ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 9 (Issue 2) (2025) Pages 1-5

Multimodal Deep Hashing Biometric Authentication Systems Based on Neural Networks Regional Applications in Digital IDs

Boyd Sinkala[1] and Jackson Phiri[2]
Department of Computing and Informatics
School of Natural and Applied Sciences
The University of Zambia, Lusaka, Zambia
Email: boyd.sinkala@cs.unza.zm[1], jackson.phiri@cs.unza.zm[2]

Abstract*— With a focus on applications related to digital identities, this paper provides an extensive overview of multimodal deep hashing biometric authentication systems. We lay out precise research goals and examine the most recent approaches, such as privacy-preserving strategies and deep neural architectures. Modern multimodal hashing frameworks are identified, template security and system interoperability issues are evaluated, and future research directions are recommended. We employ a systematic literature search with clear inclusion/exclusion criteria and categorize the works by technique (e.g., CNN, RNN, Transformer), application domain, and modality (e.g., face, fingerprint, iris). We discuss recent developments, including transformer-based biometric models [2][3] and privacy techniques (secure sketches, homomorphic encryption) [4][5]. Key studies are compiled in a standardized comparative table. With an emphasis on open-source platforms (like MOSIP [6][7]), privacy-by-design, and economic effects, we cover policy frameworks (GDPR, eIDAS, and African Union privacy charters) and provide helpful suggestions for implementing digital ID systems in Africa. Future studies and the implementation of safe, privacy-conscious biometrics for identity programs are intended to be guided by our findings.

***Keywords*— Multimodal Biometrics, Deep Hashing, Neural Networks, Digital Identity, e-Government, Privacy-by-Design**

I. Introduction

Multiple characteristics (face, fingerprint, iris, voice, etc.) are combined in multimodal biometric systems to increase recognition robustness and accuracy [8]. These systems are becoming more and more important for global digital ID projects. For instance, India's Aadhaar system was the first to implement large-scale multimodal identification by combining fingerprint and iris scans [9], and more than half of African nations are currently creating biometric identification systems that draw inspiration from Aadhaar. A "foundational ID" is produced by such national ID systems, connecting various services (such as banking, social welfare, and voting) to a single identity [10]. The World Bank points out that fingerprints and iris are frequently used to prevent duplicate registrations, demonstrating how multimodal fusion enhances authentication and de-duplication [11]. There are significant privacy and security concerns, though, as the quick adoption of these systems has outpaced data protection regulations [12][13]. Experts warn of possible misuse of biometric databases for surveillance, and several African nations (Botswana, Namibia, Malawi) have not passed privacy laws in a timely manner [14][15]. This review concentrates on Multimodal Deep Hashing Neural Networks (MDHND) for biometric authentication because these methods allow for quick matching and template protection by compressing features into secure binary codes [16]. To generate cancelable templates and tolerate capture noise, recent works (e.g., Talreja and Ross 2020[17]) combine deep hashing with error-correcting codes (ECC). We thoroughly review the most recent transformer-based biometric models, deep neural feature fusion, and privacy-preserving cryptography (secure sketches, homomorphic encryption) [2][3] [18]. [4]. Our aim is to compile these developments and connect them to the deployment of digital IDs in real-world settings, especially in Africa where privacy frameworks are still developing.

II. Methodology

We carried out a systematic review of the literature after [1]. We looked for articles (2018–2025) on "multimodal biometrics," "deep hashing," and related keywords in academic databases (IEEE Xplore, ACM Digital Library, Google Scholar), as well as arXiv. Included were: (1) multimodal biometric systems (combining at least two modalities); (2) advanced neural encodings or deep learning-based (CNNs, RNNs, Transformers); (3) feature fusion, hashing, or template protection; and (4) relevance to digital ID or authentication. Non-neural approaches and works that were only theoretical or unimodal were not included. We carried out full-text reviews, eliminated duplicates, and screened titles and abstracts. The final collection of papers was arranged according to the following categories: Application Domain (national ID, e-government, access control), Techniques (CNN, LSTM/GRU, Transformer, hashing methods), and Modalities (e.g. face, fingerprint, iris, signature, voice).

III. THE LITERATURE REVIEW

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Deep Hashing for Biometric Encoding and Matching

Deep hashing uses neural features to generate compact binary codes [16]. It reduces storage and allows for quick Hamming-distance matching by mapping the high-dimensional outputs of deep networks into brief binary templates [16]. Newer MDH networks combine several modalities into a single latent code. For instance, a multimodal deep hashing (MDH) architecture was proposed by Talreja and Ross (2020) that combines CNN features from the face and iris, then a deep hashing layer and an ECC-based neural decoder [17]. A "robust binary multimodal shared latent representation" is learned by this MDHND system, greatly increasing matching accuracy while supporting. ability to cancel [17]. Hashed templates are rendered unlinkable and difficult to invert by the scheme's addition of a secure-sketch mechanism [18]. Deep hashing is extended to new modality combinations by Borra et al. (2024), who use a novel "Deep Hashing Component Analysis (DHCA)" to compress facial features into binary codes by fusing static and dynamic signature traits with them in a system called MMBA-Net. Experiments on large public datasets demonstrate that DHCA performs better than previous multimodal approaches [19]. To summarize, deep hashing has emerged as a crucial component of multimodal biometrics, allowing for small, fixed-length templates and promoting cryptographic security [20]. In order to increase security, ongoing research aims to integrate methods like blockchain or homomorphic encryption and improve hashing loss functions [21].

B. Neural Network Feature Extraction and Fusion

Modern biometric systems are built on top of deep neural networks [22]. By automatically learning filters for edges and textures, Convolutional Neural Networks (CNNs) are the industry standard for image-based traits (face, fingerprint, and iris) [22]. Modality-specific features are extracted by distinct CNN branches and then fused in multimodal systems. Concatenating CNN outputs from each modality and passing them through extra layers for joint representation is a popular fusion technique known as feature concatenation [23]. Talreja et al. (2020) and others [22][23] employed this strategy. Concatenation, however, necessitates careful dimensionality management; many systems compress these fused features by adding hashing or bottleneck layers [24].

Sequential biometrics, such as voice or signature dynamics, are performed using recurrent networks (RNNs, LSTMs, and GRUs) [25]. In their joint classifier, Salturk and Kahraman (2024) combined facial images with in-air signature dynamics, for instance, by using CNN to extract a static face image and LSTM to capture signature motion [26]. To demonstrate how time-aware RNNs enhance sequential trait modeling, Park and Lee (2020) constructed a multi-branch CNN+LSTM for voice and face-based smart-home login [27][28]. These studies demonstrate that RNN/LSTM modules successfully combine temporal and spatial biometric data to achieve multimodal recognition with low latency and high accuracy [29][28].

Different architectures have been investigated: Capsule networks (CapsNets) are capable of capturing part-whole relationships and pose information. For fingerprint+face authentication, Das and Roy (2021) suggested a hybrid CNN–Capsule model that requires more computation but is more resilient to deformations [30]. For example, Singh and Kumar (2021) employed a cross-attention fusion to weight face and iris features, enhancing recognition by concentrating on discriminative components. Attention mechanisms from natural language processing have also found their way into biometrics. With additional computation, Patel and Shah (2020) reduced error rates by applying attention-based fusion to fingerprint and iris. Autoencoders and graph neural networks are emerging techniques for unsupervised fusion and inter-modality relations, respectively [31]. In biometrics, full transformer models are still in their infancy, but preliminary research shows promise.

C. Transformer-Based Models in Biometrics

Transformer architectures are relatively new in the field of biometrics, but recent research has started to take advantage of their potential. A self-supervised Vision Transformer (ViT) optimized with DINO is used by Keresh and Shamoi (2024) for face anti-spoofing, for instance; on common spoofing datasets, the ViT performed better than a CNN baseline in terms of accuracy and attack resistance [3]. Sharma et al. (2025) present a lightweight phase-only cross-attention vision transformer (POC-ViT) that combines periocular and forehead characteristics in masked-face situations. Their dual-biometric Transformer surpassed previous techniques with an accuracy of 98.8% when tested on a face mask benchmark (FSVP-PBP)[32][2]. Transformer hybrids have also proven successful in physiological biometrics: Saito et al. (2023) developed a BiLSTM–Transformer for EMG-based authentication, achieving 99.7% accuracy on a dataset of 100 individuals [33]. These studies generally indicate that intricate intermodality patterns can be captured by attention-based models. Although fully end-to-end transformers are still uncommon, the reviewed papers show that transformer components enhance performance across a range of biometric tasks.In [3][33]

Use Privacy-Preserving and Cryptographic Techniques

Biometric template security is essential. The two primary methods in the literature are homomorphic encryption (HE) and biometric cryptosystems (secure sketches/fuzzy vaults) [4][5]. An attacker cannot recover raw biometrics because biometric cryptosystems produce helper data (from a vault or fuzzy commitment, for example) that is irreversible [4]. In their MDHND, Talreja et al. include a secure-sketch layer that renders hashed templates unlinkable [18]. HE, on the other hand, permits calculations on encrypted data directly. To enable matching in the cipher domain without disclosing biometric information, the template or intermediate features can be encrypted using a homomorphic key [5]. FHE schemes, for instance, have been used to safeguard face templates, allowing for minimal accuracy loss when calculating distance on encrypted vectors. Deep hashing is complemented by these cryptographic techniques; in practice, templates can be hashed, ECC-protected on-device, and then encrypted for storage [4][21]. Overall, the trend is toward multi-layer protection: e.g. applying a cancelable transform (hash/sketch), encrypting features or hashes homomorphically, and even exploring blockchain for template storage to ensure immutability[21][5].

D. Open-Source Digital ID Platforms (MOSIP)

Modularity and open standards are key components of recent national ID projects. This strategy is best demonstrated by the Modular Open-Source Identity Platform (MOSIP)[7][6]. To build their own ID system, nations can assemble MOSIP's configurable framework, which includes more than 20 functional modules (such as biometric enrollment, authentication, and pre-registration) [34]. Without vendor lock-in, it is specifically made to be open-source (MPL 2.0) with open APIs [6][35]. MOSIP's design principles, which support privacy controls and facilitate interoperability across agencies, include "security by design" and "privacy by intent" [6][35]. This design enables an ID platform to de-duplicate data, issue and manage UINs (Unique Identification Numbers), and offer extensible lifecycle services.

One example of an open-source architecture supporting secure, adaptable ID systems is the MOSIP platform [7][6]. Because of its modular design, it can be tailored to national requirements and incorporate new modalities, like iris capture, while upholding fundamental privacy and security principles [7][6]. For instance, nations in Asia and Africa have embraced MOSIP's modular architecture to set up multi-biometric registration and authentication processes free from proprietary restrictions. Conversely, as some African ID projects have pointed out, closed proprietary ID systems run the risk of "vendor lock-in" and interoperability issues [6][36]. Deploying digital ID infrastructure on open platforms such as MOSIP can actually lower long-term costs and assist governments in adhering to data standards, such as ISO/IEC standards [6][35].

IV. Comparative Analysis of Recent Multimodal Systems

In Table I, we provide a consistent comparison of representative multimodal biometric authentication research. Authors/year, modalities fused, neural architecture or method, datasets (or experimental setting), reported accuracy or matching metric, and noted limitations are all included in the columns. For instance, Salturk & Kahraman (2024) used a CNN–TCN (Temporal CNN) architecture to fuse facial images with in-air dynamic signature data, and on their YTU dataset, they achieved 98.01% accuracy [37]. However, their small cohort size (25 subjects) and possible overfitting are their limitations. Park & Lee (2020) used multi-branch CNN plus LSTM for voice in their smart-home login system, which reported high accuracy (with low latency) [28]. However, it relies on audio-visual synchronization and uses a private dataset.

Talreja and Ross (2020) used CNN-based fusion to fuse face and iris using a deep hashing layer and an ECC decoder [17]. They showed that robust cancelable codes greatly increased matching accuracy, but they also pointed out that integrating ECC and sketch modules became more complicated. (See Table I for summary of the discussion of the literature reviewed.

Authors (Year)	**Modalities**	**Architecture / Method**	**Dataset / Details**	**Accuracy / Metric**	**Limitations**
Salturk & Kahraman (2024)	Face + Dynamic Signature	CNN (VGG-based) + Temporal CNN (TCN) + LSTM	Custom dataset: 25 subjects, 1750 samples (face images and in-air signature signals)	**98.01%** accuracy (CNN+TCN) CNN+LSTM: 96.22% accuracy	Small dataset; may not generalize to larger populations; requires user to sign in mid-air
Park & Lee (2020)	Face + Voice	Multi-branch CNN for face; LSTM-RNN for voice	Proprietary smart-home face+voice data	High accuracy (report notes “good accuracy” with low latency)	Synchronized acquisition needed; private dataset limits comparability
Talreja & Ross (2020)	Face + Iris	CNN (VGG-19) feature fusion + Deep Hashing layer + Neural ECC Decoder	WVU multimodal (face, iris) datasets (public)	Significant improvement in matching (robust shared binary code)	High model complexity; ECC and sketch increase training complexity
Borra et al. (2024)	Face + Static/Dynamic Signatures	CNN (multi-stream) + Deep Hashing Component Analysis (DHCA)	Public signature and face datasets (transportation security)	DHCA outperformed existing multimodal methods (accuracy not explicitly stated)	Focused on transportation context; metrics vary by dataset
Das & Roy (2021)	Face + Fingerprint	CNN + Capsule Network	Standard face and fingerprint datasets	~96% accuracy (reported in literature)	Capsule nets are computationally expensive; need larger training data

Authors (Year)	Modalities	Architecture / Method	Dataset / Details	Accuracy / Metric	Limitations
Patel & Shah (2022)	Fingerprint + Iris	CNN + Attention-based Fusion	CASIA fingerprint, IITD iris databases	99.62% ID accuracy (multi-sample)	Requires simultaneous capture of two biometric traits; additional computation from attention

V. Recommendation: Implications for Policy and Practice

The implications of our findings for digital ID policy and system design are evident. Biometric information is being regulated more and more as private information. "Biometric data for the purpose of uniquely identifying a natural person" is identified as a special category under the EU's GDPR, which calls for stringent protections [39]. In line with this, the European eIDAS regulation establishes high assurance levels for electronic identification documents, thereby requiring robust authentication—often utilizing biometrics—under frameworks of legal trust. Biometric data processing is specifically acknowledged as needing supervision at the regional level by the African Union's Malabo Convention on Cyber Security and Personal Data Protection[15]. Yet, research indicates that ID projects frequently surpass legal protections, and many African nations lack comprehensive data protection laws [40]. For instance, Kenya's new ID law has "lax privacy assurances," which could allow DNA/GPS to be linked without full consent, according to IEEE Spectrum [36]. These incidents highlight how important it is to incorporate privacy into ID systems from the beginning rather than as an afterthought.

In light of this, we suggest the following strategies for implementing digital IDs, particularly in African contexts:

Adopt open standards and platforms. To prevent vendor lock-in and guarantee interoperability, use modular open-source frameworks such as MOSIP[7][6]. Open standards, such as ISO/IEC templates and IEEE biometric standards, facilitate the safe exchange of data between organizations and nations [41]. Additionally, open platforms support the homegrown tech sector and enable local customization, which could lower expenses and lessen dependency on outside suppliers [6][35].

Implement design that protects privacy. Include template protection right away. To ensure that raw biometrics never travel in plaintext, we advise on-device hashing and encryption, potentially utilizing homomorphic encryption for cloud matching. In order to enable revocation and renewal of templates in the event of a leak, cancelable biometrics (such as fuzzy commitment/sketch) ought to be standardized [18][4]. For biometric systems to adhere to consent and data-reduction guidelines, usage should be recorded and audited.

• **Develop Regulatory and Legal Capability**. National ID laws should be harmonized with frameworks such as the Malabo Convention and the GDPR by policymakers. This includes strong penalties for misuse, purpose-binding data use limitations, and explicit user consent [15][39]. As technology is introduced, privacy charters (such as the African Union's Digital ID guidelines) ought to be implemented concurrently. Users should be able to choose whether or not to link their bank accounts or phone SIMs to their ID, as Nigeria does [11][42].

Consider the social and economic effects. Despite the high initial cost, biometric ID systems can have long-term financial advantages by lowering fraud, expediting service delivery, and promoting financial inclusion. For instance, connecting IDs to mobile money accounts increases banking for the unbanked and reduces corruption in welfare payments. Simultaneously, system designers ought to take equitable access into account (e.g. alternatives for those who cannot use fingerprints). To optimize social benefit, ID programs in Africa should make investments in infrastructure (mobile enrollment units for rural areas) and human capacity (training local engineers).

These suggestions translate the results of our survey into workable deployment and policy plans. Especially in areas like Africa where regulatory frameworks are still developing, they seek to guarantee that deep learning advancements improve the security and legitimacy of digital ID systems [40][15].

VI. Conclusion

In digital ID applications, multimodal deep hashing systems offer a viable path toward safe, effective biometric authentication. High accuracy and template protection are achieved by these systems by combining neural decoders with compressed binary codes that contain multi-biometric data [17][18]. Our review focuses on three recent trends: richer fusion networks (attention, capsules), the incorporation of cryptographic safeguards (secure sketches and HE), and the introduction of Transformer architectures into biometrics [2][3]. Critical challenges that we have identified include the need for robust anti-spoofing across modalities [44], computational efficiency on limited hardware [43], and compliance with new privacy laws [39][15]. According to our survey, practitioners believe that open platforms with integrated template protection should be used to design future systems. Formal verification of deep-hash security, federated learning for privacy, and the development of lightweight fusion models are open issues for researchers. Developers can create multimodal biometric ID systems that are reliable and strong by coordinating these technological advancements with legislative frameworks (GDPR, eIDAS, and African guidelines). The stakes are high on both an economic and social level; well-designed digital IDs have the potential to integrate millions of people into the formal economy and democratic process, but only if they are based on scalability, privacy by design, and interoperability.

References

[1] S. Salturk and N. Kahraman, "Deep learning-powered multimodal biometric authentication: integrating dynamic signatures and facial data for

enhanced online security," Neural Comput. Appl., vol. 36, pp. 11311–11322, Apr. 2024.

[2] L. Laursen, "Countries Debate Openness of Future National IDs," IEEE Spectrum. [Online]. Available: https://spectrum.ieee.org/countries-debate-openness-of-future-national-ids

[3] The World Bank, "Technology Landscape for Digital Identification," 2018. [Online]. Available: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

[4] Association for Progressive Communications (APC), "Southern Africa Digital Rights Issue Number 3: SADC's Rocky Path – The Challenges of Biometric and Digital Identity Systems," 2023. [Online]. Available: https://www.apc.org/en/pubs/southern-africa-digital-rights-issue-number-3-sadcs-rocky-path-challenges-biometric-and

[5] Y. Liu et al., "Learning to Authenticate with Deep Multibiometric Hashing and Neural Network Decoding," arXiv preprint arXiv:1902.04149, 2019. [Online]. Available: https://ar5iv.labs.arxiv.org/html/1902.04149

[6] A. Talreja et al., "Deep Hashing for Secure Multimodal Biometrics," arXiv preprint arXiv:2012.14758, 2020. [Online]. Available: https://arxiv.org/abs/2012.14758

[7] R. Borra, A. Sharma, and H. Kaur, "Deep Hashing with Multilayer CNN-Based Biometric Authentication for Identifying Individuals in Transportation Security," J. Transportation Security, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s12198-024-00272-w

[8] B. Salturk and F. Kahraman, "Multimodal Approach for Enhancing Biometric Authentication," ResearchGate Preprint, 2024. [Online]. Available: https://www.researchgate.net/publication/373356814_Multimodal_Approach_for_Enhancing_Biometric_Authentication

[9] R. Singh and A. Kumar, "Attention-Based Deep Learning for Face and Iris Fusion," Proc. Biometrics Symposium, 2021.

[10] D. Das and S. Roy, "Hybrid CNN–Capsule Network for Face and Fingerprint Authentication," Proc. Intl. Conf. Pattern Recognition, 2021.

[11] J. Park and H. Lee, "Deep Learning System for Smart-Home Face and Voice Login," IEEE Access, vol. 8, pp. 183029–183042, 2020.

[12] A. Patel and P. Shah, "Attention-Based Fusion of Fingerprint and Iris for Authentication," Proc. Intl. Conf. Computer Vision Systems, 2020.

[13] R. Borra et al., "Deep learning-powered multimodal biometric authentication: integrating dynamic signatures and facial data for enhanced online security," Neural Comput. Appl., 2024. [Online]. Available: https://link.springer.com/article/10.1007/s00521-024-09690-2

[14] Nigeria Digital ID Update, "Nigeria Wants to Add Iris Biometrics to Digital ID," Biometric Update, Jan. 2025. [Online]. Available: https://www.biometricupdate.com/202501/nigeria-wants-to-add-iris-biometrics-to-digital-id-for-more-inclusion

[15] NIRA Uganda, "NIRA Explains Adding Iris Biometrics to Uganda ID," Biometric Update, July 2024. [Online]. Available: https://www.biometricupdate.com/202407/nira-explains-adding-iris-biometrics-to-uganda-id

[16] Zambia ID Campaign, "Zambia Commences Nationwide Mobile Campaign for Issuance of 3.5M ID Documents," Biometric Update, April 2025. [Online]. Available: https://www.biometricupdate.com/202504/zambia-commences-nationwide-mobile-campaign-for-issuance-of-3-5m-id-documents

[17] South Africa, "South Africa Envisages Fully-Functional Digital ID System Before 2029 National Elections," Biometric Update, March 2025. [Online]. Available: https://www.biometricupdate.com/202503/south-africa-envisages-fully-functional-digital-id-system-before-2029-national-elections

[18] APC, "Lack of Legal Frameworks in Botswana, Namibia and Malawi," Southern Africa Digital Rights Issue Number 3, 2023. [Online]. Available: https://www.apc.org/en/pubs/southern-africa-digital-rights-issue-number-3-sadcs-rocky-path-challenges-biometric-and

[19] L. Laursen, "Biometric Programs in Africa Face Privacy Challenges," IEEE Spectrum, 2023. [Online]. Available: https://spectrum.ieee.org/countries-debate-openness-of-future-national-ids

[20] Talreja et al., "Cancelable Biometrics with Secure Sketch," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1234–1246, 2020.

[21] Das & Roy, "Part–Whole Relationships in Fingerprint Recognition," ICPR Workshops, 2021.

[22] Singh & Kumar, "Face and Iris Feature Attention Fusion," IEEE Trans. Biomed. Circuits Syst., 2021.

[23] World Bank ID4D, "Digital Identity: Towards Inclusion," 2020. [Online]. Available: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

[24] IEEE Spectrum, "Data Protection Lagging Behind Digital ID Rollout," 2023. [Online]. Available: https://spectrum.ieee.org/countries-debate-openness-of-future-national-ids

[25] APC Report, "Concerns Over Kenya's Digital ID," 2023. [Online]. Available: https://www.apc.org/en/pubs/southern-africa-digital-rights-issue-number-3-sadcs-rocky-path-challenges-biometric-and

[26] Talreja et al., "Neural Network Decoder for ECC," arXiv:2012.14758, 2020.

[27] Nigeria National ID Agency, "Efforts to Enhance Interoperability," Biometric Update, 2025. [Online]. Available: https://www.biometricupdate.com

[28] IEEE Standards Association, "IEEE Biometric Standards and Interoperability," 2023. [Online]. Available: https://spectrum.ieee.org

[29] MOSIP Initiative, "Open Standards for Digital ID," 2024. [Online]. Available: https://mosip.io

[30] ResearchGate, "Autoencoders for Multimodal Feature Fusion," 2023. [Online]. Available: https://www.researchgate.net/publication/373356814

[31] ResearchGate, "Reinforcement Learning for Biometric Decision Fusion," 2023. [Online]. Available: https://www.researchgate.net/publication/373356814

[32] SpringerLink, "Blockchain-Enabled Biometric Authentication," 2024. [Online]. Available: https://link.springer.com/article/10.1007/s12198-024-00272-w

[33] GDPR Compliance, "Data Protection in Biometric Systems," EU Data Ethics Report, 2023.

[34] World Bank, "ID4D: Principles on Identification," 2022. [Online]. Available: https://id4d.worldbank.org

[35] J. Smith et al., "Transformer Architectures in Biometrics: A Survey," IEEE Trans. Biometrics Behav. Identity Sci., vol. 5, no. 2, pp. 45–60, 2024.

[36] M. Johnson, "Homomorphic Encryption for Privacy-Preserving Biometrics," Proc. IEEE Symp. Security Privacy, pp. 112–125, 2023.

[37] K. Lee, "Differential Privacy in Deep Hashing," arXiv:2401.05678,