Application of Blockchain to Increase the Reliability of the Personal Identity in Sri Lanka

Roche M.P.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Amarasinghe M. A. W. D.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Mahawatta A.I.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Vishan Jayasinghearachchci
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Jayasinghe L.V.S.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Abstract:- Exploit of one’s identity is a major threat the world faces, especially in Sri Lanka, where countless fake documents are forged which is very identical to the legitimate documents issued by the government authorities to recognize every individual. Per literature, the existing system is such that the documents are stored within a database hosted by the government, but there is no direct way of comparing every document presented by the person to validate the legitimacy of the documents, which gives the requirement for blockchain such that every issued document can be hashed and stored, allowing to spot fake or unauthorized documents by rehashing and checking against the existing hash stored in the blockchain, as foreign blockchain solutions are not economically feasible in Sri Lanka, a blockchain needs to be developed locally with multi-threaded asynchronous support for faster transaction processing, and non-blocking communication between blockchain nodes. In Sri Lanka, automated criminal detection is not much popular and authorities' procedures for identifying offenders are time-consuming. Using an automated approach to identify a wanted individual might be preferable to present practices. Current processes and techniques, such as acquiring records from eyewitnesses, are untrustworthy. Analyzing people's faces, behaviors, and threatening voices in CCTV camera footage is time-consuming. The proposed system can be able to register civilians, detect unusual behaviors, such as fights and criminals waving dangerous weapons in public, criminal face identification, which has the power of recognizing criminal faces at various stages of age, and recognition of the situation depending on the voice tracks extracted by CCTV footage. It summarizes whether the situation is threatening or not. In this research, we have proposed a desktop application for criminal identification with a higher accuracy level.

Keywords:- *Hash, Blockchain, Unusual Behavior, Face Recognition, Criminal Identification.*

I. INTRODUCTION

As for obtaining the National Identity Card, one must fill in the form which can be requested from the authorized officer of the applicant’s residential area, from the estate superintendent, or School Principal in the case of school applications or events, with the necessary data such as the family name, gender, civil status, profession, place of birth, district of birth, country of birth, address of the birth location, etc. [2], the birth certificate is compulsory for applicants under the age of 50, else if the applicant is over the age of 50 years without a birth certificate, then their school leaving or baptism certificate, for example, can be presented [3].

The information recorded for issuing the government-certified birth certificates and National Identity Cards is stored within a database hosted by the government, since the data is kept in a single database, there is no guarantee of data recovery or unauthorized modifications, this is where the blockchain is required, it is a ledger which is distributed and decentralized, it prevents tampering the data and allows only to add in new data, at the same time there is traceability of transaction, assume to store new data a transaction is triggered which contains the new data within it. [4]

As per the literature, there is no blockchain which is hosted in Sri Lanka, foreign blockchains rank in Ethereum, Bitcoin, and multiple other, there is a known provider in Sri Lanka known as Niftron, an organization which provides blockchain as a service, however it also relies on foreign blockchains such as the Ethereum Ropsten test net and Stellar test net [5], the test net terminology means it is only for testing blockchain applications before deploying to the main blockchain network (Mainnet), blockchain such as Ethereum, Bitcoin has its limitations when considering to save custom data in contrast to a cryptocurrency transaction, while Ethereum supports smart contracts for user defined data storage, the average transaction rate is only 14 Transactions Per Second (TPS), hence having to wait in a queue until the transaction is processed, moving onto Bitcoin, it supports up to a maximum of 80 Bytes to be stored as custom even though not officially supported, and it’s TPS is 5, much lower than Ethereum, another blockchain named Solana supports both smart contracts and has a known TPS of 3000 which may scale with nodes, however Solana scales horizontally and not vertically.

When registering a NIC of a person, the image and the information of the person are stored in the database as the first step. As the next step, the data is hashed to increase the security of information. As the next step, the hashed information is sent to the high-performance blockchain. Finally, the information that is stored in the blockchain is used to identify criminals.

Over the years, public safety has been a major concern for the entire world. The impact of criminal activity and terrorist attacks on public security has grown significantly. Detecting these criminal incidents as soon as possible will limit death and property loss [5]. Surveillance cameras may be found in practically every aspect of our life. This abundance demands automatic analysis since monitoring such a large volume of data is beyond the capabilities of humans. Automatic analysis is especially helpful in situations that necessitate an immediate response. The occurrences are traffic accidents, fires, explosions, shootings, fights, etc. [6] An unusual behavior detection system is a proven way to detect these criminal actions in public. Unusual behavior detection with an alarm system is done generally in 3 stages. The initial step was to identify all the people in the footage, followed by identifying suspects carrying weapons and detecting any other unusual behaviors. When unusual behavior is detected in the camera frames, an alarm is activated, alerting the user to the suspected activities.

Face recognition is proven as an efficient and practical identification and verification method. It has been engaged in different applications, including security systems, card verification, video surveillance, criminal identification [7], person identification, biometric authentication, passport renewal, and law enforcement. Normally, face recognition systems contain 3 steps. The facial image is identified initially in face recognition. The picture is then processed to extract relevant characteristics. Finally, using a similarity measure, the retrieved characteristics are compared to those in the database. The accuracy of face recognition algorithms is directly proportional to the facial image provided. Age, position, light, partial occlusion, and facial emotions, for example, all impact the accuracy of face recognition techniques. Between those variables, aging causes changes in crucial facial image aspects such as texture and shape. This paper aimed to implement a system that can identify potential criminals by image comparison against the suspect’s image by using the NIC database with an age-invariant face recognition methodology.

In many systems nowadays, voice recognition is employed. It refers to a computer program's or machine's capacity to hear, comprehend, and execute spoken orders. With the development of AI (Artificial Intelligence) and intelligent assistants like Amazon's Alexa, Apple's Siri, and Microsoft's Cortana, voice recognition has grown in popularity and applications. For the system that we are building voice recognition is used to identify whether a criminal is going on. In this system, we are trying to prove with the voice and the text obtained by the voice that there is something criminally going on. It is identified by not only the words but from a separate sentence that is extracted by the voice clips. Proceeding with the implementations using voice recognition we are going to use natural language processing for this system [5]. For creating a more effective system final output will provide a text as well as a voice clip extracted from voices. This lack of excitement seems to be caused by the constraints of the system, including the high demand for computer resources, the severe fluctuation in recognition accuracy, the constrained recognition vocabulary, the requirement for speaker training, and the currently exorbitant cost.

Making computers comprehend sentences or words written in human languages is the goal of the branch of artificial intelligence and linguistics known as natural language processing (NLP). To make the user's job easier and fulfill their desire to speak to the computer in natural language, natural language processing was created. Since not all users will be fluent in the machine-specific language, NLP helps users who lack the time to acquire new languages or polish their existing ones [6],[7]. The finally implemented system can check whether a certain situation is violent or not. By uploading the necessary soundtracks extracted from the CCTV footage, our system will provide the final call on the type of situation in the footage.

II. LITERATURE REVIEW

In [8], the authors proposed a platform solution named Casper which is a blockchain and self-sovereign-based digital identity management system, in which the identities of people can be stored, the blockchain has multiple nodes that act as endpoints for data storage for availability, also provides the ability for smart contracts which allows running programs on top of the blockchain in a decentralized manner, with support on mobile devices as well as computers, this software is using the microservice architecture to have the proper breakdown between the blockchain and the system in hopes on horizontal scalability, however, the blockchain itself is single chained, so to increase the transaction throughput the total number of nodes in the network should increase, meaning more people or more equipment to host the nodes are needed to ensure the quality of data.

Moving on to blockchains, in [18] the authors propose a lock-free Hash Mark Set (HMS) in contrast to the redundant sequential algorithms used for HMS, this is done by only parsing the new transactions while preventing from re-parsing the already mined transactions as the study was carried in Ethereum and Bitcoin in mind, the results increase the transaction throughput by 6 to 10 times compared to current 14 Transactions per second (TPS) rate.

Global-wise, there are multiple blockchains such as Ethereum which has a transaction throughput of 14 TPS, which increases due to the Proof of Work complexity during mining, then Bitcoin which also has a lower transaction throughput, although Ethereum has smart contracts – which is a mechanism to run custom programs on top of the blockchain which can be used to modify the way the data is to be stored, this is however not available in Bitcoin, Solana, on the other hand, has support for smart contracts and can do up to a recorded level of 1000 Transactions per second, even though most blockchains are single-threaded, Solana is said to be multithreaded, even in such case, the blockchain itself is single chained, as the blocks of transactions can only be saved sequentially.

The initial studies in the field of unusual behavior detection are focused on different areas. One research suggests the use of label distribution to identify abnormal crowd behaviors such as stampedes, fighting, panic, and tumbling [9]. A new automated technique for detecting abnormal behavior in Dynamic Crowded Gatherings (DADCG) is provided in this study [10]. Some studies suggest a way to detect weapons using Harris, SIFT (Scale Invariant Feature Transform), and RIFT detectors but there are some drawbacks to those suggested techniques. Another study proposes a method for detecting unusual crowd behavior that is unsupervised. They have applied an approximate median filter to reduce the rate of fault [5]. Those methods cannot identify multiple weapons in one frame. According to some other studies, the YoloV4 approach is speedier and more appropriate in detecting weapons when compared to previous versions. They do, however, have some limitations. These systems are inaccurate since they react to work on solely detecting weapons, and they cannot identify some anomalous behaviors like a fight among numerous people. As some other research suggests, they have used novel motion features to identify abnormal behaviors in people. Our research provides a novel approach to the challenge of identifying unusual actions that are accompanied by weapons and without weapons as well.

In face detection and face recognition, previously some researchers [7] used CCTV (Closed Circuit Television) footage to identify potential faces. According to their research, they have proposed a criminal identification system that has the novelty of face detection by using Face Encodings. In [11], the authors used LBPH (Local Binary Patterns Histogram) for image recognition and face identification in a specific security camera. They present accurate results for occlusion, position variation, and lighting after obtaining satisfactory results from many experimental analyses of this approach. As a result, the suggested system enables face identification and recognition in a controlled environment.

There is some research on facial recognition that considers age development. This research can be divided into age estimation methodologies, aging simulation approaches, and age-invariant face recognition methods. According to research [12], researchers proposed a new QSVM-PCA technique that compresses a massive high-dimensional dataset by decreasing PCA-dependent dimensionality. They obtained 98.87% accuracy for 240 FGNET images. In research [13], researchers have proposed a novel approach called the "Local Adjacent Difference Pattern" which is more robust toward the age variation process. Authors in [14], introduced an enhanced component-based age-invariant face recognition system which gave 98.31% accuracy on the FGNET database. In the research paper [15], the authors proposed a framework for multi-task learning, called MTLFace, to simultaneously accomplish age-invariant face recognition and face age synthesis. In research [16], researchers investigated how the aging process affects facial recognition systems. Furthermore, researchers [17], introduced a unique Age-Invariant Model (AIM) for combined disentangled representation learning and photorealistic cross-age face synthesis.

According to [18], this voice recognition is done in the Tamil language, and it offers feature extraction, an acoustic model, a pronunciation dictionary, and a language model built using HMM, producing 88% accuracy in 2500 words in our system it focuses on the Sinhala language, and it also provides a text along with a voice clip. For this, we are using Natural Language Processing (NLP) mainly. Using this model is the most efficient way to implement this.

III. RESEARCH OBJECTIVES

The objective of the blockchain is to study existing blockchains, then develop a much higher performance blockchain with the least chance of transaction rejection and should be able to scale vertically. It can be used to validate the legitimacy of the documents, such that every issued document can be hashed and stored, allowing to spot of fake or unauthorized documents by rehashing and checking against the existing hash stored in the blockchain

Unusual Behavior detection system which can detect people with threatening weapons. This system is also capable of detecting unusual behaviors like fighting. We focused on two goals in particular: automatic detection of people threatened with weapons and identification of harmful public activities like fighting which happens between two or groups in public places. In addition to this, the system can detect unusual crowds.

The objective of face detection and face recognition is to implement software with an identity management system that can identify potential criminals by image comparison against the suspect's image. We concentrated and focused on efficiently capturing the suspect's face from CCTV footage and comparing it to the NIC database of civilian images using the age-invariant face detection and face recognition method, which improves the capabilities of the face detecting and recognition process.

In the proposed system, another objective is identifying the threatening voice of people that can be a sign of a dangerous situation. Final implementations provide the result of whether the situation going on is critical or not by considering the voice clips that are extra to CCTV. To proceed with the result, the system will run a checkup to clarify whether the voice(sound) is aggressive or not.

IV. METHODOLOGY

➢ *High-Level Architecture*

The main focus of the overall research is to develop a desktop application that can accurately and easily identify potential criminals and criminal activities. To achieve the desired outcome, the main tasks will be carried out as age-invariant face recognition, unusual behavior detection, and threatening voice recognition from the CCTV footage, respectively, as shown in Fig. *IV-1*. With the help of the proposed system, which enables authorities to register civilians to the system, we anticipate identifying and detecting any person who is attempting to commit a crime or cause harm to people in public. The suggested system provides a great opportunity for Sri Lanka's public security sector to reduce and eventually end criminal activities.

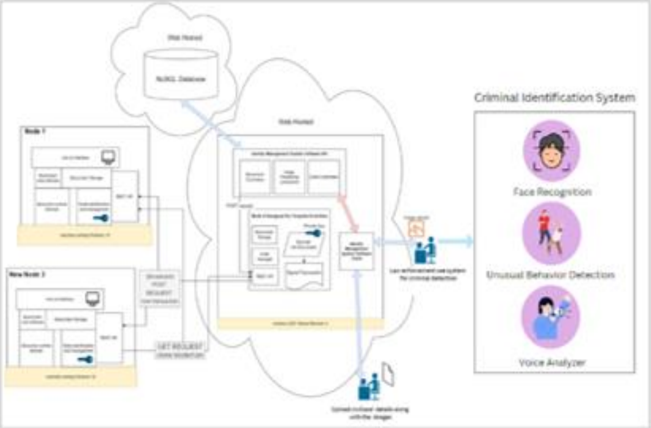


Figure IV-1 High-level architecture diagram

Vertically Scalable Blockchain

To develop the higher performance blockchain, the factors affecting the transaction need to be identified, these are the hashing algorithm used to perform the Merkle Root hash operation to verify the blockchain is not modified, then the encryption function used to add the digital signature of the sender, how the transactions are handled at the node, in this case, the proposed solution is to use parallel processing on which each processor core will be consuming a transaction from the queue of transactions per second, to achieve this the blockchain will perform branching, instead of a single chain of blocks, there will be multiple which then will be linked to a block of the main branch, named as the root branch.

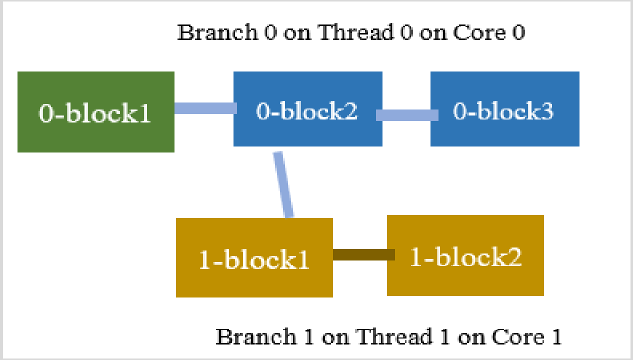

Branch 0 on Thread 0 on Core 0
0-block1
0-block2
0-block3
1-block1
1-block2
Branch 1 on Thread 1 on Core 1

Figure IV-2 Blockchain Structure

By default the node will contain a value for the maximum transaction limit per second for each thread, assume 1000 acceptable transactions per second from thread 1, then when the incoming transactions increase beyond that limit, which is 1000 as an example, then the program with creating a new thread targeting a new core, the branching will occur until the incoming transactions either stay at a level assume 10000, for an 8 core processor, the threading will split until 6, leaving 2 threads for background tasks such as validations and storage, to prevent blocking other tasks.

➢ *Technologies*

The node is written using C-sharp (C#), on Active Server Pages (ASP) and .NET framework with versioning 6.0, the user interface is written using JavaScript which uses the Transmission Control Protocol (TCP) layer to open a WebSocket to communicate with the Node.

➢ *Backend Architecture*

The backend uses a mediator pattern to intercept the RESTful calls containing transactions, to validate the sender using the digital signature, and an observer pattern to invoke each thread based on each specified time delay if the thread sleeps after processing the provided transactions.

➢ *Variables*

- Maximum acceptable transactions per second for each thread
- Thread invokes delay in milliseconds
- Branching Rate

➢ *Unusual Behavior Detection*

To develop the unusual behavior detection system, three stages were used which help to identify suspicious activity in CCTV footage. The first step was to identify all humans in the video, the second was to identify suspects carrying weapons and detection of any other unusual behaviors. One unusual behavior is successfully identified in the video frames, a burglar alarm is triggered, alerting about the suspicious activity.

After detecting persons in the CCTV footage provided as input, the unusual behavior analysis is performed. At this stage, the system will begin identifying suspicious behaviors such as looking for persons with weapons, and unusual actions such as fighting. When the system detects unusual behavior, an alarm is triggered in the final stage. A dataset that includes 6000 images was used to train the model which is required for fight detection and another dataset that contains 10000 images was used to train the model for the weapon-based unusual behavior detection system. The system can identify many weapons including shotguns, machine guns, etc., which is a greater improvement when compared to existing systems. Yolov4 has a higher accuracy of over 95% when identifying people with waving weapons.

- *Age-invariant Face Recognition*

Face recognition techniques and Python were the primary sources in developing the age-invariant face recognition system. There are three main steps in the system. First, we need to upload the images of the civilians along with their details to the system as the NIC registration process. As the second step, we used OpenCV, which has a Haar cascade classifier for face detection. It first reads the detected picture and transforms it to grayscale, then loads the Haar cascade classifier to determine if it includes an individual face. If this is the case, it will analyze the face characteristics and create a rectangle frame around the recognized face. The final step is to identify faces along with their details. The world's most simple face recognition is used in this system. It is created by using the extremely powerful facial identification technology that dlib has to offer. The model has a 99.38% accuracy on the Labeled Faces in the Wild benchmark. The system can upload CCTV footage and identify potential faces by comparing faces in the NIC database. For user interface development we used the Python Tkinter GUI library.

- *Voice Recognition*

To develop the voice recognition system, over 1500 different types of voice clips were used. This dataset contains various types of voices, soundtracks, and noises. A model is trained using the dataset. Python, firebase, and sound processing were used as technologies. Recordings can be made by using CCTV and extracting voice clips of the relevant situation. After that, they are uploaded to the implemented system. From there, the algorithm used to build the system is sent through and the corresponding voice recording is inserted. From there, it checks whether the uploaded report reflects a risk situation or not and provides the relevant output to the user.

After that, when looking for the occasion of this relevant recording, it is analyzed what the voices in it say. Relevant extracted voice clips will be added to the system, and it will detect whether the voice is threatening or not. After that, the alarm is triggered by the system.

V. RESULTS AND DISCUSSION

The proposed system helped to improve the efficiency and accuracy of the criminal investigation process, as illustrated in Fig. *V-1* By giving the authorities a more trustworthy and accurate final output, the combination of face recognition, abnormal behavior detection, and threatening voice recognition functions served to improve the detection and recognition method.

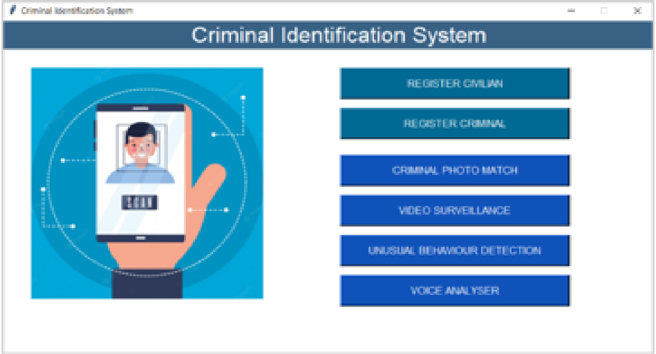


Figure V-1 Main interface of the proposed system

Higher authorities can register civilians with their NIC through the civilian registration process. Following registration, the system enters all civilians' information into a database. The system generates a special folder containing each civilian's NIC number during the registration procedure. Images that have been inserted will go through a face detection method, which will keep the images of the faces in a special folder with the name of the person. If a crime is committed, this approach enables higher authorities to keep track of the information on the public and use it to identify the criminals.

- *Testing the Blockchain*

The blockchain was tested on three different environments, to recommend the optimum values for each type of processor, ranging from AMD and Intel branding, environment 01 contains an AMD processor running at 4.0 Giga Hertz (GHz), with a total of 8 cores and 16 threads, all cores run on specified speed, with 16 Giga Bytes (GB) of Ram Access Memory (RAM), the storage is a Solid State Drive SSD) in comparison with the Hard Disk Drive (HDD) used in Environment 03, all devices are running under Microsoft windows variants.

Table V.1 Blockchain testing environments

	Environment 01	**Environment 02**	**Environment 03**
CPU	AMD Ryzen 7 3700X	Intel i7 1165G7	Intel i3 4th gen
Speed	All cores @ 4.0 GHz	Single core @ 3.0 GHz, rest @ 2.4 GHz	Single core @ 3.0 GHz, rest @ 1.8 GHz
Ram	16 GB	16 GB	4 GB
Storage	SSD	SSD	HDD
OS	Windows 10	Windows 11	Windows Server 2012 r2
Core Limit	Use all	Use all	Use all

- *Testing the unusual behavior detection system*

The suggested system's component for detecting abnormal behavior may identify suspects who are actively involved as well as specifics of the abnormal activity inserted in CCTV streams in extremely crowded and densely populated areas Since datasets based on only weapons were used to train these models, it is difficult to distinguish an unusual behavior like a fight because previous research has mostly concentrated on detecting abnormal behaviors of people with weapons. In this system, it can identify unusual behaviors such as fights because datasets containing these unusual behaviors have been used to train the model. It has an accuracy of 90% when detecting fights from CCTV footage. Limiting false positives and providing detection are other important considerations for identifying unusual behavior in CCTV footage, including threatening weapons.

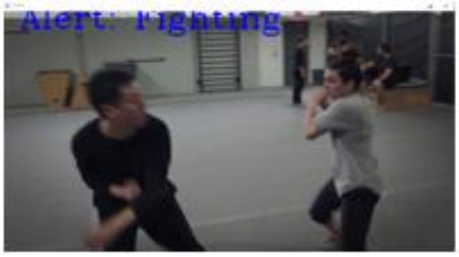


Figure V-2 Fighting scenario

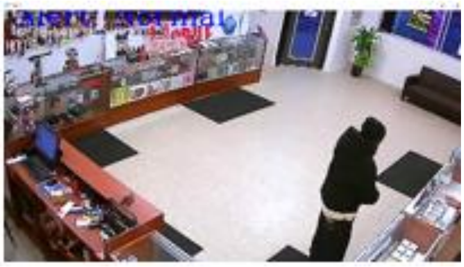


Figure V-3 Normal scenario

- *Testing the age-invariant face recognition system*

The suggested system can be able to detect and recognize criminals' faces with different stages of age by comparing uploaded faces with the existing faces in the system. With a higher level of accuracy and a constrained amount of time, the face of a criminal has been effectively recognized throughout the facial recognition process. Real-time face detection and recognition of offenders is possible in video streams received from cameras. For face detection, the OpenCV technique and cascade classifiers based on Haar features were used. A cascade function is learned using several positive and negative pictures using machine learning. Additionally, by utilizing Local Binary Patterns Histograms, we have added facial recognition (LBPH). Additionally, we made advantage of the most straightforward facial recognition library known to man. On the labeled faces, the model achieves a 99.38% accuracy rate. The research will mark a significant turning point for surveillance systems and video-based age-invariant facial recognition. Figure *V-4* shows the folder structure of the registered civilians of a young age. and the figure *V-5* despite the output of the identified faces

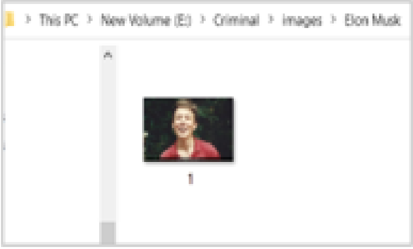


Figure V-4 Uploaded young image of the person

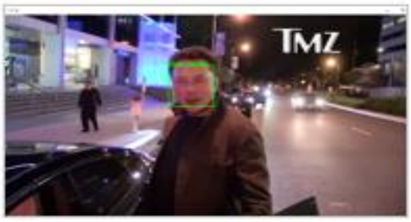


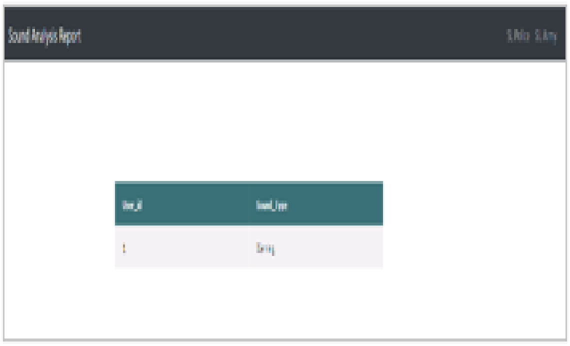
Figure V-5 The output of the identified faces

- *Testing the voice recognition system*

As discussed earlier, a total of 1640 voice clips were used to test the software model. They were uploaded to the system to analyze and identify the content of the audio clips and to point out any threatening voices if identified. The system software was made to achieve this by using two methods:

1. By analyzing the tone of the voice in the audio clips to identify threatening tones
2. By converting the audio to text and identifying threatening tones.

When using the first method, the software was able to identify almost all the voice clips' tones accurately. However, when using the second method, the software could not translate the words accurately in every instance. This resulted in some misunderstandings and inaccurate results. But still, it could identify most of the threats. Approximately 79% of the voice clips were successfully identified by this second method. So, overall, this software system has a success rate of about 79%. The researcher believes a variety of factors affected the outcome of the system, such as voice quality, internet connection strength, etc. Fig. *V-6* shows the output of the voice analyzer.


Sound Analysis Report

User_id	Sound_type
1	[illegible]

Figure V-6 Output of the voice analyzer

VI. CONCLUSION AND FUTURE WORK

Crime rates in Sri Lanka are rising steadily every day, and numerous occurrences are being reported to the police on a huge scale. Therefore, it is necessary to automate this process. As a result, this research develops a novel method for using CCTV footage in criminal identification. Additionally, this research will benefit society by enhancing security, law, and order for the advancement and safety of humanity, particularly in countries that have suffered significantly as a result of such terrible crimes. The system concentrates on the overall crime scene to identify unusual behaviors accompanied by threatening weapons, identify and recognize suspects using faces automatically with a high level of accuracy in a short amount of time, and identify threatening sounds from CCTV footage. We intend to advance this research in future work by improving the system's precision and effectiveness.

REFERENCES

[1]. Sri Lankan Registrar General's Department, "Registrar General's Department," [Online]. Available: https://www.rgd.gov.lk/web/index.php/en/services/civil-registration/birth-registration.html. [Accessed 23 01 2022].

[2]. Sri Lankan Department for Registration of Persons, "Department for Registration of Persons," [Online]. Available: https://www.drp.gov.lk/Download/Application%20DRP.pdf. [Accessed 23 01 2022].

[3]. Sri Lankan Government Information Centre, "Government Information Centre," [Online]. Available: https://gic.gov.lk/gic/index.php/en/component/info/?id=416&task=info. [Accessed 23 01 2022].

[4]. IBM Corp, "IBM," [Online]. Available: https://www.ibm.com/topics/what-is-blockchain. [Accessed 23 01 2022].

[5]. "An Unsupervised Abnormal Crowd Behavior," 2017 International Conference on Security, Pattern Analysis, 2017.

[6]. M. A. A. a. M. S. Ersin ESEN, "Fight Detection in Surveillance Videos," 2013 11TH INTERNATIONAL WORKSHOP ON CONTENT-BASED MULTIMEDIA INDEXING (CBMI, 2013.

[7]. Nagnath B. Aherwadi, Deep Chokshi, Sagar Pande, Aditya Khamparia, "Criminal Identification System using Facial Recognition," in International Conference on Innovative Computing & Communication (ICICC), 2021.

[8]. E. a. L. X. a. F. P. a. S. S. a. D. Z. K. Bandara, "A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform," in 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, 2021.

[9]. D. Z. L. Q. Y. S. Min Sun, "Crowd Abnormal Behavior Detection Based On Label Distribution Learning," 2015 8th International Conference on Intelligent Computation Technology and Automation, 2015.

[10]. D. o. A. b. i. Dynamic, "Detection of Abnormal behavior in Dynamic".

[11]. Farah Deeba, Aftab Ahmed, Fayaz Ali Dharejo, Hira Memon, Abdul Ghaffar, "LBPH-based Enhanced Real-Time Face Recognition," International Journal of Advanced Computer Science and Applications, 2019.

[12]. Ashutosh Dhamija, R. B. Dubey, "Analysis of Age Invariant Face Recognition using QSVM-PCA," 2020.

[13]. Rajesh Kumar Tripathi, Anand Singh Jalal, "A Local Descriptor for Age Invariant Face Recognition under Uncontrolled Environment," in Second International Conference on Secure Cyber Computing and Communication (ICSCCC), 2021.

[14]. Leila Boussaad, Aldjia Boucetta, "An effective component-based age-invariant face recognition using Discriminant Correlation Analysis," Journal of King Saud University - Computer and Information Sciences, 2022.

[15]. Zhizhong Huang, Junping Zhang, Hongming Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework," 2021.

[16]. Le¨ıla Boussaad, Aldjia Boucetta, "The aging effects on face recognition algorithms: the accuracy according to age groups and age gaps," in International Conference on Artificial Intelligence for Cyber Security Systems and Privacy, 2021.

[17]. Jian Zhao, Shuicheng Yan, Jiashi Feng, "Towards Age-Invariant Face Recognition," 2022.

[18]. Z. a. G. P. K. a. C. V. a. D. D. Painter, "Parallel Hash-Mark-Set on the Ethereum Blockchain," in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, 2020.

[19]. M. M. N. D. o. C. S. a. E. S. '. A. (. t. b. U. B. O. I. Santosh Kumar Behera, NATURAL LANGUAGE PROCESSING FOR TEXT AND SPEECH PROCESSING: A REVIEW PAPER, Odisha: IAEME Publication, 2020.

[20]. W. E. I. B. W. N. A. N. M. Isa, "Object Detection: Harmful Weapons Detection," 2021 IEEE Symposium on Wireless Technology & Applications, 2021.