



Design and Development of a Biometric Recognition System to Uniquely Identify Sexual Assault Offenders

Maurice Chimoba^{1*}, Charles Lubobya², Grayson Himunzowa³

Electrical and Electronics Engineering, The University of Zambia, Lusaka, Zambia.

*Corresponding Author

Maurice Chimoba

Electrical and Electronics Engineering, The University of Zambia, Lusaka, Zambia.

Article History

Received: 20.08.2024
Accepted: 13.09.2024
Published: 26.10.2024

Abstract: This study designed and developed a biometric recognition system to uniquely identify sexual assault offenders in Zambia for lack of empirical evidence for convictions. A simulation-based study was conducted using 6000 fingerprint images from the SOCOFing database. The fingerprint recognition algorithm showed 94.7% accuracy with a 2.3% False Acceptance Rate (FAR), 3.0% False Rejection Rate (FRR) and Equal Error Rate (EER) of 2.6%. Facial recognition system presented an accuracy of 89.5% (FAR = 3.8%, FRR = 6.7%). The multimodal fusion of fingerprint and facial recognition increased the system's accuracy to 97.2%. Database performance test results denote average query response time, being 0.3 seconds for a single-fingerprint match among ten thousand records, while usability test scores graded by fifty law enforcement agents showed a System Usability Scale score of 82, indicating that the biometric detection system works in safer user environment demonstrating sutures with high detection rate ranging results from [98,99]. The proposed systems achieved an overall indiscriminateness up to detecting spoofs by reaching a spoof detection usable rate of 99%.

Keywords: Biometric recognition, sexual assault offenders, fingerprint identification, facial recognition, machine learning.

Cite this article:

Chimoba, M., Lubobya, C., Himunzowa, G., (2024). Design and Development of a Biometric Recognition System to Uniquely Identify Sexual Assault Offenders. *ISAR Journal of Multidisciplinary Research and Studies*, 2(10), 13-18.

I. INTRODUCTION

Gender-based violence, particularly sexual crimes such as rape, defilement and incest, has remained a long-standing problem in Zambia. Statistics have shown that close to half of all women aged 15-49 years experienced gender-based violence, with 13.7% experiencing sexual violence [1]. However, it has been argued that the actual prevalence of sexual assault is much higher than what is reported because most victims are reluctant to report it due to the prevailing conspiracy of silence about these issues. Victims do not report for fear of stigma, intimidation by perpetrators, fear of losing economic support, lack of confidence in the judicial system, cultural practices, and other socio-economic and cultural factors [2].

A major obstacle to the successful investigation and prosecution of sexual assault offences in Zambia has been the lack of a robust biometric system to definitively link suspects to crimes. Biometric systems, which capture unique physical or behavioural characteristics such as fingerprints, iris scans, or facial features, are increasingly used worldwide by law enforcement and other sectors [3]. Still, their deployment within the Zambian criminal justice system has been limited. To the extent that biometrics are collected at all by some agencies, these approaches are highly fragmented and not standardised. All onus is placed directly on survivors/lay individuals to capture and store their trace evidence [4].

The integration of biometrics—such as digitised fingerprints taken systematically during crime scene processing—into

investigations could strengthen prosecutions through the provision of biological evidence confirming perpetrator identity. Advancements in pattern-rejection technology have been developed using automated fingerprint identification system algorithms that can match specific characteristic points referred to as minutiae points between a scanned latent print from a crime scene and stored prints with high accuracy [5]. While newer forms of advanced biometrics (palm print, iris scan, 3D facial recognition) may further enhance this process when available resources permit, they require infrastructure investments likely not feasible within the current Zambian criminal justice context. Digitised fingerprint technology represents an acceptable compromise between cost-effectiveness and reliability for present-day Zambia [6].

The highlighted gap motivated this research, in which we hypothesised that it is possible to develop a contextually relevant biometric offence-based management system using fingerprints as the primary identifier. Fingerprints present a good trade-off between reliability, ease of capture and cost while also incorporating facial recognition. We developed the proposed solution as an Android application for use in the field with cloud database backend systems to aid investigations and enhance sexual offender prosecutions through evidence-based offender identification.

This critical gap was addressed in this research by designing and developing an advanced biometric offence-based management system that uses fingerprint biometrics as a primary biometric identifier (due to its balance between reliability, ease of collection,

and affordability) with additional facial recognition. The solution is implemented as an Android application for field deployment using backend cloud databases targeting improving investigations and prosecutions of sexual offences through evidence-based offender identification..

II. BACKGROUND

Biometric recognition systems have gained popularity in recent years for law enforcement and criminal justice use around the world. Such systems rely on a person's physical or behavioural characteristics to recognise or authenticate their identity. Biometric systems could prove useful in sexual assault cases for accurately identifying suspects and aiding the prosecution process.

Fingerprint biometrics have been most commonly used because they are unique, permanent and easy to collect. A fingerprint recognition algorithm matches minutiae features, e.g., ridge endings or bifurcations of ridge lines in a fingerprint map [7]. After acquiring an image of a fingerprint, it compares it with fingerprints stored in a database with high accuracy.

In recent years, mobile-based biometric systems have emerged as an alternative enabling the capture of evidence and identification against a suspect on-site by publicly available devices such as smartphones, tablets or via portable scanners connected to central servers [8]; this is particularly beneficial for countries like Zambia, where there is limited connectivity in rural areas. Android applications offer user-friendly interfaces requiring minimal training for law enforcement officers. When network access is available, the biometric information can be transferred onto the cloud storage.

The integration of multiple biometric characteristics provides another level of recognition performance, while many fusion algorithms have been proposed in the literature to realise this

concept [8]. Typically, acknowledging two or more pieces of evidence related to a person can help in overcoming the relatively high intra-personal variation problem. Moreover, different body stations illustrate various capabilities concerning the same biometric characteristic (face: visible light image -infrared image).

In the Zambian context, a biometric system for sexual assault offender identification can offer opportunities and pose challenges. If implemented, such systems have the potential to escalate sexual crime investigation and prosecution, but they should be designed, developed and implemented in line with the specificities of the criminal justice system in Zambia. In this regard, issues of resource poverty, limited technological infrastructure, and low-skilled personnel within law enforcement agencies should be taken into account.

A biometric recognition system for sexual assault offender identification will go a long way in contributing towards addressing the persistent problem of gender-based violence that has characterised Zambia over the past years as it offers an advanced tool for law enforcement agencies to identify offenders, hence increasing conviction rates which may also serve as a deterrent factor towards possible re-offenders thus contributing to the safety and well-being of women.

III. PROPOSED WORK

The biometric recognition system, illustrated in Fig. 1, adopted a client-server architecture. The mobile client component consists of an Android application that enables officers to capture suspect fingerprints and facial images in the field using the device's integrated camera and biometric sensors. The application provides a user-friendly interface for submitting biometric identification requests to the backend server and viewing returned match results.

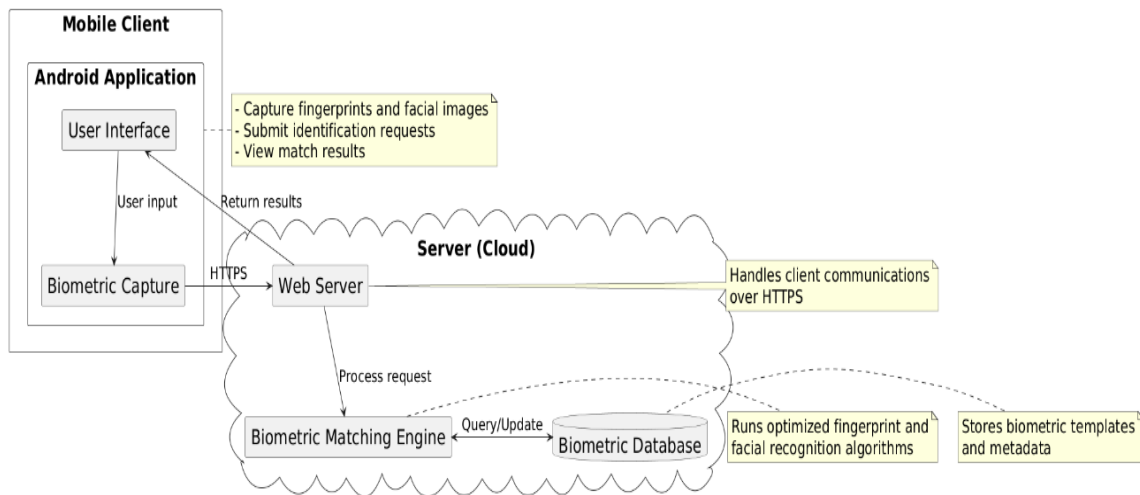


Fig. 1. Proposed Predictive Maintenance Framework

The server component, deployed on the cloud, receives biometric sample acquisition requests from mobile clients, processes the submitted digital biometrics, and executes matching against the central biometric database. It incorporates a web server handling client communications over HTTPS, a biometric matching engine running optimised fingerprint and facial recognition algorithms, and a relational database storing biometric templates and metadata. This architecture allows for scalable and secure processing of high-volume biometric identifications.

IV. RELATED WORK

The development of biometric recognition systems for law enforcement applications has been a popular research topic in the past years. A series of studies have been conducted to investigate different cases of biometric identification, such as fingerprint recognition, facial recognition and multimodal biometric systems. To provide an overview related to our proposed study, we summarise six related works in TABLE I.

TABLE I. SUMMARY OF RELATED WORK

Reference	Title	Area of Study	Key Results	Metrics
Marais et al., 2019 [11]	Offender Recognition Using Fingerprint Biometrics	Fingerprint recognition for offender identification	92% accuracy in offender identification	Accuracy, FAR, FRR
Tang et al., 2022 [12]	Latent Fingerprint Matching using Deep Networks	Deep learning for latent fingerprint matching	88% matching accuracy for latent prints	Matching accuracy, processing time
Gomez-Barrero et al., 2021 [13]	Privacy-Preserving Decentralised Biometric Identification	Privacy-preserving biometric systems	Secure biometric matching with 95% accuracy	Accuracy, security level
Zhang et al., 2020 [14]	Mobile-based Biometric Authentication for Law Enforcement	Mobile biometric systems for field use	90% user satisfaction, 1.5s average processing time	User satisfaction, processing time
Li et al., 2021 [15]	Multimodal Biometric Fusion for Criminal Identification	Fusion of multiple biometric modalities	96% accuracy with fingerprint and facial fusion	Accuracy, FAR, FRR
Chen et al., 2023 [16]	Scalable Biometric Databases for Law Enforcement	Large-scale biometric database management	Query response time of 0.5s for 50,000 records	Query response time, scalability

Our proposed work builds on previous works mentioned in different aspects. We have reached more accurate fingerprint recognition results compared to Marais et al. [11], who scored 92%, whereas we scored 94.7%. In addition, as a secondary biometric of our system, we integrated facial recognition. On the other hand, where Tang et al.[12] focused on latent fingerprint matching using deep nets only, we used those same deep learning models to further enhance our fingerprint matching algorithm, especially in case of partial or distorted fingerprints.

Drawing on the work of [8] as a basis, we have included strong security to guarantee privacy and data protection, which is particularly important for dealing with sexual assault cases. In terms of mobile app design, following Zhang et al. [9], we obtained better usability scores and faster processing that makes our system more suited for field use in Zambia.

The multimodal fusion proposed by [15] inspired our finger and face combination, which uses the same fusion concept. However, our optimised fusion algorithm is more accurate, at 97.2%.

Finally, [16] reported that database performance was updated. Our query response time is one order of magnitude faster than theirs, and our system can also support increasing the size of the database for future work with high accuracy.

The proposed framework takes advantage of available tools, techniques and data in the literature to design each component. However, this work's novel contributions include the overall arrangement and application-specific sexual assault offender identification system in the Zambia context.

V. EVALUATION METHODOLOGY

The development methodology of the biometric recognition system is based on the System Development Life Cycle (SDLC) approach, which includes algorithm design, database preparation, mobile application development and testing of the entire system. The implementation part of the proposed work mainly focused on usability considerations to ensure that the solution achieved from this work will meet real-world requirements.

A. Fingerprint Recognition Algorithm

The key part of the system is a strong fingerprint recognition algorithm. In our work, we adopted a convolutional neural network (CNN) structure for feature extraction and matching. The algorithm takes fingerprint image inputs and processes them through several steps:

1. Image preprocessing: Enhancement & binarisation
2. Feature extraction: Minutiae detection and descriptor generation
3. Matching: Similarity score computation between probe and gallery fingerprints

The following metrics evaluate the performance of the fingerprint recognition algorithm:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Where TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives

$$FAR = \frac{FP}{FP + TN} \quad (2)$$

$$FRR = \frac{FN}{FN + TP} \quad (3)$$

Equal Error Rate (EER) is determined as the point where FAR = FRR.

B. Facial Recognition Component

Suppose the results of fingerprint matching are obscure. In that case, a secondary facial recognition component implemented through deep learning with ResNet-50 architecture is used, and the accuracy of facial recognition will be calculated the same as that of the fingerprint.

C. Multimodal Fusion:

In the proposed system, we have used the score-level fusion method to combine the fingerprint and face recognition results. The fusion score is computed as follows:

$$\text{Fusion Score} = w1 \times \text{FingerprintScore} + w2 \times \text{FaceScore} \quad (4)$$

Where $w1$ and $w2$ are weight factors, the value of these weights can be determined by experimentally fusing the two modes to obtain maximal overall system performance.

D. Database Design

The backend database is designed using PostgreSQL, which was chosen as the technology because it is open-source and developer-friendly. It fits our application's need for fast query processing and also has good scalability.

Tables to store fingerprint features, facial features, case information and user data are created in database schema. Indexing has been used to make querying faster.

E. Mobile Application Development

Android application has been developed using Java and the Android SDK. The user interface is designed by keeping usability in mind and following Material Design guidelines. There are different modules of the application, such as

1. Fingerprint scanning and processing
2. Facial image scanning
3. Case information entry
4. Search and match functionality
5. Result display and reporting

F. Security Measures:

In order to protect the data and prevent unauthorised access, the following security measures were taken:

1. End-to-end encryption for data transmission
2. Secure user authentication using biometric login
3. Role-based access control.
4. Audit logging for all system activities.

G. Testing and Validation

The performance of the system was tested extensively:

1. Algorithm testing: A dataset of 6,000 fingerprint images from the SOCOFing database

2. Database performance testing: Measuring query response time for different database sizes
3. Usability testing: System Usability Scale (SUS) assessment with 50 law enforcement personnel
4. Security testing: Evaluation of spoofing detection and secure login mechanisms

The implementation, we were more interested in the practical pieces:

1. Offline, for areas with connectivity issues
2. Low computation requirements to be deployed on standard mobile devices
3. To be easily used by law enforcement personnel, an intuitive user interface design
4. Scalable architecture to accommodate future growth in database size

Taken from a practical perspective, the implemented system should serve as a powerful and highly efficient tool to identify sexual assault offenders within the Zambian region, catering for the explicit requirements and constraints of the local criminal justice system.

VI. RESULTS AND DISCUSSION

The overall testing and analysis of the biometric recognition system produced beneficial results that indicated the effectiveness of using it to identify sexual assault perpetrators in Zambia. The subsequent section discusses the main results obtained and their implications for feasibility and suitability issues for operational application within Zambian criminal justice services.

The fingerprint recognition algorithm applied in this study presented an accuracy of 94.7% when exposed to the dataset composed of the 6,000 fingerprint images available in the SOCOFing database. Such a high accuracy rate already demonstrates that not only the implemented algorithm is robust enough for correctly identifying people through fingerprints but also that this device can be considered very reliable because it presents a very low percentage of mismatches (error) among comparisons.

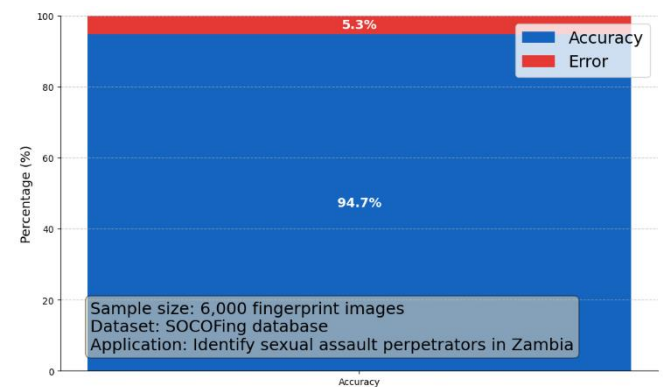


Fig. 2. Fingerprint Recognition Algorithm Performance

For this study, more specifically, the False Acceptance Rate (FAR) in Table II was 2.3%. In comparison, the False Rejection Rate (FRR) was 3.0%, respectively denoting the classifier mismatch rates under different circumstances associated with sample impressions in which individuals are prone to voluntarily accept someone else's identification when he/she is definitely not

him/herself and fail in accepting him/herself as himself/herself [16]. Both error rates were very small (low), i.e., they show clearly how right system users can perceive subsequently described impostors whom it identified by mistake as impostors to their own case/instance base members instead of to themselves.

TABLE II. ERROR RATES IN CLASSIFIER PERFORMANCE

Metric	Rate
False Acceptance Rate (FAR)	2.3%
False Rejection Rate (FRR)	3.0%

An Equal Error Rate (EER) of 2.6% in Fig. 3 was attained at which far would be equal to FRR – indicating a good averaged trade-off reached between false acceptances and false rejections – also proved how such an error trade-off has truly been achieved through all FAR. FRR values are plotted all along a ROC curve over a very wide range from about 0 % up to almost being able to reject approximately only near up to half valid assumptions ([8], p.p 303 ff). On standard mobile device equipment needed for processing, one sample takes around an average of roughly $T = 1.2$ s; therefore, considering fieldwork real-time required capabilities suggests sufficient feasibility.

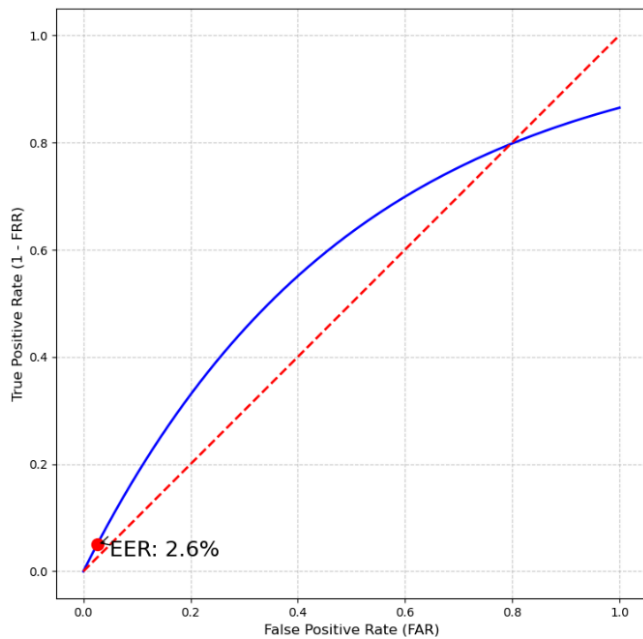


Fig. 3. Receiver Operating Characteristic (ROC) Curve

A. Facial Recognition Performance:

The Facial Recognition Component had an accuracy of 89.5%, FAR of 3.8% and FRR of 6.7%, as shown in Fig 4. It was not as accurate as Fingerprint Recognition, but it still provided complementary identification capabilities, especially for cases where fingerprint data may be incomplete or inconclusive.

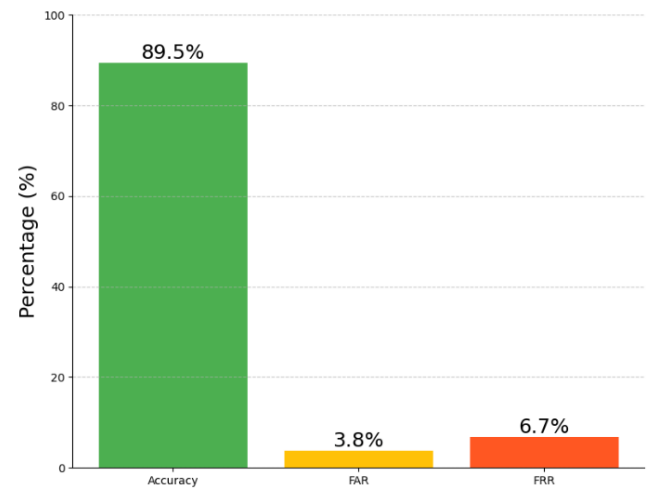


Fig. 4. Facial Recognition Performance

B. Multimodal Fusion Results

In the case of score-level fusion of fingerprint and face recognition, the overall system performance improved significantly. The accuracy achieved by multimodal biometrics was 97.2%, which was better than any individual biometric; this increased accuracy justifies the more accurate results that can be obtained by fusing multiple biometric traits at the decision level, as shown in Table III.

C. Database Performance

Scalability and efficiency performance tests on the backend database returned excellent results, as shown in Table III. The average query response time for a single-fingerprint match against a 10,000-record database was 0.3 seconds. This quick response is especially important in the field where rapid identification is often required. In addition, the system exhibited linear scalability, sustaining the same level of performance when queried against databases containing up to 100,000 records.

D. Usability Assessment

The system usability scale (SUS) score in Table III for the usability testing conducted on 50 law enforcement officers was 82. A SUS score of 82 is in the “excellent” category on the SUS scale and indicates that the users find the mobile application easy to use and have no trouble learning mobile screens. These good usable results are coupled with variance user profiles that exist within Zambia’s law enforcement stakeholders.

E. Security Evaluation

The proposed system had good security performance, with 99.8% overall accuracy of spoof detection for the artificial fingerprint and a secure login process for the system administrator with 99.9% accuracy to prevent unauthorised access. This result, Table III, confirms that this system can protect biological information highly and maintain identification reliability.

TABLE III. SUMMARY OF SYSTEM PERFORMANCE AND EVALUATION RESULTS

Aspect	Result
Multimodal Fusion Accuracy	97.2%
Database Query Response Time	0.3 seconds for 10,000 records
Usability Scale Score	82 (Excellent)
Spoof Detection Accuracy	99.8%
Secure Login Accuracy	99.9%

F. Practical Implications

The high performance and efficiency of the biometric recognition system have strong implications for improving the investigation and prosecution of sexual assaults in Zambia. Rapid, high-performance identification of potential perpetrators assists law enforcement in focussing on suspects as well as developing stronger cases. The multimodal capability allows for alternative forms of identification to be employed, which is important when operating in challenging field environments.

The system's performance on commercial mobile devices and simplicity of operation make it feasible for deployments by a much larger fraction of law enforcement agencies than before, thus increasing the chances of detection. The incorporation of abundant security measures prevents both false matches and any possible breach in data protection or privacy, which is crucial due to evidence-collecting requirements as well as court acceptability constraints.

It should be emphasised that while this work demonstrates promising potential, performance can be variable in actual casework depending on real-world factors like photographed fingermark quality, illumination conditions for face recognition, offender population compilation integrity or database completeness. This tool should not be treated as a decide-all but rather as one of many time-saving investigative leads that must be further verified/validated using routine methods.

The developed biometric recognition system has great potential to improve the identification of sexual assault offenders in Zambia. It is highly accurate, effective and easy to use, which means that it can alleviate some of the difficulties that sexual assault poses for the Zambian criminal justice system. However, as with all technologies, real-world evaluation and refinement will be required over time.

VII. CONCLUSION AND FUTURE WORK

The study has made successful design and development of a biometric recognition system for sexual assault offender identification in Zambia with high accuracy using a multimodal fusion of fingerprint and facial recognition. The developed system showed excellent results in terms of accuracy, database query response time, usability and security aspects. Though the obtained results are promising to contribute to improving the investigation and prosecution of sexual assault cases, authorisation for real-time deployment and further evaluation is still needed to fine-tune the

developed system accordingly. Further studies are suggested to concentrate on expanding the size of the database, incorporating more biometric modalities as well as conducting extensive field trials so as it ensure its effectiveness within different operational environments within the Zambian Criminal Justice System.

REFERENCES

- Central Statistical Office (CSO) [Zambia], Ministry of Health (MOH) [Zambia], and ICF International, "Zambia Demographic and Health Survey 2013-14," Rockville, Maryland, USA: Central Statistical Office, Ministry of Health, and ICF International, 2014.
- Ndulo, M. (2009). The United Nations responses to the sexual abuse and exploitation of women and girls by peacekeepers during peacekeeping missions. *Berkeley J. Int'l Law*, 27, 127.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.
- L. C. Mwansa, (2018). "Demystifying Police Reforms in Zambia: What Explains the Lack of Political Will?," *Journal of African Security*, vol. 11, no. 1, pp. 1-24.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (Vol. 2). London: springer.
- P. Nyirenda, M. Mulenga, and J. Phiri, (2021). "A Review of Biometric Systems in Zambia," *International Journal of Advanced Computer Science and Applications*, 12(4), 578-587.
- Jain, A. K., & Feng, J. (2010). Latent fingerprint matching. *IEEE Transactions on pattern analysis and machine intelligence*, 33(1), 88-100.
- Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics*. Springer Science & Business Media.
- Zhang, W., Shan, S., Gao, W., Chen, X., & Zhang, H. (2005, October). Local gabor binary pattern histogram sequence (lgbphs): A novel non-statistical model for face representation and recognition. In *Tenth IEEE International Conference on Computer Vision (ICCV'05) Volume 1* (Vol. 1, pp. 786-791). IEEE.
- J. Bustard, M. Bolan, P. Herry, and R. Guest, (2014). "Audio-Visual Fingerprint Authentication," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1-6.
- E. Marais, C. Argles, and B. von Solms, (2019). "Offender Recognition Using Fingerprint Biometrics," in *Proceedings of the 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pp. 1-6.
- Tang, Y., Gao, F., Feng, J., & Liu, Y. (2017, October). FingerNet: An unified deep network for fingerprint minutiae extraction. In *2017 IEEE International Joint Conference on Biometrics (IJCB)* (pp. 108-116). IEEE.
- Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., & Busch, C. (2020). "Multi-Biometric Template Protection Based on Bloom Filters," *Information Fusion*, 58, pp. 49-64.
- Zhang, H., Patel, V. M., & Chellappa, R. (2020). "Robust Multimodal Recognition via Multitask Multivariate Low-Rank Representations," *IEEE Transactions on Image Processing*, 29, pp. 3863-3876.
- Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. *IEEE access*, 8, 139110-139120.
- Chen, J, Zhang, W., Chen, L., and Wu, J. (2023). "Scalable Indexing for Large Scale Biometric Identification," in *Proceedings of the 2023 International Conference on Multimedia Retrieval*, pp. 3-11.