various techniques are available to extract the most pertinent features from preprocessed facial images for face recognition purposes. Among these methods is the Local Binary Pattern (LBP) technique, introduced by Ojala et al. in 1996 [3]. LBP offers a modern approach to delineating the texture and shape of digital images. It achieves this by segmenting an image into numerous small regions, from which features are subsequently extracted (refer to figure 18).

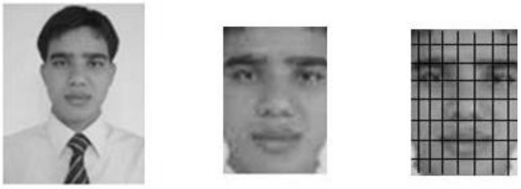
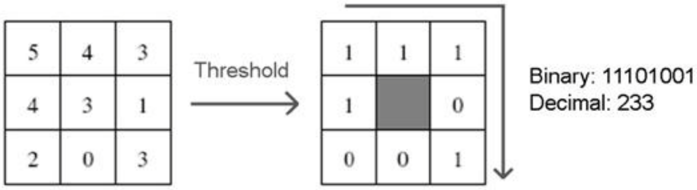


Figure 16 Depicts a preprocessed image segmented into 64 regions

These features comprise binary patterns that depict the pixel surroundings within the regions. These region-derived features are merged into a single feature histogram, creating an image representation. Comparisons between images are then facilitated by assessing the similarity (distance) between their histograms. Multiple studies [1][14] indicate that face recognition utilizing the LBP method yields highly favorable outcomes, demonstrating both rapid processing and discrimination performance. Due to its depiction of image texture and shape, this method appears notably resilient against variations such as different facial expressions, lighting conditions, image rotation, and aging of individuals.

II.6.1 Fundamentals of Local Binary Patterns

The initial LBP operator was proposed by Ojala et al. [2]. This operator operates on the eight neighboring pixels of a central pixel, utilizing the value of the central pixel as a threshold. If a neighboring pixel possesses a higher gray value than the central pixel (or the same gray value), it is assigned a value of one; otherwise, it receives a value of zero. The LBP code for the central pixel is subsequently generated by combining the eight ones or zeros into a binary code (figure19)



5	4	3
4	3	1
2	0	3

1	1	1
1		0
0	0	1

Figure 17 The Original LBP Operator

The LBP operator was subsequently expanded to accommodate neighborhoods of varying sizes. Here, a circular region with a radius R is created around the center pixel. P Sampling points along the circumference of this circle are selected and compared to the value of the central pixel. Achieving the values of all sampling points within the neighborhood for any given radius and number of pixels requires (bilinear) interpolation. The notation (P, R) is employed to denote such neighborhoods. Figure 20 illustrates three sets of neighbors for different combinations of P and R.

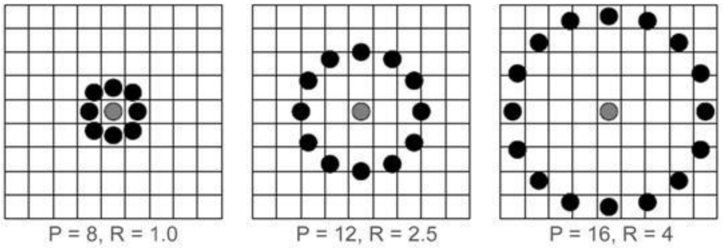


Figure 18 illustrates circular neighbor sets for three distinct combinations

Given the coordinates of the center pixel as ($x_{c,}$ y_c), the coordinates of its P neighbors (x_p, y_p) situated on the edge of the circle with radius R can be computed using trigonometric functions:

$$x_p = x_c + R\cos(2\pi p/P\ ) \qquad (1)$$
$$y_p = y_c + R\sin(2\pi p/P\ ) \qquad (2)$$

If the gray value of the center pixel is g_c and the gray values of its neighbors are g_p, where p ranges from 0 to P - 1, then the texture T in the local neighborhood of the pixel (x_c, y_c) can be defined as:

$$T = t(g_c, g_0, \ldots, g_{P-1}) \qquad (3)$$

Once these values of the points are obtained, it is also possible to describe the texture in another manner. This is achieved by subtracting the value of the center pixel from the values of the points on the circle. In this manner, the local texture is represented as a joint distribution of the value of the center pixel and the differences.

$$T = t(g_c, g_0 - g_c, \ldots, g_{P-1} - g_c) \qquad (4)$$

As t (g_c) represents the overall luminance of an image, which is independent of the local image texture, it does not offer valuable insights for texture analysis. Hence, the original joint distribution (Eq. 3) retains much of the information regarding textural characteristics in the joint difference distribution (Ojala et al., 2001).

$$T \approx (g_0 - g_c, \ldots, g_{P-1} - g_c) \qquad (5)$$

While the differences remain unaffected by gray scale shifts, they are influenced by scaling. To ensure invariance to any monotonic transformation of the gray scale, only the signs of the differences are taken into account. Consequently, if a point on the circle possesses a higher gray value than the center pixel (or an equivalent value), it receives a value of one, otherwise, it is assigned zero:

$$T \approx (s(g_0 - g_c), \ldots, s(g_{P-1} - g_c) \qquad (6)$$

Where: $s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$

In the final stage of generating the Local Binary Pattern (LBP) for the pixel (xc, yc), a binomial weight of 2p is allocated to each sign of s(g_p – g_c). These binomial weights are then aggregated through summation

$$LBP_{P.R}(x_c, y_c) = \sum_{p=0}^{p-1} s(g_p - g_{c)} 2^p \qquad (7)$$

The Local Binary Pattern (LBP) determines the texture of the local image surrounding (x_c, y_c). The initial LBP operator illustrated in figure 19 closely similar to this operator with parameters P = 8 and R = 1, denoted as $LBP_{8,\ 1}$. The primary distinction between these operators lies in the fact that in $LBP_{8,\ 1}$, pixel values require interpolation to obtain the values of points along the circle.

II.6.2 Local Binary Patterns Uniformity:

A Local Binary Pattern is classified as uniform if it exhibits either zero or two bitwise transitions from 0 to 1 or vice versa. This stipulation arises from the circular consideration of the binary string, rendering a single transition impractical. Examples of uniform patterns include those with no transitions (e.g., 00000000 and 11111111) and those with two transitions (e.g., 00011100 and 11100001) within an eight-bit sequence. Additionally, patterns with two transitions offer P(P-1) possible combinations.

For uniform patterns with P sampling points and radius R the notion $\mathcal{L}BP^{u2}_{P,R}$ is used.

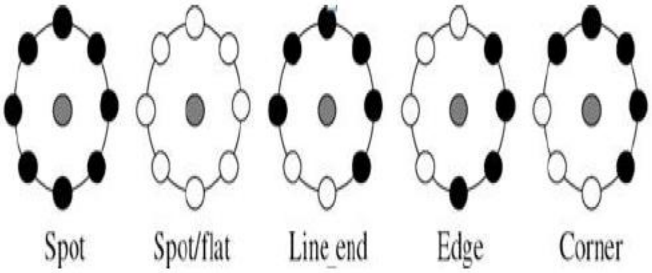


Figure 19 Different texture primitives detected by the ∠BPu2P,R

Exclusively employing uniform Local Binary Patterns provides two significant advantages. Firstly, it conserves memory. In contrast, non-uniform patterns necessitate handling 2^P potential combinations. With $\mathcal{L}\mathrm{BP}^{u2}_{P,R}$ there are P (P − 1) + 2 patterns possible.

For a neighborhood of 16 (interpolated) pixels, the standard LBP yields 65536 possible patterns, while LBPu2 reduces this number to 242. The second advantage lies in LBPu2's capability to specifically detect crucial local textures such as spots, line ends, edges, and corners. Refer to figure 21 for illustrations of these texture primitives.

II.6.3 Facial Recognition Utilizing Local Binary Patterns:

We've outlined how the LBP method can be implemented on facial images to extract features for assessing their similarity. The fundamental concept involves computing the LBP code for each pixel in an image and recording the frequency of each pattern encountered. These pattern occurrences form histograms, or labels, constituting a feature vector that represents the image's texture. By comparing these histograms, one can gauge the likeness between images by computing the distance between them.

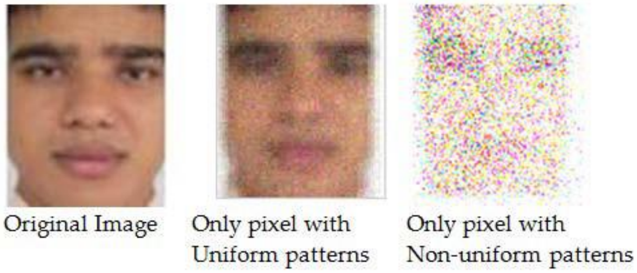


Figure 20 Dividing a facial image into two separate images: one containing only pixels with uniform patterns, and the other containing pixels with non-uniform patterns ℒBPu216,2 .

Figure 22 illustrates an image divided into two parts: one comprising pixels with uniform patterns and the other with non-uniform patterns, generated using the $L\mathrm{BP}^{u2}_{16,2}$ operator. Surprisingly, even the image containing only pixels with uniform patterns retains a significant portion of the original image, comprising 99% of its pixels. Hence, 99% of the pixels in the image retain

Uniform patterns, as determined by LBP (Local Binary Patterns), constitute as much as 99% of the image content. An intriguing observation is that selecting only pixels with uniform patterns preserves the background, as background pixels typically exhibit consistent color (gray value), resulting in patterns with zero transitions. Additionally, a notable proportion of pixels surrounding facial features such as the mouth, noise, and eyes (especially the eyebrows) also exhibit uniform patterns.

Constructing Feature Vectors Following the calculation of the Local Binary Pattern for each pixel, the image's feature vector can be formulated [15]. To efficiently represent facial features, the image is initially partitioned into K^2 regions. For instance, in figure 23, a face image is divided into 8^2 = 64 regions. Subsequently, for each region, a histogram encompassing all possible labels is generated. Each bin within these histograms denotes a specific pattern and records its frequency within the region. The feature vector is then composed by concatenating these regional histograms into a unified histogram.

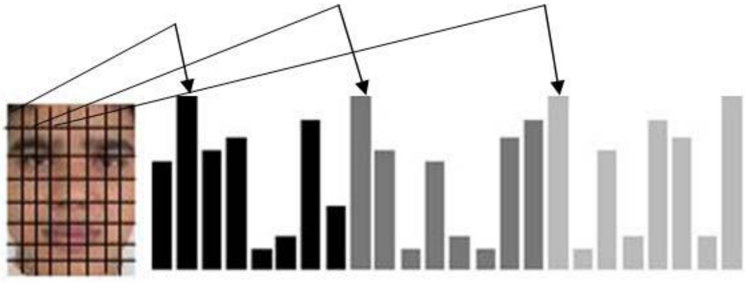


Figure 21 Face image divided into 64 regions, with every region a histogram

In each region, all non-uniform patterns (those with more than two transitions) are assigned a single label. Consequently, every regional histogram comprises P(P - 1) + 3 bins: P(P - 1) bins for patterns with two transitions, two bins for patterns with zero transitions, and one bin for all non-uniform patterns. Consequently, the overall feature vector for an image encompasses K^2(P(P-1) + 3) bins. Therefore, in an image partitioned into 64 regions with eight sampling points on the circles, the LBP code cannot be computed for pixels located within a distance R from the image edges. Consequently, during feature vector construction, a small border area of the image is excluded from consideration. For an N × M image

The feature vector is constructed by calculating the LBP

Code for every pixel (xc, yc) with xc ∈{R + 1 . . . N − R}

y_c ∈{R + 1. . . M − R} If an image is divided into

k × k regions, then the histogram for region (kx, ky), with

$k_x \in \{1, . . . , k\}$ and $k_y \in \{1, . . . , k\},$ Defined as:

$$H_i(K_x, K_y) = \sum_{x,y} I\{LBP_{P,R(x,y)} = L(i)\}, i = 1, \dots \dots \dots . P(P-1)+3 \qquad (8)$$

$$x \in \begin{cases} \{R+1, \dots \dots \dots \dots \dots \quad , {}^{N}/_{K}\} & K_x = 1 \\ \{(K_x - 1)(N/K\} + 1, \dots, N - R & K_x = K \\ \{(K_x - 1)(N/K\} + 1, \dots , \ K_x(N/K) & else \end{cases}$$

$$\in \begin{cases} \{R+1, \dots \dots \dots \dots \dots \quad , {}^{M}/_{K}\} & K_y = 1 \\ \{(K_y - 1)(M/K\} + 1, \dots, M - R & K_y = K \\ \{(K_y - 1)(M/K\} + 1, \dots , \ K_y(M/K) & else \end{cases} \qquad (9)$$

L is the name of bin i and

$$I(A) = \begin{cases} 1, & A \text{ is true} \\ 0, & A \text{ is false} \end{cases} \qquad (10)$$

The feature vector serves as a comprehensive depiction of the face across various levels of detail: the labels encapsulate pixel-level pattern details, the aggregated regions offer insights into localized patterns, and the concatenated histograms provide a comprehensive review of the face.

II.6.4 Feature Vector Comparison

When comparing two face images, a sample (S) and a model (M), the difference between their feature vectors needs to be measured. This can be accomplished using various dissimilarity measures tailored for histograms.

_ Intersection Histogram

$$D(S,M) = \sum_{j=1}^{k^2}\left(\sum_{i=1}^{P(P-1)+3} \min(S_{i,j}\,, M_{i,j})\right) \quad (11)$$

− Log-likelihood Statistic

$$L(S,M) = \sum_{j=1}^{k^2}\left(-\sum_{i=1}^{P(P-1)+3} S_{i,j}\ log\ M_{i,j}\right) \quad (12)$$

− Chi square statistic (x2)

$$x^2(S,M) = \sum_{j=1}^{k^2}\left(\sum_{i=1}^{P(P-1)+3}\frac{(S_{i,j}-M_{i,j})^2}{S_{i,j}+M_{i,j}}\right) \quad (13)$$

In the given equations, Si,j and Mi,j represent the sizes of bin i from region j (indicating the number of appearances of pattern L(i) in region j). Since certain regions of the face images, such as those containing the eyes, may carry more significant information than others, it's possible to assign a weight to each region based on the importance of the contained information. As per article [31], the chi-square (x^2) method demonstrates slightly superior performance compared to histogram intersection and the log-likelihood statistic. Introducing a weight wj for region j modifies the equation for the weighted x^2 accordingly.

$$x_w^2(S,M) = \sum_{j=1}^{k^2} w_j\left(\sum_{i=1}^{P(P-1)+3}\frac{(S_{i,j}-M_{i,j})^2}{S_{i,j}+M_{i,j}}\right) \quad (14)$$

The weighted x^2, derived from histograms of two face images, serves as a metric for measure their similarity. A lower x^2 value, x^2 referred to as the "distance" between the images, indicates greater similarity between them.

In this research, we introduce the Local Binary Patterns methodology for face recognition implementation. Local Binary Patterns utilize the LBP operator to capture local features and summarize the unique structural characteristics of a face image [7]. LBP involves a set of binary comparisons of pixel intensities between the central pixel and its eight surrounding pixels, defined as an ordered sequence. This comparison process is achieved through the following formula:

$$LBP(x_c, y_c) = \sum_{n=0}^{7} s(i_n - i_c)2^n \qquad (15)$$

The value I_c represents the center pixel (x_c , y_c) , while I_n represents the values of the eight surrounding pixels. This calculation aids in identifying local features within the face and operates through the fundamental LBP operator. Initially, the feature extraction matrix is sized at 3 x 3, where comparisons are made based on the center pixel's value. Subsequently, a binary pattern code is generated, and further, the LBP code is derived by converting the binary code into decimal format.

```
Face Recognition Algorithm Input: Training Image
Set Output: Features extracted from face images, comparison with center pixel, and recognition of unknown face images
Initialize temp = 0
FOR each image I in the training image set
Initialize the pattern histogram, H = 0
FOR each center pixel $tc \in I$
Compute the pattern label of tc, LBP(1)
Increment the corresponding bin by 1
END FOR
Identify the highest LBP feature for each face image and combine into a single vector
Compare with the test face image
If it is the most similar face in the database, then it is successfully recognized
```

Diagram depicting the Local Binary Patterns (LBP) algorithm

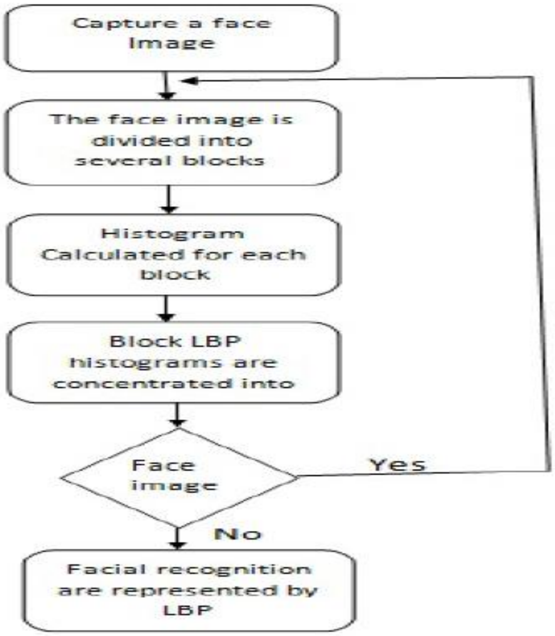

Capture a face Image
The face image is divided into several blocks
Histogram Calculated for each block
Block LBP histograms are concentrated into
Face image
Yes
No
Facial recognition are represented by LBP

Figure 22 Illustrates The LBP process flowchart

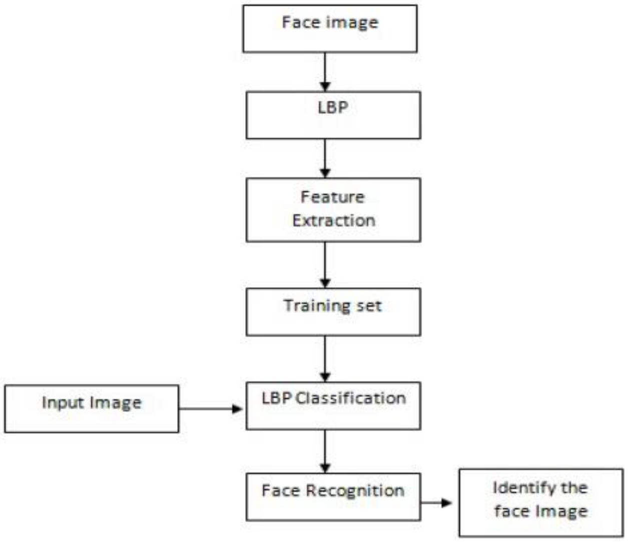


Figure 23 Diagram outlining the Proposed System's Workflow

II.7 Conclusion:

This part of work examines the complexities of face recognition, which is of great importance in various fields such as law enforcement, banking, security and personal identification. It focuses on three main aspects: face representation, feature extraction and classification. Face representation involves determining how to represent a face effectively, while feature extraction isolates crucial attributes from facial images. Classification involves comparing facial images against a database to identify matches. This study evaluates face recognition techniques that incorporate shape and texture information, in particular by exploiting Local Binary Patterns (LBP) for person-independent recognition.

III. Chapter 03: Visual markers

III.1 Definition of visual markers in prisoner monitoring:

Visual markers are signs or symbols designed to be easily recognized by machines. We use it to identify and track inmates within correctional facilities. They can be natural, such as unique physical features, or artificial, such as identification numbers or barcodes on detainees' clothing or bracelets.

Their role is essential to maintain order, observe the movements of inmates, and ensure security within Jails.

III.2 Examples of visual markers used in prisons:

III.2.1 Identification Numbers:

Identification Numbers serve as fundamental visual markers within jails, ensuring efficient inmate management and tracking. Each inmate is assigned a unique numerical identifier, visibly displayed on their uniform or bracelet. This numerical code not only helps in quick and accurate inmate identification but also simplifies administrative processes such as record-keeping and communication. By providing a standardized method of inmate identification, these numbers provide to the overall organization and security of the facility.

III.2.2 Barcodes or QR codes:

Barcodes and QR codes have emerged as indispensable tools for automated tracking and access control within prisons. These codes, printed on inmate uniforms or identification cards, enable rapid and accurate data capture during various procedures, including attendance checks and access to different areas of the facility. By simply scanning these codes, staff can efficiently verify inmate identities and monitor their movements, enhancing operational efficiency and security. Barcodes and QR codes allows for seamless integration with electronic systems, enabling real-time tracking and organization of prisoners' information.

III.2.3 Colored Bracelets:

Colored Bracelets serve as flexible visual indicators within jails, transmitting important information about inmate attributes and situations. These bracelets, assigned based on specific criteria such as security risk levels or privileges, provide valuable insights to staff for effective inmate supervision and management. For example, different colors may signify varying security clearance levels, medical conditions, or behavioral assessments, allowing staff to quickly identify and respond to individual needs. By incorporating color-coded bracelets into inmate identification protocols, prisons can enhance safety, streamline operations, and maintain a secure environment for all residents.

III.3 Examples of visual markers:

III.3.1 QR Codes:

QR Codes(Quick Response Codes) represent a sophisticated form of two-dimensional barcodes . These codes consist of a square grid composed of numerous small black and white squares, known as modules, arranged to encode information. Each module corresponds to a binary value, with white representing 0 and black representing 1. This binary pattern, structured according to a standardized format, enables seamless interpretation of the encoded data by any digital reader. The arrangement of modules within the QR Code ensures optimal readability and reliability, facilitating quick access to the information stored within.

QR Codes can be so flexible that they can store all varieties of information, such as texts, URLs, contacts, and more, they are valuable tools when we use it on applications and also industries.[16]

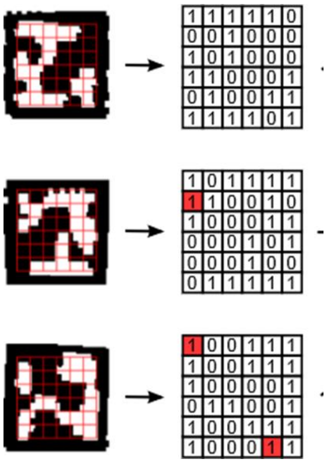
Figure 24 example of QR code

III.3.2 Aruco markers:

ArUco Markers are synthetic square fiducial markers used to aid detection and tracking in computer vision applications, including augmented reality.

An ArUco marker is composed of a wide black border and an internal binary matrix which determines its identifier (ID). The black border allows rapid detection in the image, and the binary coding allows its identification as well as the application of error detection and correction techniques.

The internal binary matrix is what distinguishes one ArUco marker from another, allowing each marker to have a unique ID. When an ArUco marker is detected in an image, it determine its presence by showing its unique id and this what we need to determine the identification of a prisoner each prisoner has a unique Aruco id printed on his suit.[10]



1	1	1	1	1	0
0	0	1	0	0	0
1	0	1	0	0	0
1	1	0	0	0	1
0	1	0	0	1	1
1	1	1	1	0	1

1	0	1	1	1	1
1	1	0	0	1	0
1	0	0	0	1	1
0	0	0	1	0	1
0	0	0	1	0	0
0	1	1	1	1	1

1	0	0	1	1	1
1	0	0	1	1	1
1	0	0	0	0	1
0	1	1	0	0	1
1	0	0	1	1	1
1	0	0	0	1	1

Figure 25 Binary code extraction from the ArUco marker

III.4 The Localization of ArUco Markers:

III.4.1 Enhancing Localization Efficiency with ArUco Marker Detection:

ArUco markers consist of square grids filled with black or white cells. The detection algorithms for these markers are highly reliable and accurate. [8]

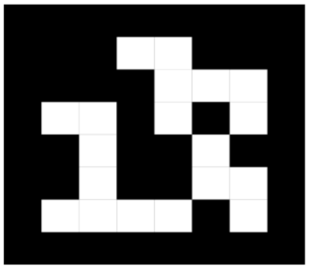


Figure 26 sample of ArUco Marker

A minimal library, based on OpenCV, has been developed for generating and detecting these markers.[11] These algorithms are designed to detect the marker even when it varies in orientation and size. This capability is crucial for relative localization. Detecting the marker and its four corners simplifies extracting its orientation relative to the camera, making the process efficient.

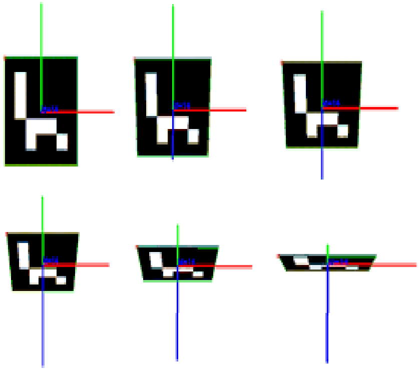


Figure 27 illustrates the detection process across different orientations

With a single camera, it's possible to calculate the marker's width, height, and orientation relative to the camera, but this requires precise camera parameters and possibly calibration.[17][18] However, for the proposed method, it's unnecessary to compute all these parameters. Calculating the yaw angle of the marker is deemed sufficient.

III.4.2 Improving 2-D Localization in Indoor Settings: Emphasizing Camera-Based Techniques:

This method focuses on the 2-D localization within inside environments, Hence, extracting two important pieces of information from the marker: the Relative Yaw angle between the marker plane's normal vector and the camera's line-of-sight and distance from the camera. The extracted information used to define a two-coordinate system. The model assumes that the normal vector of the marker plane and the camera's line of sight are on the same plane or parallel planes. That is, the camera plane and the marker plane are both perpendicular to the xy plane (floor).The localization module works more in localizing the camera relative to a single marker in polar coordinates. The node graph can be built to connect several markers. One of the markers will be designated as the "home marker" with coordinates set to local and global at (0,0).

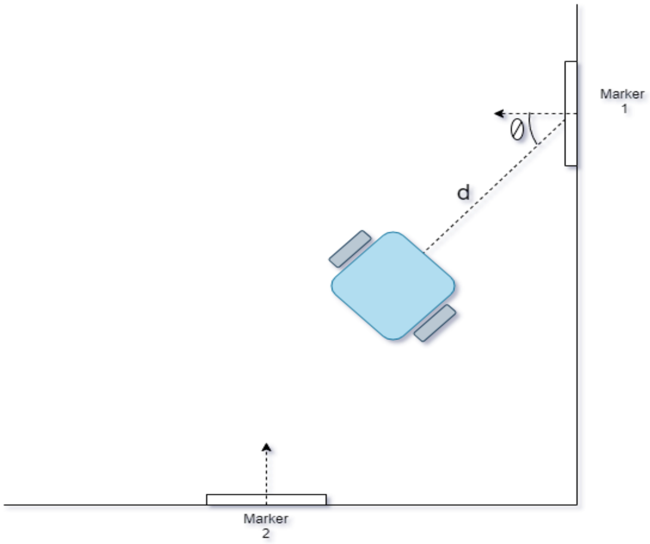


Figure 28 The visualization of the camera within the 2-D environment

From (Fig. 32), creating the 2-D pose of the camera relative to the marker requires two parameters: the angle θ (yaw), which indicates the rotation in the Z-axis of the marker concerning the camera, and the distance (d). Determining the distance can be achieved through various methods. a depth camera was employed to measure the distance (d). calculating the angle θ (yaw) value accomplished by using a camera without the need for calibration.

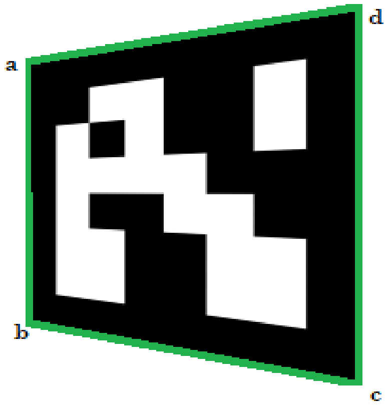


Figure 29 Marker rotated along the Z-axis

The ArUco library in OpenCV offers a method for obtaining orientation through Rodrigues rotation [19]. It needs a calibrated set of camera parameters and distortion coefficients. For obtaining the Yaw value. The library provides a list of four points with pixel coordinates representing the four corners of the marker: (xa, ya), (xb, yb), (xc, yc), and (xd, yd). Figure 33 provides an approximation of what the camera might perceive based on the previous illustration of the environment setup (Figure 32). To calculate the Yaw angle (θz), we first compute the apparent horizontal side length (s_a).

$$s_a = \frac{|x_a - x_d| + |x_c - x_b|}{2}$$

It is assumed that the ideal or true horizontal side length (si) is equal to one of the apparent vertical sides.

$$s_i = |y_a - y_b|$$

or

$$s_i = |y_d - y_c|$$

The value of the angle θ_z is calculated with this formula:

$$\theta_z = \arccos(\frac{s_a}{s_i})$$

We assumed that s_i is the side ab and θ_z:

$$\theta = \begin{cases} +\theta_z, & \text{if } |y_a - y_b| < |y_d - y_c| \\ -\theta_z, & \text{if } ||y_a - y_b| > |y_d - y_c| \end{cases}$$

This implementation provided accurate measurements of the angle (θz), However, it was observed that the measurement became less accurate when the marker was not aligned at the center of the frame. Similar issues were noted concerning the distance measurement.

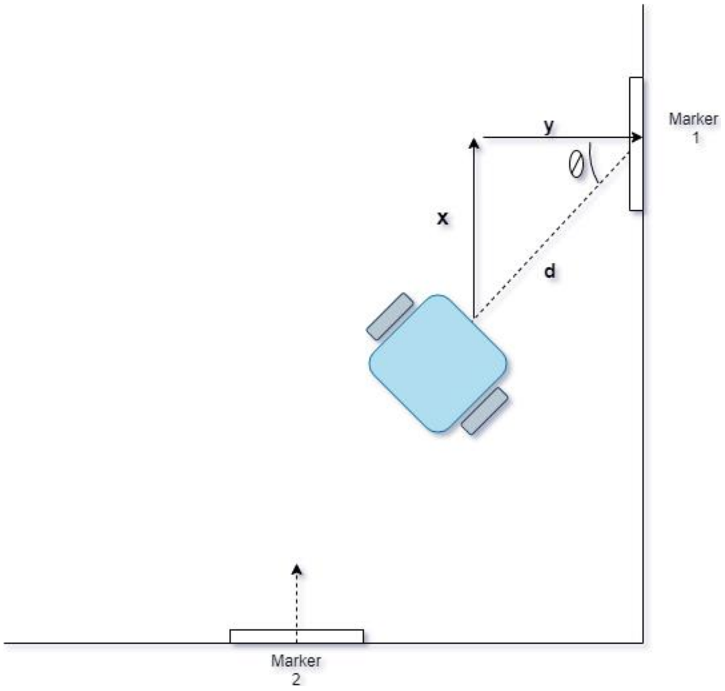


Figure 30 Displays the trajectory of the implementation

The alignment of the depth camera to the center of the frame was necessary to ensure reliable results. This alignment proved advantageous when constructing the node graph.

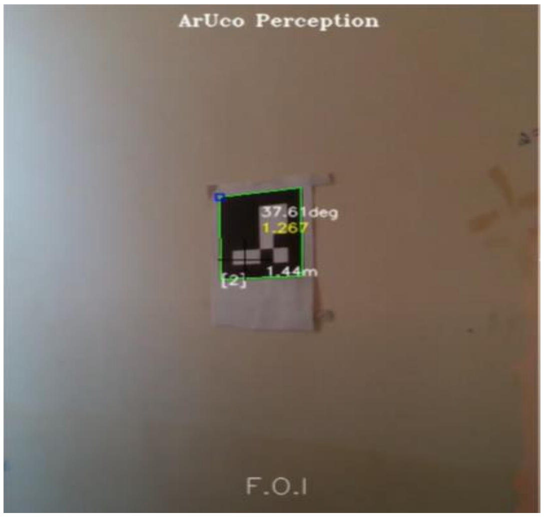


Figure 31 Corresponding the Marker ID=2

Cartesian coordinates were calculated using standard trigonometric formulas to create a trajectory for the camera to move towards the marker. The values of x and y, as shown in Figure 34, were computed, and the error was very low.

III.5 ArUco Marker identification:

III.5.1 Decoding Aruco Markers: Understanding Structure

Aruco markers are square in shape, featuring a black border and an internal grid utilized for storing a numeric identifier in binary format. These markers are identified using a dictionary, which outlines specific rules for computing the marker identifier, conducting validation, and implementing error correction. The original Aruco dictionary is employed in this study,[8] utilizing bits from the second and fourth columns of the marker grid to encode the marker identifier in standard binary format, while the remaining bits are allocated for parity checking. Figure 36 illustrates the initial four markers included in this dictionary.

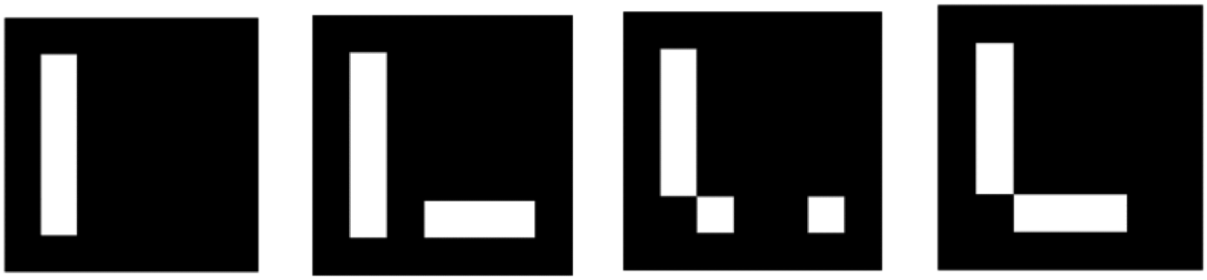
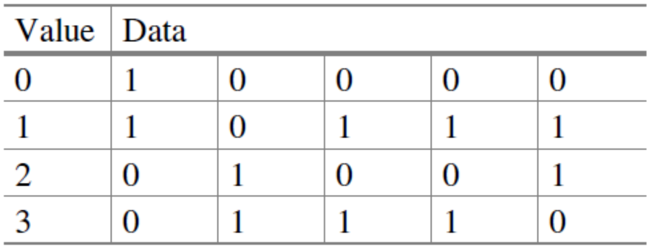


Figure 32 Aruco markers labeled with IDs 0, 1, 2, 3

To ensure the validity of the marker, a signature matrix is employed. Each row within this matrix encodes a possibility of 2 bits. For an Aruco marker to be considered valid, each of its rows must match one of the rows of the signature matrix. This ensures that the marker has only one valid rotation. Table 1 illustrates the signature matrix utilized in this dictionary.



Value	Data				
0	1	0	0	0	0
1	1	0	1	1	1
2	0	1	0	0	1
3	0	1	1	1	0

Tableau 1 showcases the signature matrix utilized for the validation of Aruco markers.

Analyzing the signature matrix reveals that it may not sufficiently ensure a single possible rotation for each marker. Figure 37 illustrates marker 1023, which exhibits horizontal symmetry, indicating multiple possible rotations.

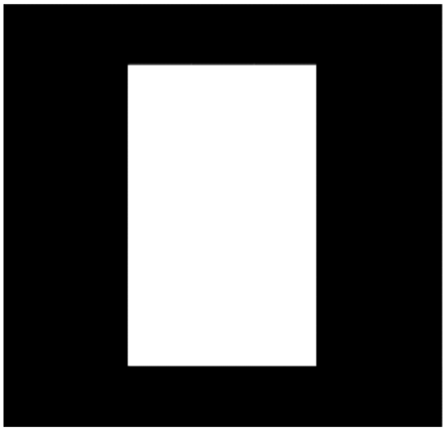


Figure 33 depicts Aruco marker 1023

III.5.2 Algorithm for Detecting Aruco Markers

The detection algorithm was executed utilizing the OpenCV library due to its extensive collection of image processing algorithms. Figure 38 illustrates the sequential steps employed for detecting and recognizing markers.

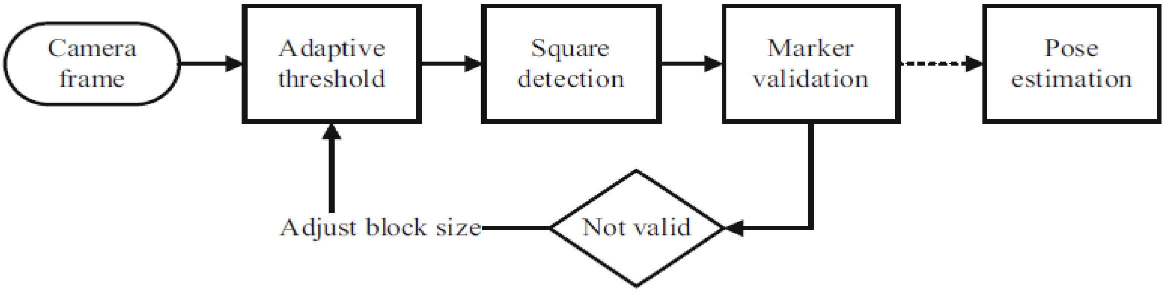


Figure 34 illustrates the diagram of the algorithm

The algorithm starts by employing adaptive thresholding [4] on the image. This method calculates a threshold value for each pixel based on the histogram of its surrounding neighborhood. It’s useful for scenarios with varying lighting conditions, adaptive thresholding ensures robustness. Figure 39 shows the outcomes following the application of adaptive thresholding.

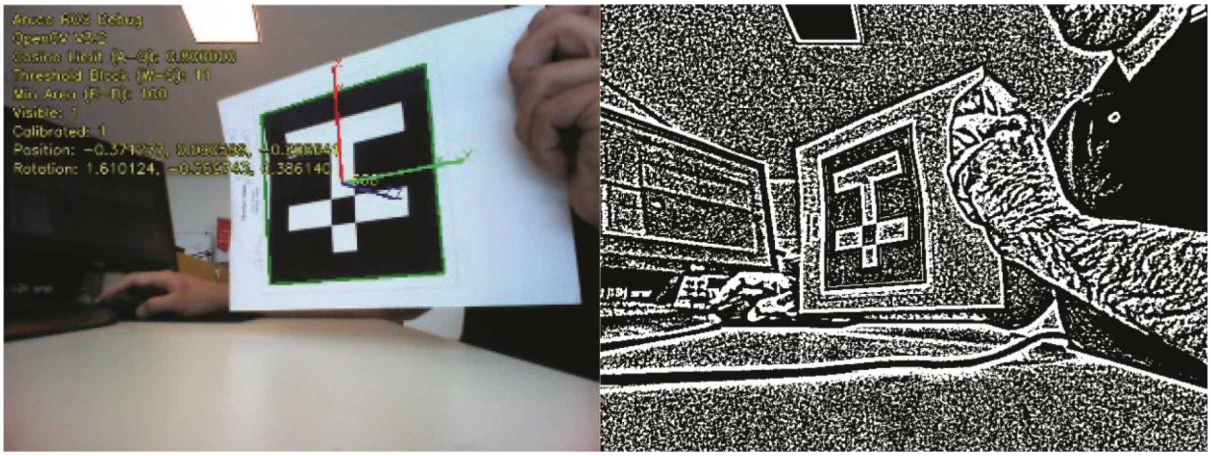


Figure 35 The result adaptive thresholding

For each frame, the block size selection is based on the average size derived from all block sizes where the maximum numbers of markers were detected. The block size is reassessed in instances where no markers are visible. Following the application of thresholding to the image, square detection is performed by identifying contours using a border-following algorithm [5], succeeded by the Douglas-Peucker contour simplification algorithm [6]. The Quadrilateral Sum Conjecture is employed as a criterion for square detection based on the detected contours. Despite significant perspective distortion, a square always remains a convex quadrilateral. Another criterion involves ensuring that the sum of the cosines of all inner angles is below a predefined threshold. Additionally, to eliminate noise, a third criterion is incorporated: contours forming geometry with an area below a predefined threshold are discarded.

These three criteria effectively filter squares, even in scenarios of significant distortion from the contour list. Figure 40 illustrates the resulting outcome obtained with a maximum sum of cosine set.

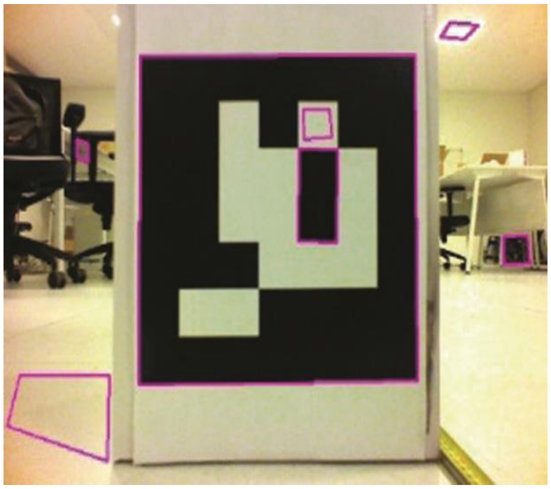


Figure 36 The outcome of the square detection algorithm

Perspective distortion is rectified in the identified squares, which are subsequently resampled into a 7 × 7 matrix through linear interpolation. A threshold is then applied using Otsu's Binarization algorithm [20], resulting in a matrix containing the marker data. Figure 41 depicts the matrix obtained following the binarization process.

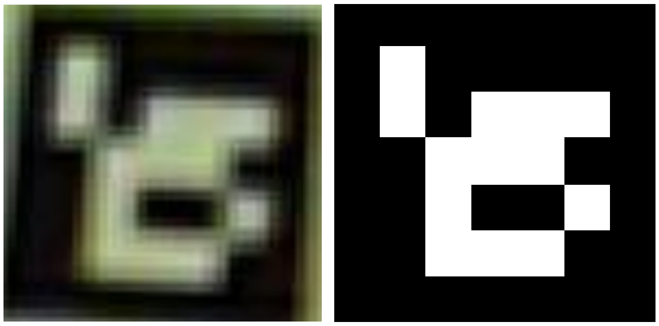


Figure 37 Marker reading process

At this point, the marker data undergoes validation as Aruco using the signature matrix. Markers may be detected in various orientations. The algorithm evaluates the data with different rotations (90º, 180º, 270º), and if the marker remains unrecognized for any rotation, it is discarded.

For pose estimation, the method solvePnp from OpenCV is utilized, employing iterative mode with Levenberg-Marquardt optimization.

To verify the camera position, markers must be registered within the program, each marker represented by its identifier and real-world pose (position and rotation). The corners obtained from all visible known markers are utilized to estimate the camera pose.

III.6 Conclusion:

In conclusion, this chapter has provided a comprehensive examination of visual markers and their crucial role in inmate tracking within jails. Through an analysis of various types of visual markers, such as identification numbers, barcodes, QR codes, and ArUco markers, a diverse of methods aimed at enhancing security and efficiency in inmate tracking have been explained. We focused on this chapter on ArUco markers, including their structure and application in localization and identification; we highlighted their paramount importance in modern monitoring systems. Moreover, the discussion on advancements in marker detection technology offers huge potential to enhance the precision and reliability of prisoner tracking, thereby promoting improved management and safety within jails.

IV. Chapter 4: Implementation and Integration of face and Visual Markers system.

IV.1 Introduction:

In this chapter, we design and implement the tracking system, which merges some technologies to obtain strong performance and enhance security and tracking in the prison perimeter. The system is designed to submit the actual time tracking in many different places, ensuring the identification and tracking of the unspecified prisoners. The main components consist of the generation of face recognition and visual signs structures, each of which contributes to increasing the ability to track. By combining these two technologies, we intend to expand a strong device that guarantees a special and continuous follow. Where, we prepare our planning and implementation planning, which merges some technologies to obtain strong general performance and improve safety and control in the prison perimeter.

IV.2 Class Diagram:

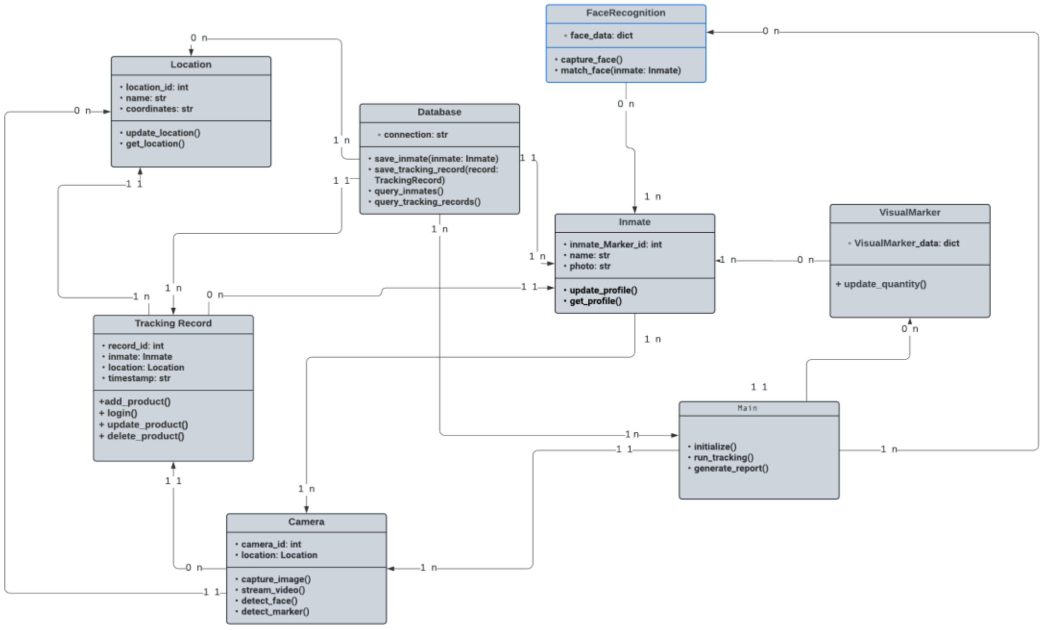


Figure 38 Class Diagramme

IV.3 Integration of visual markers into facial recognition systems:

Combination of Face and marker detection techniques for enhanced jail security: The combination of these two techniques allows us to capture and identify prisoners more precisely, pinpointing their position and location within the jail. In some cases, the Face recognition may not work because of bad lighting or due to a wrong position of the face. The ArUco markers are, therefore, a backup in such conditions. As soon as such a marker is detected, the ID of the prisoner is shown along with his name for quick identification. Moreover, an exchange of suits having ArUco identifiers triggers a different visual alert that depicts the distinction between the inmate's face and the ArUco marker on his attire enabling guards to take immediate action. Offenders face disciplinary action.[32]

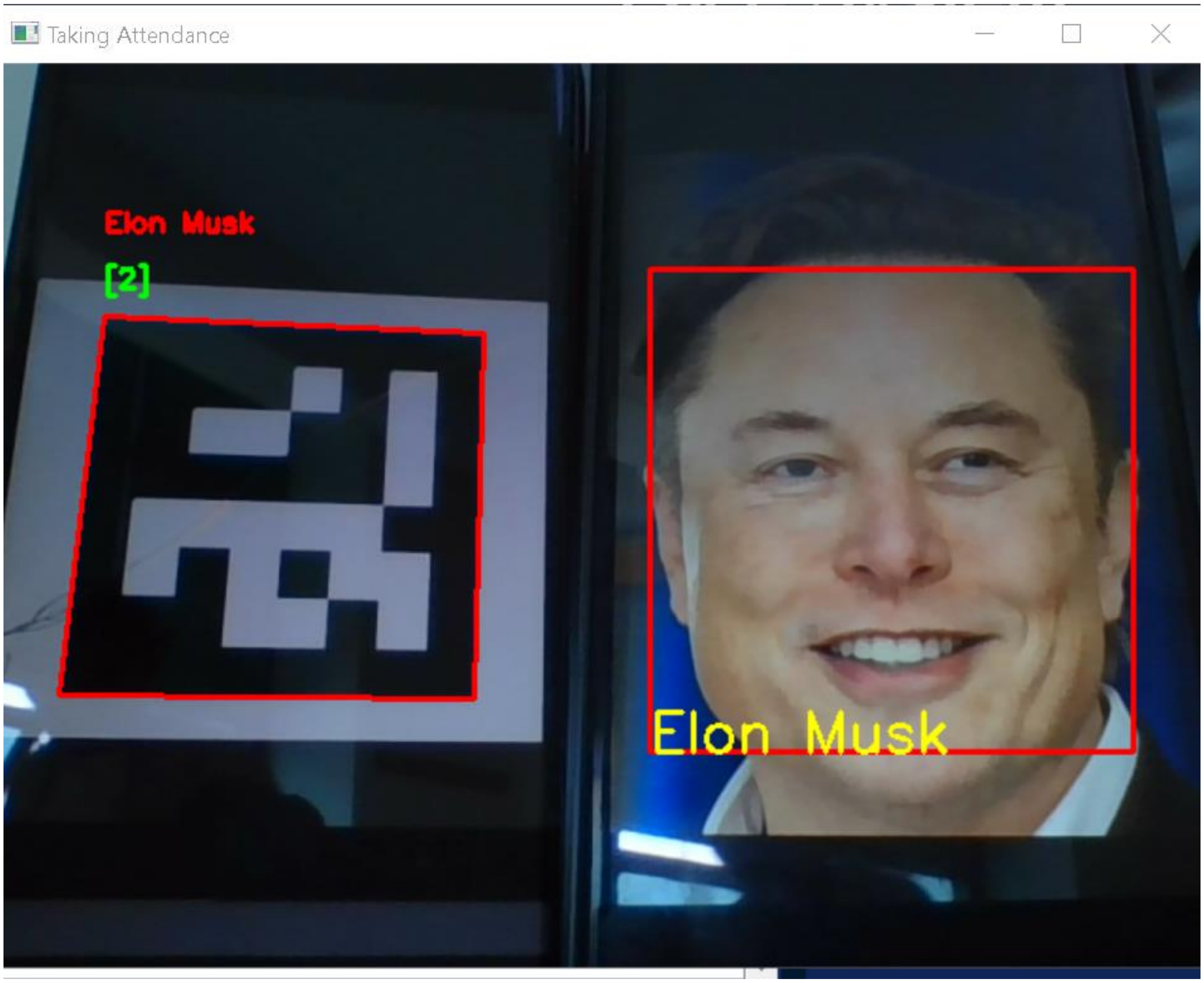


Figure 39 Integration of Face and ArUco Detection

IV.3.1 Image capture:

The initial level of integrating visual markers into facial systems entails capturing the photo of the user's face together with any visible markers they're sporting. capturing each the facial features and the exclusive items which include unique glasses or stickers at the skin. These visible markers are designed to be easily identifiable and might include encoded information like a completely unique ID or calibration facts, affecting the overall accuracy and reliability of the system.

IV.3.2 Face Detection:

Once the image is captured, the machine movements directly to the face detection stage. This includes using state-of-the-art algorithms to discover the face within the photo with the aid of identifying key features such as the contours, eyes, nose, and mouth. One of the most generally used algorithms for this cause is the Haar-Cascade, a machine gaining knowledge of-based technique that entails schooling a cascade feature with numerous fine and poor images. The set of rules detects edges and lines within the preliminary levels, combining them to pick out complicated patterns like faces. Accurate face detection is vital because it directly influences the effectiveness of subsequent levels in facial characteristic extraction and popularity.[32]

IV.3.3 Analysis of visual markers:

Simultaneously, the machine detects and analyzes the visual markers within the picture. These markers, designed to be without problems recognizable, can also include encoded facts together with a completely unique ID. The device's algorithms identify these markers and extract the encoded statistics. Upon detecting a marker. This step adds an extra layer of verification, reducing the chance of fake positives and improving the robustness of the identification process. The integration of visible markers complements and the Face recognition system, imparting a multifaceted technique to identification verification.[10]

IV.3.4 Feature extraction:

Facial recognition with LBP is mainly by the face of the face, then face features are extracted from an image, then LBP is used to extract the fabric features of some areas of the face. LBP, being the operator, is the small domestic biology of the pixel in relation to the center pixels, thus providing the details of the texture of the face in the form of bilateral patterns. These patterns work as unique features used to compare with a database for well -known faces to get the best matches. This integrated approach enables the system to identify the individual according to his texture file.

IV.3.5 Comparison and identification:

The extracted data includes facial features and visual signs, which are then matching with a database of known faces and signs. Among the discovered features and stored in the database, the user's identity is confirmed. The multi -step process in this way really gives the system the ability to identify prisoners with a high degree of accuracy and reliability using the facial features and unique visual signs.

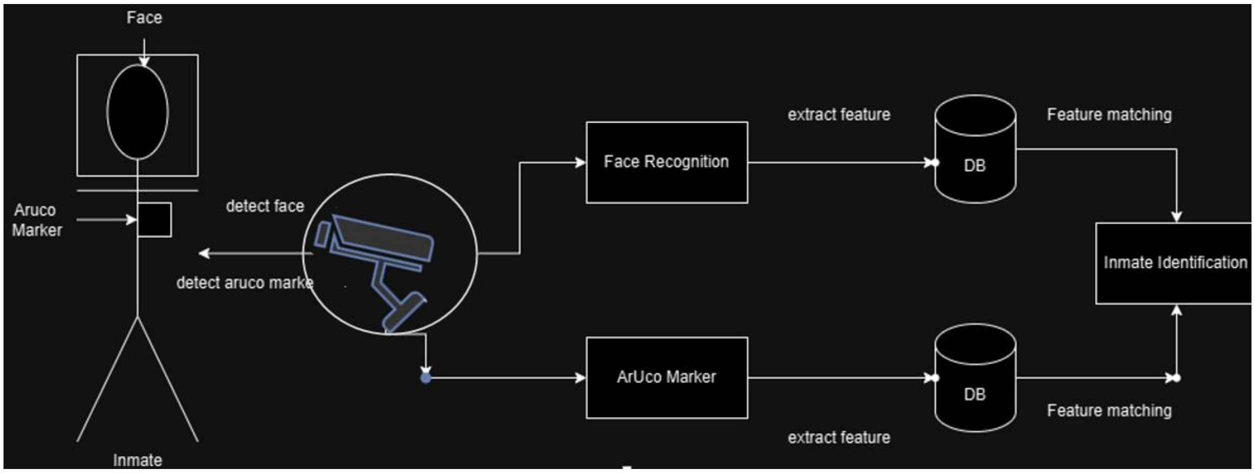
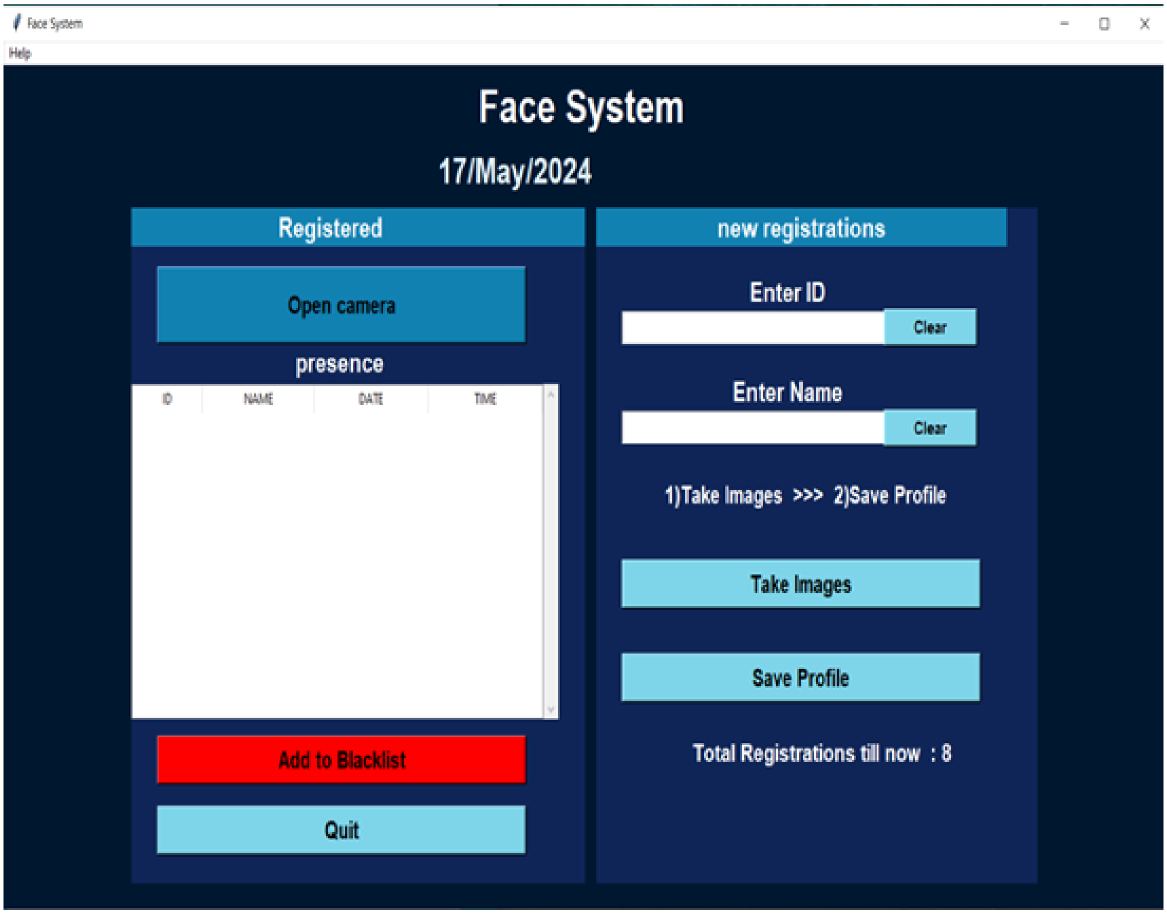


Figure 40 Comparaison and identification

IV.4 Application Interface :



17/May/2024

Total Registrations till now : 8

Figure 41 application Interface

1. Run the program
2. Enter your identification (ID, name) the id is the same as the id marker.
3. Take images to yourself (a video cam will be appeared to take a lot of images of yours)

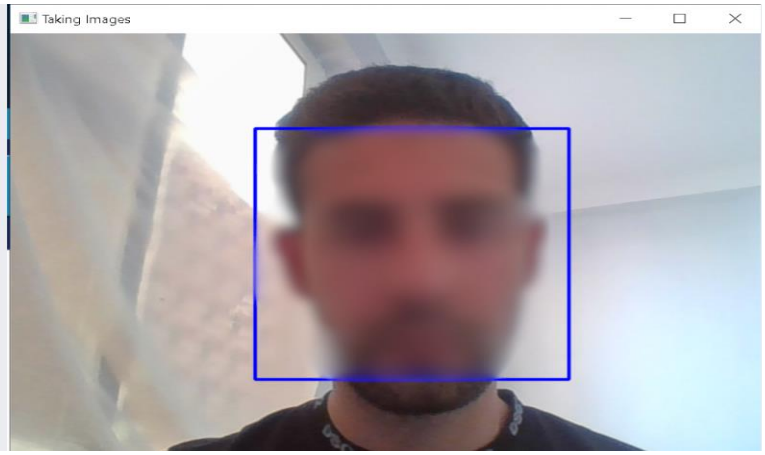
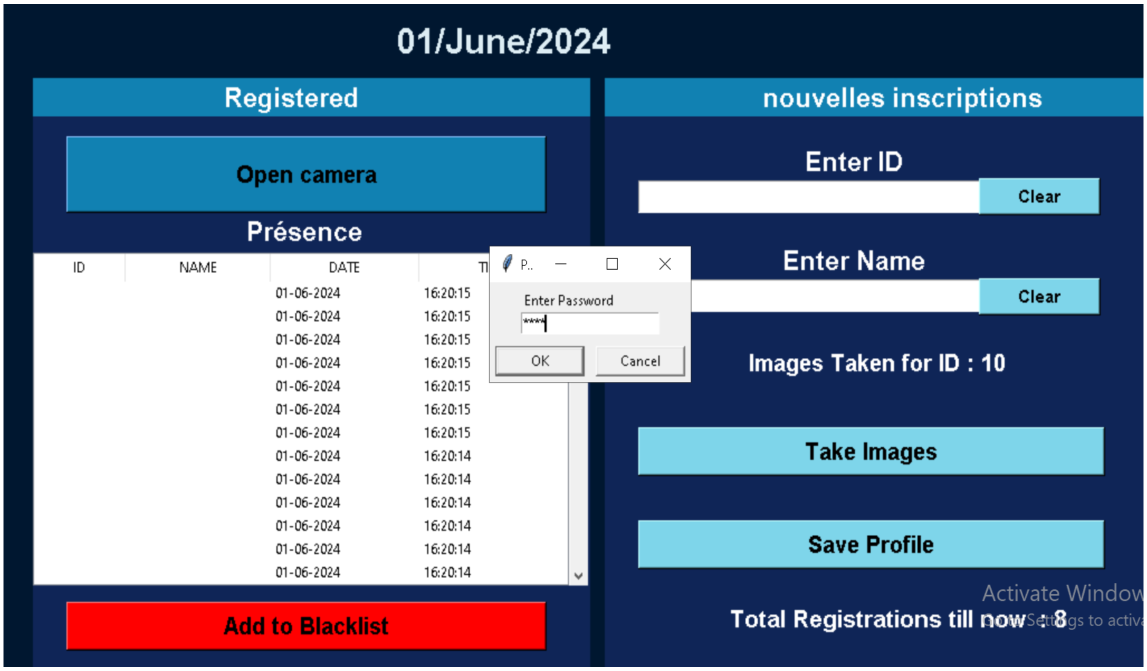


Figure 42 Take images

4. Save the profile and then enter the password to save the profile



ID	NAME	DATE	TI
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:15
		01-06-2024	16:20:14
		01-06-2024	16:20:14
		01-06-2024	16:20:14
		01-06-2024	16:20:14
		01-06-2024	16:20:14
		01-06-2024	16:20:14

Images Taken for ID : 10

Total Registrations till now : 8

Figure 43 shows the profile saves

5. Open camera to test your web application

Here is the integration of face recognition and Aruco marker

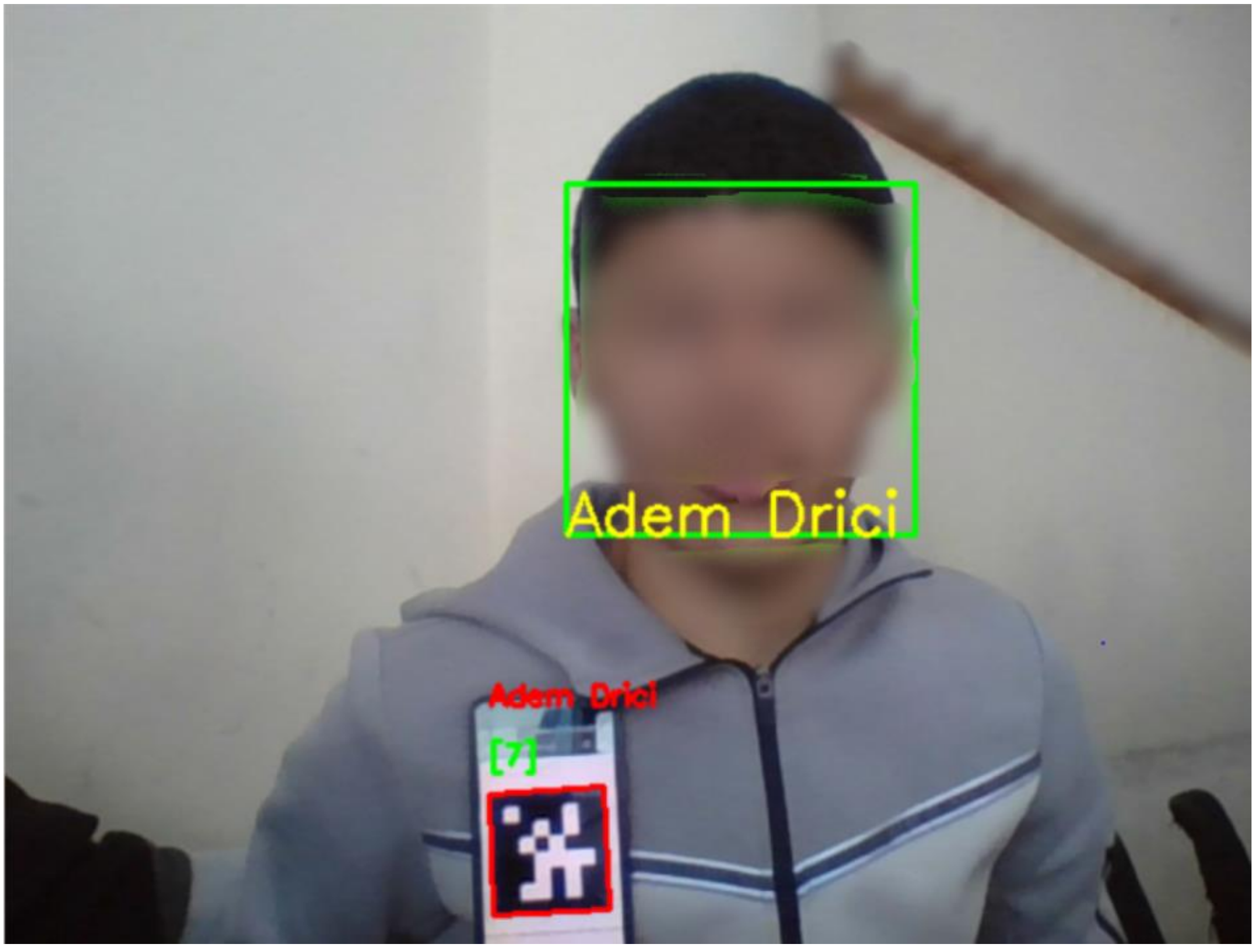
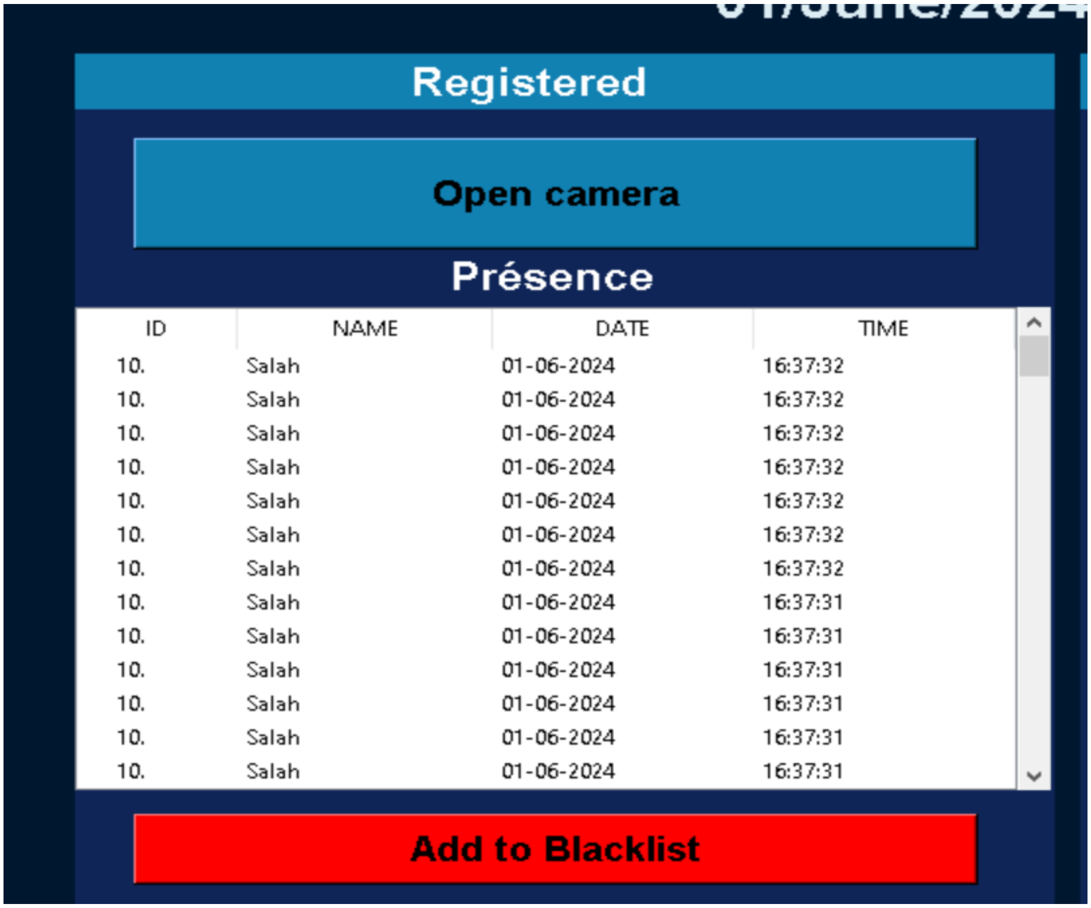


Figure 44 the integration of aruco marker with the face

7. Press (q) to close the window

Finally, it displays the ID marker of the prisoner along with their name, as well as the date and time of attendance, tracking the prisoner's presence until they leave their designated area.



ID	NAME	DATE	TIME
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:32
10.	Salah	01-06-2024	16:37:31
10.	Salah	01-06-2024	16:37:31
10.	Salah	01-06-2024	16:37:31
10.	Salah	01-06-2024	16:37:31
10.	Salah	01-06-2024	16:37:31
10.	Salah	01-06-2024	16:37:31

Figure 45 the identification of a prisoner with the time attendance.

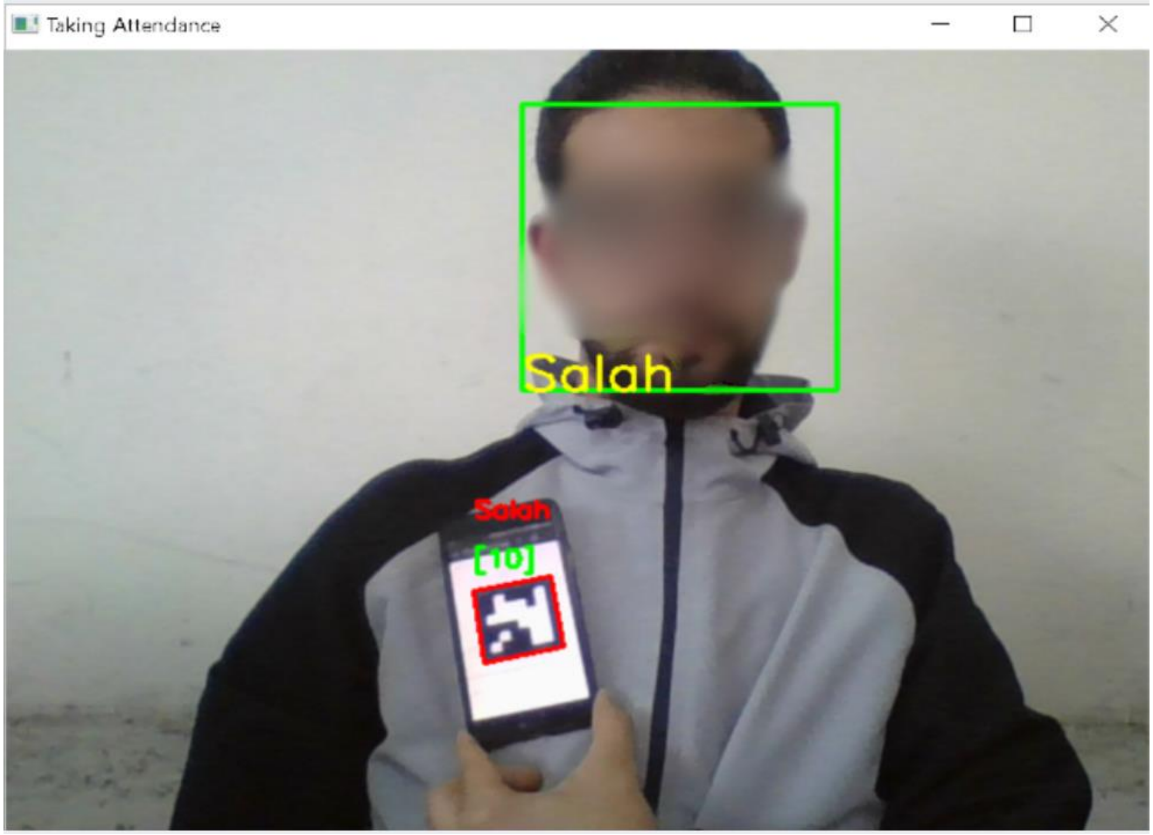
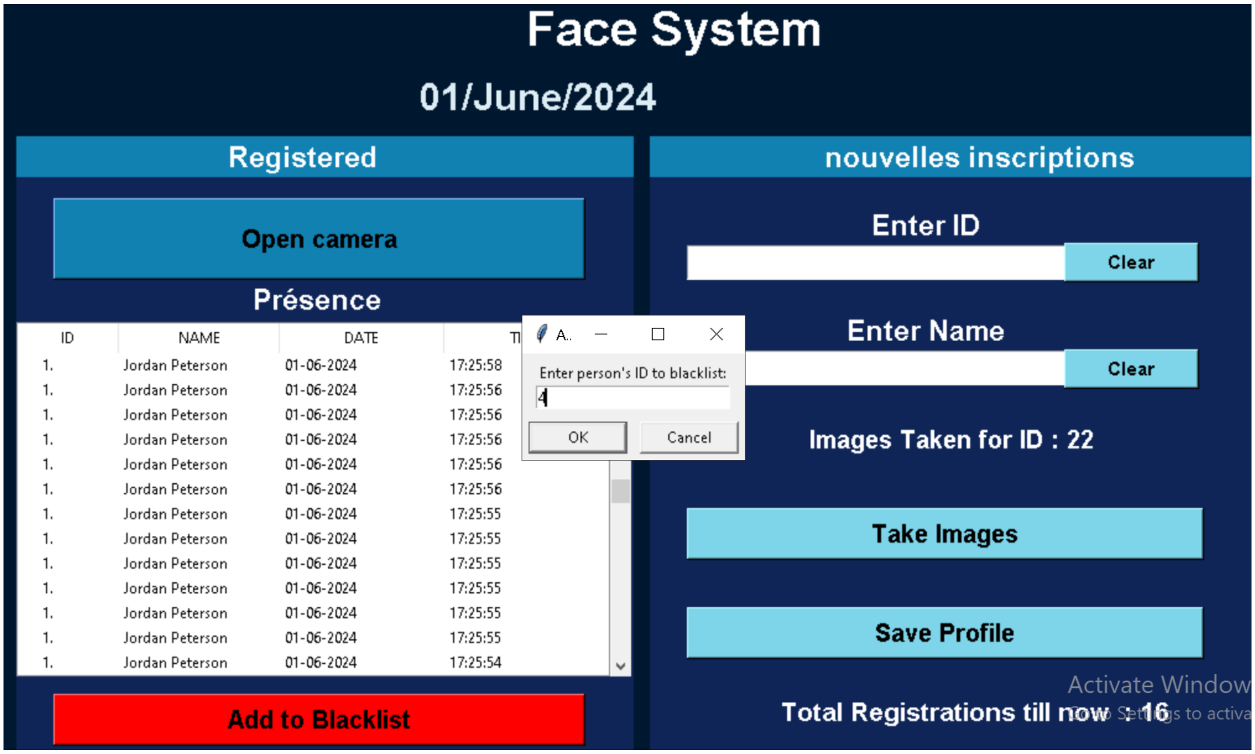


Figure 46 face recognition and the identification of the unique Aruco marker

We can also add a dangerous prisoner to the blacklist to highlight his face we determine a red rectangle on his face Here is the steps:

1. Enter the information of the prisoner (ID, name) like we did before.
2. Save the profile
3. Press on the red key (Add to Blacklist)



Enter person's ID to blacklist: 4

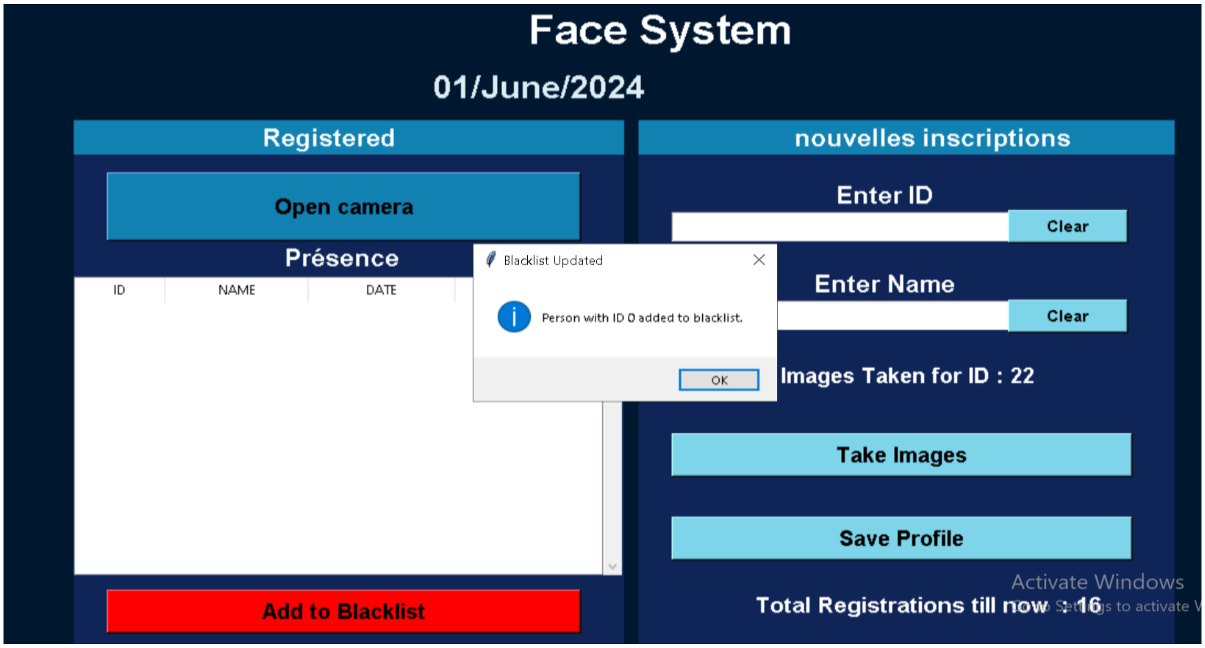
Images Taken for ID : 22

Total Registrations till now : 16

ID	NAME	DATE	TI
1.	Jordan Peterson	01-06-2024	17:25:58
1.	Jordan Peterson	01-06-2024	17:25:56
1.	Jordan Peterson	01-06-2024	17:25:56
1.	Jordan Peterson	01-06-2024	17:25:56
1.	Jordan Peterson	01-06-2024	17:25:56
1.	Jordan Peterson	01-06-2024	17:25:56
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:55
1.	Jordan Peterson	01-06-2024	17:25:54

Figure 47 add the prisoner with the id 4 to the blacklist

4. Enter the prisoner's id to add them to the blacklist



Person with ID 0 added to blacklist.

Images Taken for ID : 22

Total Registrations till now : 16

Figure 48 a prisoner added to the blacklist with success

5. Open the camera to check for the inmate

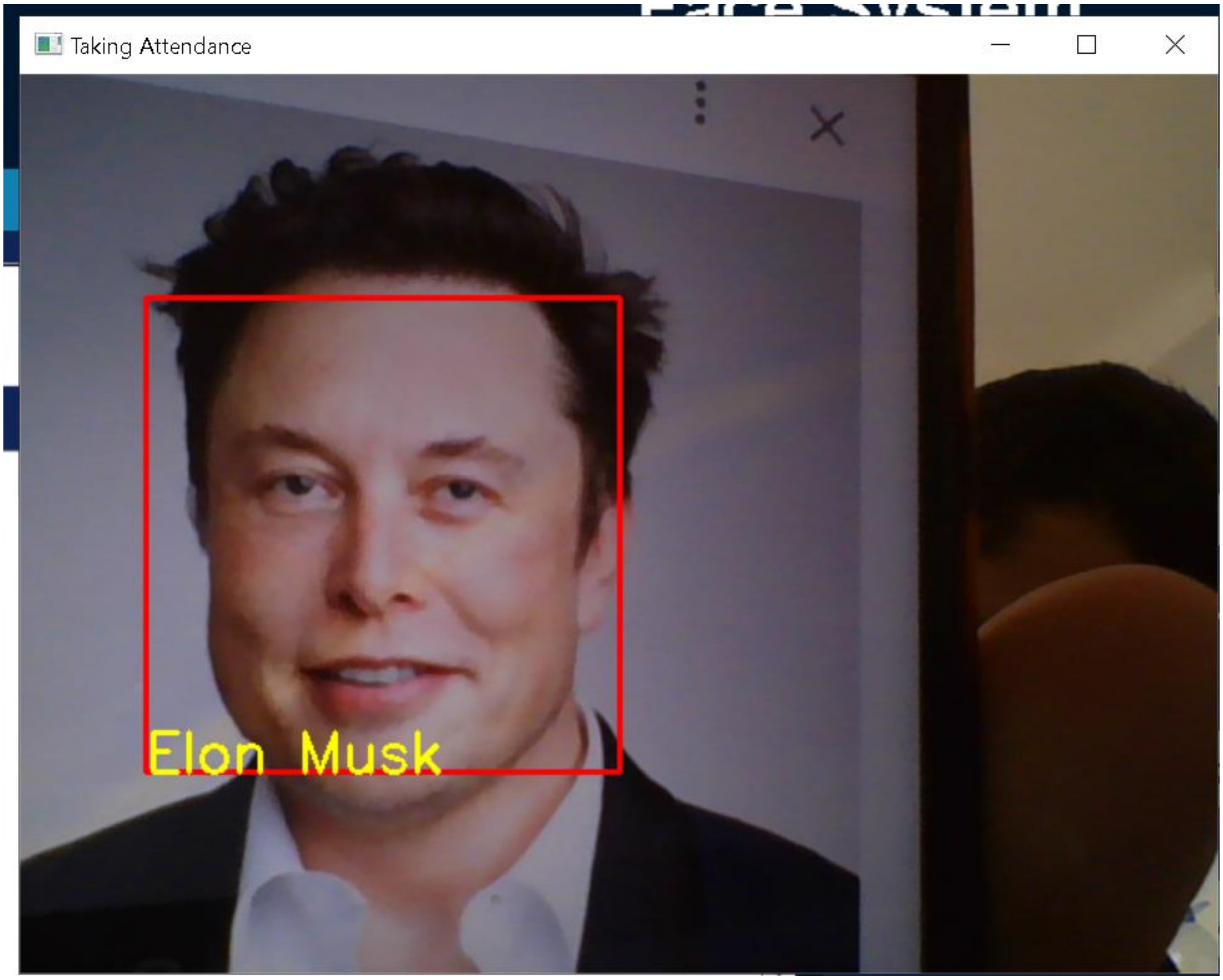


Figure 49 shows a dangerous prisoner with the red border on his face.

IV.5 Implementation

IV.5.1 Architecture of the tracking system:

IV.5.1.1 General structure of the system:

The Tracking system is designed with a storage system that allows Connected different components through a storage: the set of core modules comprises a video recording module, which includes high-definition cameras and video recording equipment placed throughout the prison; a processing module, which cleans and enhances the captured images for better quality for further analysis; a facial recognition module that uses the algorithms to extract and analyze facial features; a Visual Marker Detection Module that applies a unique algorithm to detect and identify visual markers on prisoners. The module integrates results on facial detection and facial recognition to produce reliable signals. All data, including images and analysis results, are safely stored in the database and data management. , the user interface lets administrators monitor system results in real time.[1]

IV.5.1.2 Data flow:

System performance Data includes several important steps. Initially, images are captured by the camera and sent via a secure network to the processing model where they are cleaned and enhanced. Preprocessed images are analyzed with both face recognition and pattern recognition. The results of this analysis are combined in the Data Fusion Module to produce final diagnostic results that are stored in the database. The results are then displayed to user, allowing monitoring the system in real time.

IV.5.1.3 Workflow:

The operation of the Tracking system works via registering the detainee, taking a video and photograph of the detainee, identifying him, and storing all data, along with facial popularity profiles and physical marks, in the database. For actual-time monitoring, video cameras continuously record the prisoner's moves and ship them to facial recognition and signal processing offerings. Detected alerts are blended with a database to create and save a series of logs that show detection instances and place. It provides instant tracking of prisoners and guards. The device also gives clear reporting of tracking statistics to permit historical analysis of protection audits and upgrades.

IV.5.2 System testing and validation:

IV.5.2.1 Test scenarios:

System monitoring system includes a comprehensive evaluation of diverse additives to make sure most fulfilling overall performance and reliability. Facial reputation testing makes a specialty of comparing the accuracy of the system's algorithms in special lighting conditions and shooting the extraordinary personalities of prisoners in order that the system can appropriately recognize people irrespective of those changes. The identity check demonstrates the algorithms' potential to appropriately perceive and examine the identification tags worn with the aid of inmates, which might be critical for proper identification. Data fusion testing confirms the importance of mixing facial recognition and gesture improves basic accuracy the usage of each strategies. Finally, performance checking out measures the velocity and capability of the device whilst processing big quantities of data, so you can keep performing properly below load and during height intervals. These tests display that the monitoring gadget is strong, dependable and geared up to be used in prisons.

IV.5.2.2 Challenges:

The trouble in making current jail monitoring systems effective lies inside the various demanding situations it poses. Environmental conditions consist of versions in lighting fixtures and digital camera conditions, each of which pose a hard undertaking to technique and require the device's algorithm to continuously adapt to adjustments to maintain its accuracy and reliability. These environmental constraints are important in growing algorithms which might be adaptable and powerful in extraordinary conditions. Privacy and ethical problems associated with the implementation of this kind of application also are essential, as the rights and dignity of prisoners have to be blanketed. Privacy troubles are addressed at the same time as retaining appropriate ethical requirements in handling and storing records and ensuring that the gadget operates in a obvious and accountable manner. By efficiently addressing those problems, the tracking gadget achieves its purpose at the same time as keeping the concepts of fairness, transparency, and admire for privateness.

IV.5.2.3 Validation methods:

the effectiveness of the monitoring system involves utilizes strong approaches in real-time verification of its precision and reliability. By employing an existing database well-known picture and branding to display instrument results in line with specified parameters, testing through the existing database offers a basis for validation. This approach guarantees reliability in that it ensures that the results of the system match the desired results. In addition, real-time experience offers profound insight into software performance in a surround that is constantly changing. Through the use of the system in a real environment, you can be aware of potential weaknesses for higher overall performance. This form of testing not only verifies the general performance of the machine but also enhances its adaptability in fixing specific problems within the environment. Control structures can offer consideration, reliability, and compliance to enhance safety and control in correctional facilities.

IV.5.2.4 Expected results:

Precision is expected in the system high rates of correctly identifying the face, together with the precise detection of visual markers. High precision implies that the system is sure to correctly identify individuals, thereby enhancing its overall accuracy. Second, the identification error rate is highly expected to be low, such that there will be a reduced false identification rate. Such improvements shall be seen because two methods facial recognition and the detection of visual markers are combined in ways that the likelihood of misidentification decreases. Third, the system wherein it is capable of quickly processing images and returning results in a timely fashion. This responsiveness shall be paramount for the system to effectively work in real time with quick and reliable feedback.

IV.6 Discussion of Findings:

From the analysis, some vital findings had been mentioned on the effectiveness of inmate tracking the use of face and visible markers: the facial recognition system validated excessive accuracy in identifying inmates throughout special camera angles and lighting situations. Visual markers brought vital supplementary facts, especially while facial popularity is hampered by means of occlusions or low image nice.

However, the evaluation additionally threw up some weaknesses inside the monitoring gadget, which include fake positives from facial recognition in some instances and troubles in tracking in crowded or chaotic situations. The demanding situations deliver out the want to have monitoring algorithms and surveillance infrastructures stay subtle and optimized.

Overall, the effects from this study have contributed to our knowledge of inmate monitoring technologies and possible uses in correctional settings.

IV.7 Technical Choices:

IV.7.1 Programming Language:

- **Python:** Python changed into decided on because the number one programming language. It boasts a complete suite of libraries designed for device reading and image processing, which encompass OpenCV and Dlib. These libraries are pivotal for implementing facial reputation systems. Python's syntax is clear and readable. Furthermore, the language enjoys big community guide, making sure that developers can with no hassle discover solutions to capability issues and constantly enhance the machine. Python’s seamless integration with other technologies and its powerful skills in dealing with complex responsibilities make it a desire for this task.

IV.7.2 Facial Recognition Technology:

- **OpenCV:** is used for primary image processing and face detection. OpenCV is known for its excellent functionality and user-friendly interface, which helps in the processing of photos. For real face obligations, Dlib is used because of its high accuracy and strength. Dlib algorithms are up to date to ensure singular identity and reliable performance generally under different circumstantial conditions. This combination of OpenCV and Dlib takes advantage of the better features of each of these libraries in order to offer a greener and more accurate facial recognition system.

IV.7.3 Visual Marker Technology:

ArUco Markers: ease of identification was the main reasons for choosing ArUco Markers. They are very efficient because they can easily be distinguished and hence detected with accuracy from images. The OpenCV package itself has functions to handle the ArUco Markers, hence the ease of implementation. This technology will ensure that there will be precise identification of data since it is a critical application.[10]

IV.7.4 Database Management:

Pandas: is used for statistics processing and storage in CSV files, which offers a truthful and transparent solution for dealing with data. Pandas is a powerful records manipulation device that helps clean managing, cleansing, and processing of data. Storing statistics in CSV documents ensures flexibility, as those files are without difficulty reachable and may be speedy edited or analyzed. This approach is particularly wonderful during the improvement and testing levels, bearing in mind fast iterations and changes.

IV.7.5 Hardware:

Cameras: These cameras are strategically placed to ensure superior coverage of the regions beneath surveillance. High-resolution capabilities are critical as they offer clean, certain pictures that may be critical for figuring out individuals and incidents. The cameras are ready with superior capabilities which include night time imaginative and prescient, motion detection. Their IP-based connectivity allows, allowing remote access and control, which enhances the flexibility and scalability of the surveillance machine.

Servers: To take care of the huge amounts of statistics generated by the cameras, the device employs high-overall performance servers. Models, that is critical for studying video feeds in real-time and extracting actionable insights. The servers additionally provide ample storage capability to accommodate the massive volumes of information produced. Efficient processing and garage competencies make certain that records are conveniently available for evaluation and retrieval when wanted. This setup no longer most effective supports the actual-time processing demands but additionally permits for the storage of ancient statistics, which can be useful for fashion analysis and lengthy-time period planning.

IV.8 Conclusion:

The implementation of a tracking system based on facial recognition and visual markers in the correctional facility made tremendous improvement in correctness of identity and efficiency. The system designed as modular and scalable proved to be efficient in the adaptation of the facility's needs, while real-time processing capabilities improved security management. Environmental factors and privacy issues are among the many issues that made the success of the case study shallow. This case study proves that this kind of system has the potential to be applied in many correctional institutions. Further research and development are needed to refine the technology further and deal with the remaining issues so that it can be used with even more reliability and acceptance.

V. General Conclusion:

Ensuring the safety and security within prisons relies heavily on effective inmate tracking systems. Our exploration begins with both traditional and modern methods used to monitor inmates. Traditional methods include video surveillance, visual and direct inspections, and frequent communication between officers. These approaches ensure continuous monitoring and quick responses to any issues.

In addition to these methods, biometric tools such as facial recognition, fingerprint identification, and retina and iris scans have become integral to modern inmate tracking. Behavioral characteristic tools, like signature and voice recognition, further enhance monitoring capabilities. The use of RFID technology allows real-time location tracking of inmates, significantly improving monitoring accuracy and efficiency.

Facial recognition technology is a sophisticated system that involves several key steps: face detection, face analysis, image-to-data conversion, and comparison and identification. This chapter delves into each of these steps, outlining their roles and significance in the overall process.

In our system, we employ the Haar Cascade Algorithm for face detection due to its efficiency and reliability. Following detection, we utilize the Local Binary Pattern (LBP) method for face recognition. This chapter provides a comprehensive explanation of these techniques, highlighting their advantages and how they contribute to the accuracy and effectiveness of our facial recognition system.

In our system, we utilize Aruco Markers to track inmates within correctional facilities. Here, we explore the application of visual markers in both traditional and modern contexts, emphasizing the use of Aruco marker technology to enhance inmate monitoring. In prisons, visual markers such as Identification Numbers, Barcodes or QR Codes, and Colored Bracelets are used for identification and management. Identification numbers are assigned to each inmate, while barcodes or QR codes facilitate quick scanning and digital record-keeping. Colored bracelets help in identifying different categories of inmates, such as those with medical conditions or varying security levels.

Modern applications of visual markers include QR Codes, which are widely used for accessing information and verifying identities, and Aruco Markers, which we use in our system as a backup to track inmates in cases where their faces do not appear. Identification of Aruco markers begins by explaining their structure and decoding process. This involves capturing an image, applying adaptive thresholding, extracting squares, validating these squares through inner codification, and finally extracting and displaying the marker's ID.

Integrating facial recognition technology with ArUco markers enhances prisoner tracking and monitoring within correctional facilities. We begin with a class diagram illustrating the structure of our program, providing a clear overview of its components and their interactions. This integrated approach leverages two advanced technologies: facial recognition and ArUco markers. ArUco markers, affixed to the prisoners' suits, serve as unique identifiers for each inmate. The program is designed to track inmates using both facial recognition and ArUco marker detection.

When a prisoner's face is not detected, the ArUco marker acts as a backup identifier, ensuring continuous tracking. Additionally, when an ArUco marker is detected, the program displays the prisoner's name alongside the marker's ID. A critical feature of the program is its ability to detect and alert authorities if a prisoner exchanges suits with another inmate. If the face recognition result does not match the ArUco marker ID, an alert is triggered, indicating a mismatch between the face's name and the marker's name. This mechanism helps maintain security and enforces disciplinary action against offenders who attempt to deceive the system.

We provided practical examples demonstrating the program in action, accompanied by images and performance metrics, showcasing the accuracy and reliability of the tracking system. Additionally, we covered the tools and technologies used in the development of the program, such as Python, OpenCV, and pandas. We also presented a use case diagram that explains the method and workflow of the integrated system, offering a visual representation of how the program operates. This comprehensive understanding of the integrated facial recognition and ArUco marker system highlights its innovative approach to enhancing prisoner tracking and security within correctional facilities.

VI. Bibliography

[1] Hickman, L. J., Davis, L. M., Wells, E., & Eisman, M. Document Title: Tracking Inmates and Locating Staff with Active Radio-Frequency Identification (RFID): Early Lessons Learned in One US Correctional Facility.

[2] Ahonen, T., Pietikainen, M., Hadid, A., & Maenpaa, T. (2004, August). Face recognition based on the appearance of local regions. In Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004. (Vol. 3, pp. 153-156). IEEE.

[3] Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. Pattern recognition, 29(1), 51-59.

[4] Sezgin, M., & Sankur, B. L. (2004). Survey over image thresholding techniques and quantitative performance evaluation. *Journal of Electronic imaging*, *13*(1), 146-168.

[5] Suzuki, S. (1985). Topological structural analysis of digitized binary images by border following. *Computer vision, graphics, and image processing*, *30*(1), 32-46.

[6] Wu, S. T., da Silva, A. C., & Márquez, M. R. (2004). The Douglas-peucker algorithm: sufficiency conditions for non-self-intersections. *Journal of the Brazilian Computer Society*, *9*, 67-84.

[7] Chen, T., Yin, W., Zhou, X. S., Comaniciu, D., & Huang, T. S. (2006). Total variation models for variable lighting face recognition. IEEE transactions on pattern analysis and machine intelligence, 28(9), 1519-1524.

[8] Garrido-Jurado, Sergio, et al. "Automatic generation and detection of highly reliable fiducial markers under occlusion." Pattern Recognition 47.6 (2014): 2280-2292.

[9] Zhang, X., Fronz, S., & Navab, N. (2002, October). Visual marker detection and decoding in ar systems: A comparative study. In *Proceedings. International Symposium on Mixed and Augmented Reality* (pp. 97-106). IEEE.
Chicago

[10] Kedilioglu, O., Bocco, T. M., Landesberger, M., Rizzo, A., & Franke, J. (2021, October). ArUcoE: enhanced ArUco marker. In 2021 21st International Conference on Control, Automation and Systems (ICCAS) (pp. 878-881). IEEE.

[11] Romero-Ramirez, F. J., Muñoz-Salinas, R., & Medina-Carnicer, R. (2018). Speeded up detection of squared fiducial markers. Image and vision Computing, 76, 38-47.

[12] Viola, P., & Jones, M. (2001, December). Rapid object detection using a boosted cascade of simple features. In *Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001* (Vol. 1, pp. I-I). Ieee.

[13] Lienhart, R., & Maydt, J. (2002, September). An extended set of haar-like features for rapid object detection. In *Proceedings. international conference on image processing* (Vol. 1, pp. I-I). IEEE.

[14] Ahonen, T., Hadid, A., & Pietikainen, M. (2006). Face description with local binary patterns: Application to face recognition. *IEEE transactions on pattern analysis and machine intelligence*, *28*(12), 2037-2041.

[15] Zhao, W., & Chellappa, R. (1999). *Robust face recognition using symmetric shape-from-shading*. College Park: Computer Vision Laboratory, Center for Automation Research, University of Maryland.

[16] Soon, T. J. (2008). QR code. synthesis journal, 2008, 59-78.

[17] Babinec, A., Jurišica, L., Hubinský, P., & Duchoň, F. (2014). Visual localization of mobile robot using artificial markers. *Procedia Engineering*, *96*, 1-9.

[18] Lim, H., & Lee, Y. S. (2009, August). Real-time single camera SLAM using fiducial markers. In *2009 ICCAS-SICE* (pp. 177-182). IEEE.

[19] Dai, J. S. (2015). Euler–Rodrigues formula variations, quaternion conjugation and intrinsic connections. *Mechanism and Machine Theory*, *92*, 144-152.

[20] Otsu, N. (1975). A threshold selection method from gray-level histograms. *Automatica*, *11*(285-296), 23-27.

[21] Miles, C. A., & Cohn, J. P. (2006). Tracking prisoners in jail with biometrics: An experiment in a navy brig.

[22] Viola, P., & Jones, M. J. (2004). Robust real-time face detection. *International journal of computer vision*, *57*, 137-154.

[23] Yang, B., Yan, J., Lei, Z., & Li, S. Z. (2014, September). Aggregate channel features for multi-view face detection. In *IEEE international joint conference on biometrics* (pp. 1-8). IEEE.

[24] Pham, M. T., Gao, Y., Hoang, V. D. D., & Cham, T. J. (2010, June). Fast polygonal integration and its application in extending haar-like features to improve object detection. In *2010 IEEE computer society conference on computer vision and pattern recognition* (pp. 942-949). IEEE.

[25] Zhu, Q., Yeh, M. C., Cheng, K. T., & Avidan, S. (2006, June). Fast human detection using a cascade of histograms of oriented gradients. In *2006 IEEE computer society conference on computer vision and pattern recognition (CVPR'06)* (Vol. 2, pp. 1491-1498). IEEE.

[26] Mathias, M., Benenson, R., Pedersoli, M., & Van Gool, L. (2014). Face detection without bells and whistles. In *Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part IV 13* (pp. 720-735). Springer International Publishing.

[27] Yan, J., Lei, Z., Wen, L., & Li, S. Z. (2014). The fastest deformable part model for object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 2497-2504).

[28] Zhu, X., & Ramanan, D. (2012, June). Face detection, pose estimation, and landmark localization in the wild. In *2012 IEEE conference on computer vision and pattern recognition* (pp. 2879-2886). IEEE.

[29] Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). Biometric systems: Technology, design and performance evaluation. Springer Science & Business Media.

[30] https://endurid.com/products/corrections/software-corrections/

[31] Carter, A. (2018). Facing Reality: Benefits and Challenges of Facial Recognition Technology for the NYPD. Homeland Security Affairs.

[32] Crumpler, W., & Lewis, J. A. (2021). How Does Facial Recognition Work?.

[33] Wang, J., & Tan, T. (2000). A new face detection method based on shape information. Pattern Recognition Letters, 21(6-7), 463-471.

[34] Paul, L. C., & Al Sumam, A. (2012). Face recognition using principal component analysis method. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(9), 135-139.