A User-Centered Interface Enabling Secure Multimodal Biometric Search in Cross-Border Law Enforcement Operations

Kyriaki Miniadou[1], Eirini Kyriakou[1], Asterios Leonidis[1,2][0000−0002−6800−3895], Maria Korozi[1][0000−0001−6577−4339], and Constantine Stephanidis[1,2][0000−0003−3687−4220]

[1] Institute of Computer Science (ICS), Foundation for Research and Technology - Hellas (FORTH), Heraklion, Crete, Greece
[2] Computer Science Department, University of Crete, Heraklion, Crete, Greece
{kminiadou, kyriakou, leonidis, korozi, cs}@ics.forth.gr

Abstract. Suspect identification is a critical task for Law Enforcement Agencies (LEAs) and biometric data —being inherently unique to individuals— play a pivotal role. However, the usability and interpretability of biometric identification systems remain challenging, especially for officers with limited technical expertise. These challenges are amplified in cross-border scenarios involving multiple biometric modalities (e.g., face, fingerprint, and voice) from heterogeneous sources. This paper presents a user-centered interface designed to support multimodal biometric matching in such complex environments. The proposed User Interface extends a previously developed Large-Scale Biometric Indexer module, enabling efficient biometric comparisons across foreign collaborating LEAs. It supports incomplete input data, harmonises results from heterogeneous sources, and clearly distinguishes between local matches, which provide full identity details, and external matches, which initially provide only confidence scores due to jurisdictional constraints. This UI aims to bridge the gap between complex biometric processing and operational decision-making, ensuring that identification results are presented in an understandable and actionable manner for law enforcement personnel.

Keywords: User Interface · Biometrics · Multimodal Biometric Data · Deep Learning · Security · Cross-Border Collaboration

1 Introduction

The identification of individuals involved in criminal activities has long been a central objective of Law Enforcement Agencies (LEAs). Biometric evidence such as blood traces or fingerprints left at crime scenes along with other sources like CCTV footage and eyewitness accounts, has consistently played a pivotal role in criminal investigations. Over the years, the technology used to collect, process, and match such evidence to potential suspects has undergone significant advancements in both accuracy and reliability.

In recent years, Artificial Intelligence (AI) has emerged as a transformative force in this domain, enabling faster and more accurate biometric identification. AI-powered algorithms are continuously refined to cope with real-world variability and data imperfections. A prominent example can be drawn from the COVID-19 pandemic, which highlighted a critical limitation in facial recognition systems as widespread mask usage obscured key facial features, drastically reducing system performance. This real-world disruption prompted an influx of research aimed at enhancing recognition systems under such conditions [3], [4], [14].

However, accurate identification alone is insufficient if results are not presented in an understandable and actionable manner to Law Enforcement personnel, many of whom may lack technical expertise. In biometric identification systems, information is typically conveyed through a ranked list of potential suspects with associated confidence scores, allowing LEA to assess the biometric evidence collected from the scene.

This process becomes more complex when multiple biometric modalities are taken into consideration, since different modalities may yield conflicting top matches making unified ranking across modalities non-trivial. The inclusion of multiple biometric types is necessary since, in real-world scenarios, not all biometric modalities are always available. For instance, a suspect may leave no fingerprints at the scene, rendering fingerprint matching ineffective; however they may have been recorded on CCTV, enabling face or voice matching. This complexity is further heightened in cross-border investigations, where results must be aggregated from LEAs across different jurisdictions. In such cases, the User Interface must manage input of varying completeness and harmonise results from heterogeneous sources.

To address this challenges, a User Interface (UI) was developed to assist LEAs in interpreting biometric identification results. The UI was designed to clearly present facial, fingerprint, and voice similarity results from disparate sources in a unified view [5] facilitating informed operational decision-making.

This paper is structured as follows: In Section 2, prior works related to user interfaces of biometric frameworks are discussed. Section 3, describes the motivation behind our approach as well as the Large-Scale Biometric Indexer module this work extends, Section 4 offers a detailed description of the User Interface. Finally, we conclude this paper in Section 5.

2 Related Work

The effectiveness of a User Interface directly impacts user experience (UX) and usability, which is critical in law enforcement settings where information must be delivered rapidly and accurately to support timely decision-making.

To improve the management of crime records, an Automated Fingerprint Biometric System [1] was developed. This web-based solution enables authorised personnel to register new individuals, store fingerprint data, and manage case records efficiently. By leveraging biometric data, the system ensures pre-

cise identification and reduces the risk of errors or data loss inherent in manual paper-based processes.

In addition to fingerprint-based systems, [2] explored facial recognition as a complementary or standalone biometric tool for law enforcement. An integrated Facial Recognition System was designed for real-time identification from live camera feeds or uploaded images.

Expanding on this concept, the Mobile Automated Fingerprint Identification System (MAFIS) [11] was introduced as a mobile Android-based platform for on-field operatives. It enables initial fingerprint inquiries, system dashboard access, and crime scene data collection directly from mobile devices. The UI plays a central role by presenting match results and investigation relevant data with clarity.

The system was further extended into MABIS (Mobile Automated Biometric Identification System) [12], incorporating facial recognition alongside fingerprints for enhanced identification. A follow-up study [13] evaluated MABIS in the Philippines, reporting a high System Usability Scale (SUS) score of 87.475, indicating strong usability. The User Experience Questionnaire (UEQ) highlighted improvement areas such as dependability and stimulation. Recommendations include visual enhancements, innovative features, and iterative, user-driven development to ensure continuous improvement.

3 Large-Scale Biometric Indexer Module

The proposed User Interface, as mentioned above, builds upon the Large-Scale Biometric Indexer, originally developed by the authors to facilitate suspect identification, particularly in cross-border investigations. The Indexer enables efficient and effective comparisons of biometric data, with the primary objective of identifying individuals based on their unique biometric traits. Initially introduced in [10], the Indexer applied to facial images and was later extended in [9] to incorporate additional biometric modalities, including fingerprints and voice samples. Furthermore, the Indexer operates as a core component within a broader secure ecosystem —the Biometrics Data Space— introduced in [6]. This ecosystem leverages Data Spaces technology, advanced Privacy Enhancing Technologies (PETs), and blockchain to support secure and sovereign data exchange between LEAs.

The Large-Scale Biometric Indexer accepts as input any combination of biometric modalities for a given individual and performs matching against a database (referred to as the catalogue) of previously apprehended individuals —both from the initiating LEA and external partner LEAs. Law Enforcement Agents working on a case can upload data directly from the local storage on their operational devices. Once uploaded, the biometric samples are matched against local data and securely transmitted to external LEAs for additional matching. The underlying system architecture and technical specifications are detailed in prior work by the authors.

Matching results —both local and external— are aggregated and visualised through interactive charts that summarise key statistics. These results are organised per LEA and further broken down by biometric modality and their associated confidence scores, offering users a clear and interpretable output.

It is important to note that local matches provide full access to the biometric profiles and associated information of the identified individuals, including names, addresses, and criminal histories. This information is made available to the investigating agent, as it resides within the jurisdiction of the initiating LEA. In contrast, external matches ——those retrieved from databases managed by other LEAs—— only return similarity scores or confidence values. To access detailed personal or criminal information for external matches, a formal request must be submitted to the corresponding LEA. This restriction is in place to ensure compliance with data protection regulations and to prevent the irresponsible sharing of sensitive personal data across networks.

3.1 Motivational Scenario

To illustrate the practical significance of our research objectives as well as highlight the difference between local and external matches, two motivational scenarios are presented.

- **Local Case: Drug Store Burglary:**
  A burglary occurred at a drug store and investigators recovered a fingerprint from the cash register and obtained CCTV footage showing the suspect. Tom, the police officer leading the case, uploads both biometric samples into the Large-Scale Biometric Indexer. The system returns high confidence scores from the local catalogue. Tom reviews the results and confirms that the samples match those of a previously apprehended individual. Because the match is local, the full identity details are displayed -including the suspect's name, address, prior offenses, and risk assessment profile- enabling Tom to take immediate investigative action.
- **Cross-Border Case: Human Trafficking Investigation:**
  A human trafficking investigation uncovers a hideout. The only available biometric evidence contains a voice recording intercepted during a surveillance operation and a low-quality facial image extracted from a camera. Amanda, the officer in charge, uploads the biometric data into the Large-Scale Biometric Indexer. The system finds no high confidence matches locally. However, a strong match is returned from an external LEA. Because of privacy regulations, only the confidence scores, the originating agency and a pseudonymised ID are shown. Amanda initiates a formal request to the relevant LEA to obtain the suspect's identity and background for further legal processing.

3.2 Datasets

To evaluate the performance of the Large-Scale Biometric Indexer and support realistic testing scenarios, multiple biometric datasets were employed. These

datasets were selected to reflect the diversity and complexity of real-world data encountered in law enforcement operations and cover three primary biometric modalities: face, fingerprint, and voice. For facial images, the GANDiffFace dataset [8] was used, which provides high-quality synthetic faces for robust face recognition evaluation. Fingerprint data was sourced from the FVC2000 dataset [7], which contains a diverse collection of fingerprint samples from multiple participants under varying acquisition conditions. For voice samples, the VCTK Corpus developed by the Centre for Speech Technology (CSTR) [15] was utilized. This dataset includes recordings from English speakers with a wide range of regional accents, enabling the system to be tested under diverse audio input scenarios.

4 User Interface

The proposed User Interface was developed to bridge the gap between complex biometric processing and operational decision-making. It supports seamless interaction with the Large-Scale Biometric Indexer, enabling users to upload evidence, view similarity scores, and compare results across multiple biometric modalities and jurisdictions.

4.1 Initiation of Biometric Matching

To perform the biometric profile matching, three distinct biometric modalities are available, (a) Facial Images, (b) Fingerprints, and (c) Voice Samples. As illustrated in Fig. 1, the interface allows the user to upload biometric evidence by dragging and dropping files into dedicated drop boxes, each outlined with a dotted border and clearly labeled with the corresponding modality. Each box includes a visual or audio preview of the uploaded input, depending on the modality.

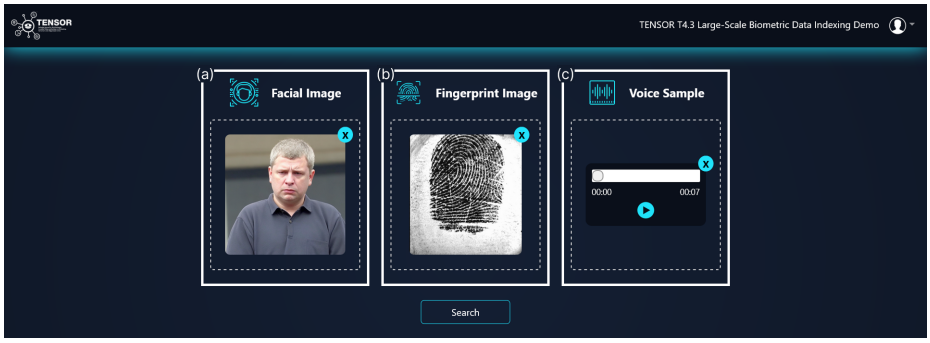

Fig. 1: Initiation of Biometric Matching

The user can choose a combination of query biometric data that pertain to the same individual. To account for real time conditions where not all biometric data can be made available each image is uploaded to a specific drop box and additionally a preview is available.

Each modality panel also includes a "X" button to remove or replace inputs, supporting error correction or changes in input before submission. This design accommodates real-world conditions, where not all biometric modalities may be available simultaneously.

Importantly, uploading biometric data does not automatically trigger a search. The user must explicitly initiate the matching process by clicking the central "Search" button, located beneath the modality panels. This deliberate action ensures that the user maintains control over the timing of the query submission.

4.2 Biometric Matching Results and Statistics

For each biometric matching request, the interface presents the detailed results among with an overview of relevant statistics, as depicted in Fig. 2.

Fig. 2: Biometric Matching Results

The statistical summary, shown in Fig. 2a, provides a concise yet informative snapshot of the overall results. It includes the total number of matching entries retrieved, the number of contributing LEAs, including the requesting one, and the average matching score across all results. Two diagrams are displayed: a

pie chart representing the contribution of each LEA to the total matches, and a Venn diagram showing the distribution of results across the three biometric modalities —face, fingerprint, and voice.

As shown in Fig. 3, additional information is revealed by hovering over each section of the diagrams. Specifically, Fig. 3a, in the pie chart displays the number and percentage of results contributed by each LEA, while in Fig. 3b the Venn diagram indicates how many results correspond to each individual modality or combination of modalities.

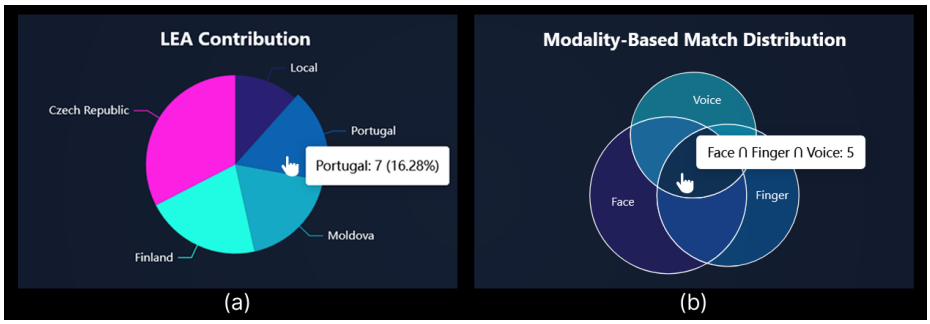

Fig. 3: Biometric Matching Statistics

The actual matching results Fig. 2b are organised by the originator LEA. The requesting LEA, and thus the local results are displayed first by default. Users can navigate between LEAs by selecting the respective tabs at the top of the results section. Each result includes a pseudonymised identifier and displays the matching scores for the available biometric modalities, provided there is a match in the corresponding biometric profile. The results are initially sorted in descending order by facial matching score. Users can re-sort the table based on fingerprint or voice sample scores by clicking the sorting button next to each modality name.

4.3 Local Biometric Matches Result

For local matches since the biometric profiles already belong to the user's LEA, full access to the associated data is granted for all possible matches. This allows the user to quickly assess whether the retrieved result corresponds to the same individual as the query. A confirmed match typically indicates that the individual has previously been apprehended by the LEA.

As shown in Fig. 4, if the matching confidence scores are relatively low, the user can manually verify the identity and confirm the match. By clicking the "View" button, the complete biometric profile becomes available. This includes the full name, personal information, and criminal background of the suspect.

Facial images and voice samples are particularly useful for manual verification, as they can be evaluated more intuitively compared to fingerprints, where

differences are often more subtle. All relevant data for the individual is displayed, including biometric samples, which can be viewed and, in the case of voice, listened to. For convenience, the original query data is also shown alongside the match, enabling direct comparison by the user.

Fig. 4: Local Biometric Matches Result

4.4 Cross-border Biometric Matches Result

When no local match is found, the user may rely on collaborating LEAs in hopes that the individual has previously been apprehended by them. As depicted in Fig. 5, the structure of the cross-border results mirrors that of local results. However, the biometric data is not immediately available for viewing, as the profiles belong to external LEAs. In such cases, the interface presents a "Request" option, allowing the user to request permission to view the data. This decision rests with the owning LEA and is granted at their discretion. Before submitting a request, the user can examine the similarity scores for each biometric modality —face, fingerprint, and voice— to determine whether the match appears reliable. If the request is approved, the full profile becomes accessible in the same manner as a local match.

Fig. 5: Cross-border Biometric Matches Result

In the example shown in Fig. 6, the Czech Republic provides a facial image that closely matches the query, as well as corresponding fingerprints and voice samples. Once approved by the owner LEA, these materials are made available to the requesting LEA for review and verification.

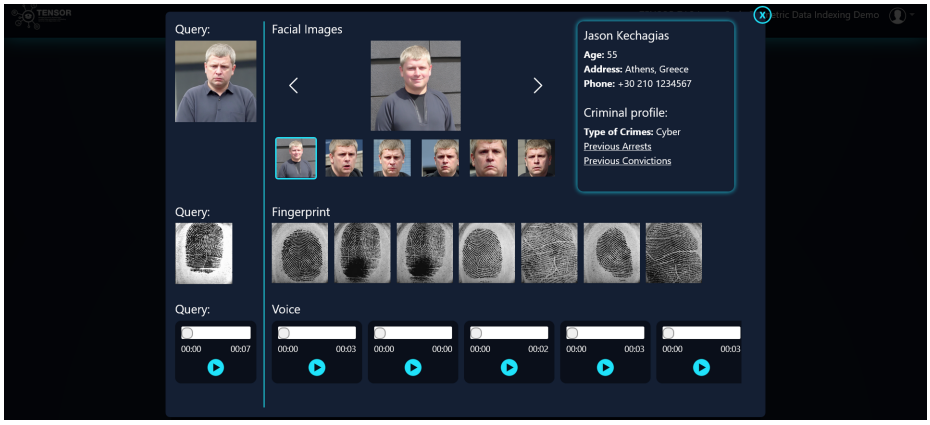

Fig. 6: Cross-border Biometric Matches Result After Request

5 Conclusion

In conclusion, this work presents a user-centered interface designed to support cross-border law enforcement investigations by streamlining multimodal biometric identification. The interface was integrated with the Large-Scale Biometric Indexer to ensure that heterogeneous biometric inputs from both local and external sources could be managed effectively, even in scenarios where data is incomplete. A clear distinction was maintained between local matches, where full identity details are accessible, and external matches from collaborating LEAs, which are presented with limited information due to privacy constraints. Complex similarity scores and match distributions were visualised interactively to aid interpretation by users without technical expertise, placing emphasis on user control and operational clarity. Through this design, a bridge was created between advanced biometric processing and practical investigative workflows.

Acknowledgment

The research leading to these results has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement No 101073920 (TENSOR). This publication reflects only the authors views. The European Union is not liable for any use that may be made of the information contained therein.

References

1. AbdulRaheem, M., Misra, S., Awotunde, J.B., Oladipo, I.D., Oluranti, J.: Automated fingerprint biometric system for crime record management. In: International Conference on Innovations in Bio-Inspired Computing and Applications. pp. 806–817. Springer (2021)

2. Chittibomma, S.S., Surapaneni, R.K., Maruboina, A.: Facial recognition system for law enforcement: An integrated approach using haar cascade classifier and lbph algorithm. In: 2024 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI). pp. 1–6. IEEE (2024)
3. Gomez-Barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A., Damer, N., Priesnitz, J., Evans, N., Busch, C.: Biometrics in the era of covid-19: Challenges and opportunities. IEEE Transactions on Technology and Society **3**(4), 307–322 (2022)
4. Guo, Y.: Impact on biometric identification systems of covid-19. Scientific Programming **2021**(1), 3225687 (2021)
5. Kim, S., Leonidis, A., Zidianakis, E.: Interaction styles. In: Interaction Techniques and Technologies in Human-Computer Interaction, pp. 1–44. CRC Press (2024)
6. Kyriakou, K., Apostolaras, A., Velentzas, P., Benos, G., Koutsoukos, K., Symvoulidis, C., Liang, K., Shi, Z., Leonidis, A., Miniadou, K., et al.: A secure and trustworthy biometric data ecosystem for cross-border suspect identification. In: 2024 IEEE International Conference on Big Data (BigData). pp. 2762–2771. IEEE (2024)
7. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., et al.: Handbook of fingerprint recognition, vol. 2. Springer (2009)
8. Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., Lawatsch, D., Domin, F., Schaubert, M.: Gandiffface: Controllable generation of synthetic datasets for face recognition with realistic variations. In: Proceedings of the IEEE/CVF International Conference on Computer Vision. pp. 3086–3095 (2023)
9. Miniadou, K., Leonidis, A., Papadopoulos, G.T., Stephanidis, C.: Encrypted biometric search: A deep learning approach to scalable and secure cross-border data exchange. In: 2024 IEEE International Conference on Big Data (BigData). pp. 2794–2800. IEEE (2024)
10. Miniadou, K., Leonidis, A., Papadopoulos, G.T., Stephanidis, C.: Enhancing secure cross-border collaboration among law enforcement agencies for facial biometric search. In: 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE). pp. 1–6. IEEE (2024)
11. P. Rey, W., V. Rolluqui, G.: Mobile automated fingerprint identification system (mafis): An android-based criminal tracking system using fingerprint minutiae structure. In: 2021 5th International Conference on E-Society, E-Education and E-Technology. pp. 62–68 (2021)
12. Rey, W.P.: Face recognition (fr) integration on mabis: A mobile automated biometric identification system for law enforcement in the philippines. In: Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering. pp. 8–16 (2023)
13. Rey, W.P.: Optimizing user interaction with mabis: An examination of usability and user experience in the mobile automated biometric identification system. In: Proceedings of the 2024 10th International Conference on Computer Technology Applications. pp. 215–222 (2024)
14. Talahua, J.S., Buele, J., Calvopiña, P., Varela-Aldás, J.: Facial recognition system for people with and without face mask in times of the covid-19 pandemic. Sustainability **13**(12), 6900 (2021)
15. Yamagishi, J., Veaux, C., MacDonald, K.: CSTR VCTK Corpus: English Multi-speaker Corpus for CSTR Voice Cloning Toolkit (version 0.92) (2019)