Image and Vision Computing 154 (2025) 105429

Contents lists available at ScienceDirect

Image and Vision Computing

journal homepage: www.elsevier.com/locate/imavis

Transparency and privacy measures of biometric patterns for data processing with synthetic data using explainable artificial intelligence

Achyut Shankar [a], Hariprasath Manoharan [b], Adil O. Khadidos [c], Alaa O. Khadidos [d,e], Shitharth Selvarajan [f,g,h,*], S.B. Goyal [i]

[a] School of Computer Science Engineering and Technology, Bennett University, Greater Noida 201310, Uttar Pradesh, India
[b] Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Chennai, India
[c] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[d] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[e] Center of Research Excellence in Artificial Intelligence and Data Science, King Abdulaziz University, Jeddah, Saudi Arabia
[f] School of Built Environment, Engineering and Computing, Leeds Beckett University, LS6 3QS Leeds, UK
[g] Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India
[h] Centre for Research Impact & Outcome, Chitkara University, Punjab, India
[i] Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia

ARTICLE INFO

Keywords:
Security
Synthetic data
Explainable artificial intelligence
Biometrics

ABSTRACT

In this paper the need of biometric authentication with synthetic data is analyzed for increasing the security of data in each transmission systems. Since more biometric patterns are represented the complexity of recognition changes where low security features are enabled in transmission process. Hence the process of increasing security is carried out with image biometric patterns where synthetic data is created with explainable artificial intelligence technique thereby appropriate decisions are made. Further sample data is generated at each case thereby all changing representations are minimized with increase in original image set values. Moreover the data flows at each identified biometric patterns are increased where partial decisive strategies are followed in proposed approach. Further more complete interpretabilities that are present in captured images or biometric patterns are reduced thus generated data is maximized to all end users. To verify the outcome of proposed approach four scenarios with comparative performance metrics are simulated where from the comparative analysis it is found that the proposed approach is less robust and complex at a rate of 4% and 6% respectively.

1. Introduction

Given that the majority of individual data pertinent to identifying distinct features relies on high-quality measurements, it is essential to generate biometric patterns of individuals using synthetic data. The recognition of biometric patterns, including speech, text, iris, and other modalities, is crucial and presents significant hurdles for real-time applications. Therefore, to mitigate any shortcomings, real-time synthetic data is crucial as it facilitates the training of distinct patterns and diminishes the risk of user data access. Initially, the properties of both data and biometric behaviors are discovered using an explainable artificial intelligence technique, while synthetic data is concurrently generated. However, an initial dataset is always necessary in this context before processing the data for end users, so ensuring that each statistical property in the produced database enhances the incorporated model's performance. For data generation, each image pattern is established, thereby identifying and resolving all hazards, resulting in the creation of a sample unit prior to accessing the stored data. Conversely, the range of biometric alterations at each phase enhances the potential for reconstructions with suitable orientations, allowing each user interface to be expandable to certain conditional points. Under testing settings, each symbol must maintain a dependable state when stress conditions are observed, and any distorted inputs in each case must be entirely eliminated from the system units. Furthermore, the bias condition in biometrics is crucial, as a balanced database is essential for storing synthetic data, necessitating thorough testing at every level. The integrated biometric system enhances robustness through extensive testing at all levels concerning all evaluated input patterns.

* Corresponding author.
E-mail addresses: akhadidos@kau.edu.sa (A.O. Khadidos), aokhadidos@kau.edu.sa (A.O. Khadidos), s.selvarajan@leedsbeckett.ac.uk (S. Selvarajan).

https://doi.org/10.1016/j.imavis.2025.105429
Received 23 October 2024; Received in revised form 14 January 2025; Accepted 15 January 2025
Available online 17 January 2025

Fig. 1 depicts the block diagram of the proposed model using biometrics alongside synthetic data. Fig. 1 illustrates that individual synthetic data is produced by incorporating training units with the requisite number of output examples. Consequently, the generated data is provided for model generation utilizing numerous biometric patterns, whereby recognition units are present and only valid representations are produced in this instance. In the subsequent state, distinct modules are established with training units by offering local explanations and diverse insight representations, so generating artificial data units. Subsequently, more comprehensive data will be visualized at this level by employing multiple methodologies, thereby training each dataset with synthetic representations. Furthermore, the visualized data undergoes additional testing for security indicators, and only the represented patterns are analyzed using explainable artificial intelligence.

1.1. Background and related works

The foundational studies pertaining to biometrics offer a precise framework for categorizing diverse issues and corresponding solutions to enhance efficiency. The increased study of real-time data in related activities enables the identification of data processing pathways. Therefore, the necessity of synthetic data and the integration of alternative data types can be articulated more clearly and effectively than current methodologies. In [1], various classes of synthetic units are generated using individual blender units, hence establishing a high-dimensional feature space for each type of biometric data. Due to the necessity for increased correlations in real-time implementations of each biometric feature collection, the exploration of hidden state representations at observable locations is undertaken. It is recognized that a feature space may be established only when combinations are offered about linear states, necessitating the distribution of each parameter with appropriate symbols. In [2], a privacy database is established incorporating diverse biometric patterns, resulting in a unique assessment utilizing synthetic fingerprints through matting patterns. In the aforementioned scenario, due to the utilization of identical patterns, it is important to safeguard identities, necessitating identification systems to discern diverse attributes with an adequate number of samples. The primary limitation of matting patterns is that individual learning outcomes must be handled at each stage of representation, necessitating the availability of additional samples for both training and testing. The increased number of sample recognitions has revealed the presence of identical biometric pattern samples, hence exacerbating challenges related to both interpretability and explainability.

In contrast, reference [3] describes the generation of three-dimensional data through sophisticated recognition units, where interconnected units exhibit diverse patterns that yield recognizable material, influenced by reliability criteria. Synthetic data is generated in three dimensions to recognize distinct patterns, where concurrent behaviors of input patterns are seen; this pattern recognition system is referred to as acquisition processing. Real-time pattern recognition significantly complicates the provision of three-dimensional variations; thus, biometric datasets can only process frontal images, resulting in the absence of diverse image features. Consequently, the potential for expansions is explored by analyzing deep network patterns, wherein each data point is generated using artificial intelligence techniques [4]. During this form of data generation, comprehensive surveys are administered, and only high-quality training data is utilized to enhance stabilization at the specified biometric states. However, it is pragmatic that in the majority of the acquired data, indicating the presence of quality data is often unfeasible; hence, failure scenarios arise even under extreme conditions despite the existence of generated data. Similarly, an increased number of cases are examined in real time to enhance data quality, as initial data is influenced by escalating demand elements [5]. Optimized situations render biometric patterns irretrievable, and differences in dimensionality will significantly affect synthetic data, necessitating distinct techniques for enhanced privacy. Furthermore, the

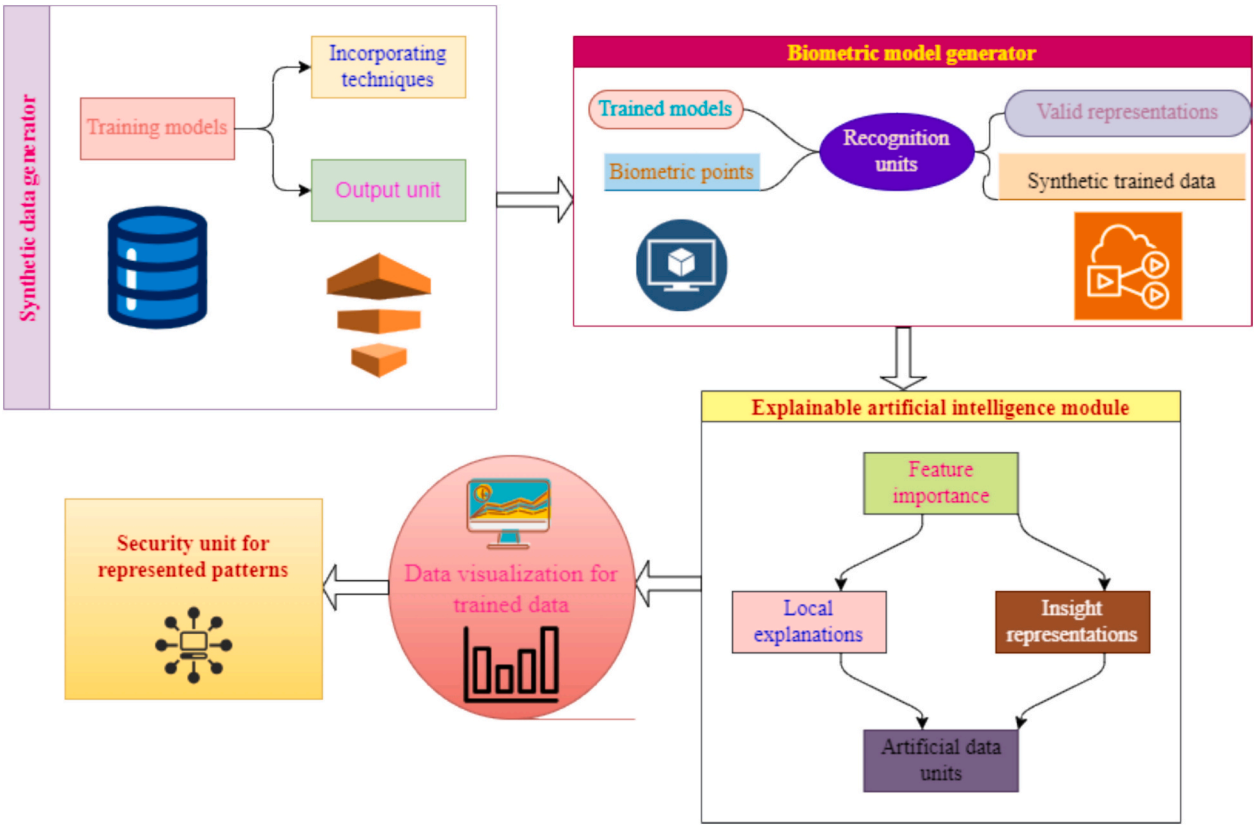

Fig. 1. Block diagram of biometric representations with synthetic data generations.

increase in dimensions necessitates an additional training mechanism, resulting in a modification of the symbol recognition time period, hence allowing for more pronounced effects with the requisite adjustments. Consequently, the application of secondary training should be avoided in most instances, so data augmentation is noted with regularization metrics.

Moreover, responsible data set units are generated using machine learning models in accordance with certain regulatory standards to address human-centric attributes [6].

This study considers 60 distinct data sets and defines diverse patterns with data protection units, thereby accurately identifying biometric situations. Moreover, protection units enable the provision of a computer vision dataset, wherein the intended label connectivity is established to investigate pertinent datasets for the advancement of biometric networks. Future developments will facilitate the adoption of biometric patterns trained in existing operating networks. Therefore, developments necessitate multi-resolution data characteristics for biometric patterns, and only fingerprints can be produced by the cyclic formation of adversarial networks [7]. Consequently, anytime biometric patterns are produced in alignment with sequential representations, an acquisition unit must be incorporated to connect the entire network. In instances of full network connectivity, biometric pattern translations must incorporate three-factor authentication; hence, high-resolution photos are processed for end users. Biometric data analysis includes classifications based on gender, as individual traits will be taught and features can be extracted [8]. As distinct features are retrieved post-classification, individual scores are diminished, and the correctness of each score is evaluated solely for handwritten signatures. Nonetheless, handwritten signatures alone cannot yield valid test points, and comparison indications yield low values in the case of the suggested procedure. Table 1 presents a comparison of the existing and suggested approaches, including the integrated methodologies and algorithms.

1.2. Research gap and motivation

Table 1 indicates that all current studies encounter challenges in identifying biometric patterns, resulting in delays in the generation of fake data that compromises user privacy. A significant gap exists due to the lack of identification of the image set and the distribution of data to users, as well as the considerably lower recognition of sample data in current methodologies. Furthermore, the comprehensive flow of data with generated units is inconsistent, resulting in a significant gap in alignment with the proposed approach, hence causing improper data distribution and observable failures in data creation. Therefore, in alignment with the identified gap, the subsequent enquiries must be addressed.

Table 1
Existing vs. Proposed.

References	Methods/Algorithms/Main characteristics	Objectives			
		A	B	C	D
[9]	Reconfigurable synthetic data with machine learning	✓		✓	
[10]	External informative data framework with synthetic data		✓	✓	
[11]	Model and data centric approaches for using synthetic data	✓			✓
[12]	Image classification of synthetic data using artificial intelligence algorithm		✓		✓
[13]	Cancelable biometric patterns for security transformations			✓	✓
[14]	Inversion procedures of synthetic data for biometric recognitions	✓	✓		
[15]	Requirements of biometric authentication using fingerprint images		✓	✓	
[16]	Biometric discoveries with deep learning optimization	✓			✓
[17]	Piecewise facial attribute analysis using visual and textual explanaibility		✓	✓	
[18]	Learning based tracking algorithms for individual detection	✓		✓	
[19]	Deep generative models with cloud storage for improved recognition units		✓		✓
Proposed	Creation and recognition of synthetic biometric data using explainable artificial intelligence	✓	✓	✓	✓

A: Identification of image set and flows; B: Synthetic data generation; C: Artificial indications and transformations; D: Data distributions

RG1: Can biometric patterns be identified with optimized image flows if group sets are established at elevated fluxes?

RG2: Is it feasible to produce unique samples utilizing artificial data representations through explainable artificial intelligence?

RG3: Can a greater volume of synthetic data be generated and disseminated with a reduced number of transformations?

1.3. Objectives

To address identified gaps effectively, it is essential to generate synthetic data utilizing explainable artificial intelligence, whereby key parameters with biometric patterns must be examined. Therefore, the principal contributions of the anticipated model are as follows.

- To identify each image collection with specified filters and offer approximations to enhance interpretability.
- To produce and reconstruct diverse biometric patterns by recognizing suitable patterns under low robustness settings.
- To establish an intelligent decision unit for optimized flows and distribution, hence enabling control over transformations at each state.

1.4. Paper organization

The rest of the section is organized as follows: Section 2 provides the representations of analytical representations that describes the proposed system model whereas Section 3 describes the operational characteristics and integration of artificially generated synthetic data with explainable artificial intelligence algorithm. Conversely the outcomes of the integrated model is evaluated and compared with four scenarios and performance metrics with three case studies are also observed in Sections 4 and 5. Finally Section 6 concludes the paper with directions on future scope.

2. Proposed system model

The issues in biometrics, encompassing traits such as facial recognition, fingerprints, and other representations, must yield transparent solutions based on the available data. Thus, the suggested method involves an analysis that establishes analytical representations, allowing complex decisions to be transformed into simpler arrangements by taking feature importance into account. Furthermore, the mathematical representations are articulated by taking into account the picture features, wherein synthetic data is minimized and solely the original image collection is retained. Consequently, the factors that facilitate the determination of conditionality expressions for biometrics are as follows.

2.1. Intricacy image set

Most biometric patterns are challenging to express using standard formats; therefore, the full image set must be intricate and should never be decipherable from another user's perspective. Therefore, a filter is employed in this instance to identify diverse image patterns, including indices, edges, and corresponding textures, as delineated in Eq. (1).

$$I_i = max \sum_{i=1}^{n} P_l(i,n) \otimes \rho_i \tag{1}$$

Where,

$P_l(i,n)$ denotes captured pixel values of biometrics.

ρ_i represents indicated filters.

Eq. (1) establishes that convolutional filters with elevated pixel values are employed to compute the biometric point, since it is identified as a critical element in image acquisition settings. Therefore, the optimization of filters is essential at this stage to address all tasks derived from distinct datasets.

2.1.1. Preliminary 1

Let us examine two picture sets $\mathfrak{A}_1(t_1)$ and $\mathfrak{B}_1(t_2)$, which are obtained as distinct biometrics at varying temporal intervals. Therefore, specific suggestions must be provided at this stage by examining essential features in high dimensions, ensuring that both images adhere to the inverse representations as specified in Eq. (2).

$$\mathfrak{A}_1(t_1) \bullet \mathfrak{B}_1(t_2) \in [\mathfrak{A}_1(t_1) \bullet \mathfrak{B}_1(t_2)]^{-1} \tag{2}$$

2.1.2. Lemma 1

According to inverse metrics, the proof for establishing two image sets can be demonstrated by the inclusion of delta functions, which forecast alterations in each acquired biometric. When delta functions are included, the original form is altered, incorporating solely identity elements as specified in Eq. (3).

$$\mathfrak{A}_1, \mathfrak{B}_1 \rightarrow \delta_i \tag{3}$$

2.2. Sample generation

For each biometric, the input unit must correspond to the representations, and the output units must interpret the data in the appropriate units. Consequently, a mapping connectivity is established for diverse images, thereby producing fresh samples by equilibrating all available units using regularization metrics as specified in Eq. (4).

$$SG_i = min \sum_{i=1}^{n} r_l(i) \times z_i \tag{4}$$

Where,

$r_l(i)$ denotes likelihood of reconstruction.

z_i represents variable for reconstruction.

Eq. (4) establishes that the maximized likelihood for picture reconstructions must be specified for each image set, allowing for the simulation of real-time data in the presence of transformations. Subsequent comprehensive distribution must be conducted in this instance by establishing sample representation prior to reconstruction.

2.2.1. Preliminary 2

The reconstruction possibilities can be determined using log-likelihood functions that are fully constrained by certain factors. Let us examine the preceding approximation functions as $\mathfrak{D}_1 + .. + \mathfrak{D}_i$, where lower limit representations can be established to yield marginal likelihoods under the subsequent condition.

$$\mathfrak{D}_1 + .. + \mathfrak{D}_i \not\subset \mathfrak{E}_l(i) \tag{5}$$

2.2.2. Lemma 2

In mathematical terms, the evidence of establishment for each generated sample can be demonstrated using the divergence theorem. Consequently, the seamless establishment of each distribution unit is essential for facilitating effective reconstructions, wherein marginal values adhere to the boundary under analogous conditions as specified in Eq. (6).

$$\mathfrak{E}_l(i) \triangle \mathfrak{F}_i \tag{6}$$

2.3. Biometric flows

To incorporate biometric patterns, the potential of sinusoidal waves must be examined for different ranges and orientations. Therefore, if the biometrics are supplied within suitable ranges, then equivalent random distributions must be furnished as specified in Eq. (7).

$$BF_i = max \sum_{i=1}^{n} \beta_{in} O_i \tag{7}$$

Where,

β_{in} represents ranges of biometrics.

O_i denotes equivalent orientations.

Eq. (7) suggests that if boundary representations are supplied correctly, ridge patterns can be incorporated, hence enhancing the security of the additional biometrics. The aforementioned ranges and orientations can be applied to all sorts of input units with equal approximations.

2.3.1. Preliminary 3

Let us examine the alterations in each image along linear trajectories, where the input image transitions across the respective ranges and orientations $\mathfrak{G}_I(i,n) \rightarrow \mathfrak{G}_n(i)$. Consequently, perpendicular measurements can be conducted to regulate the evolving patterns by adhering to the restriction in Eq. (8).

$$\mathfrak{G}_I(i,n) \propto \mathfrak{H}_i \tag{8}$$

2.3.2. Lemma 3

The proof of the aforementioned example with boundary constraints can be established by altering the direction from x to y. Consequently, with the perpendicular theorem, an edge point theorem must be articulated with line factors, so signifying entire alterations in the gradient function as stipulated by the condition in Eq. (9).

$$\mathfrak{H}_i \supsetneq \mathfrak{I}_i \tag{9}$$

2.4. Biometric data generation

Data generation from diverse sources necessitates comprehensive recognition through feature transformation metrics, wherein dimensions for each biometric data must be meticulously delineated. Consequently, the data generated at this juncture offers distinct indicators as follows.

$$DG_i = max \sum_{i=1}^{n} \begin{bmatrix} DT_1 & \cdots & DT_i \\ \vdots & \ddots & \vdots \\ DT_i & \cdots & DT_n \end{bmatrix} \lambda_{in} \tag{10}$$

Where,

$\begin{bmatrix} DT_1 & \cdots & DT_i \\ \vdots & \ddots & \vdots \\ DT_i & \cdots & DT_n \end{bmatrix}$ indicates original biometric data matrix.

λ_{in} represents data similarity.

Eq. (10) stipulates that similarity measurements must be lower and original data must be greater to enhance the privacy of biometrics, as distinct tasks for recognition are essential. Furthermore, the augmentation of original data representations enables the processing of biometric mapping through the recognition of all end users.

2.4.1. Preliminary 4

Let us examine the analogous data values represented as $\mathfrak{N}_1 + .. + \mathfrak{N}_i$, which adhere to the probable mapping with $\mathfrak{O}_p$. In this instance, the prior distribution of each biometric unit must be maintained to prevent alterations in the original data values. Therefore, the data production points must adhere to the criterion specified in Eq. (11).

$$\mathfrak{N}_1 + .. + \mathfrak{N}_i \bowtie \mathfrak{O}_p \tag{11}$$

2.4.2. Lemma 4

To demonstrate the separation, a differentiation test must be conducted, allowing each biometric unit, mixed at various time intervals, to be isolated without external interference, hence enhancing data privacy. Therefore, to conduct the differentiation test, the subsequent condition must be specified (Eq. (12)).

$$\mathfrak{O}_p \Vdash \begin{bmatrix} DT_1 & \cdots & DT_i \\ \vdots & \ddots & \vdots \\ DT_i & \cdots & DT_n \end{bmatrix} \tag{12}$$

2.5. Artificial biometrics

Once many biometric indicators are stored, the utilization of artificial biometrics should be minimized, hence enhancing the potential for authentication and privacy. Therefore, it is essential to discover erroneous probability in all listed biometric symbols, referred to as error metrics, as specified in Eq. (13).

$$F_p(i) = min \sum_{i=1}^{n} \aleph_f(i,n)\vartheta_a(i) \tag{13}$$

Where,

$\aleph_f(i,n)$ denotes false identification rates.

$\vartheta_a(i)$ represents incorrect acceptance.

Eq. (13) stipulates that if biometric units are erroneous, they must be promptly removed from associated networks. Furthermore, if inaccurate and low-precision measurements are conducted, overall efficiency will diminish; thus, it is vital to assess authentic attempts.

2.6. Synthetic data distributions

In real-time analysis, each recognized biometric sign in various forms must adhere to statistical parameters, hence ensuring data quality throughout the distribution process. Furthermore, the method of data distribution must remain unauthenticated by other users, hence adhering to the specified patterns outlined in Eq. (14).

$$DD_i = max \sum_{i=1}^{n} OD_i - \Delta D_i \tag{14}$$

Where,

OD_i denotes original data.

ΔD_i represents distributed data.

Eq. (14) demonstrates that the disparity between dispersed and original data yields statistical features, with the whole data set derived from prior reference units. Furthermore, for dispersed data types, the Smirnov test should be taken into account to enhance the quality of data in each test instance.

2.7. Biometric transformations

To facilitate customer service using synthetic data, comprehensive transformations must be executed, involving the scaling and exchange of images. Consequently, these transformations enable each accessible unit to revolve around central points, thereby facilitating the detection of biometric signals with great precision, as demonstrated in Eq. (15).

$$TS_i = min \sum_{i=1}^{n} SF_t - SF_{nt} \tag{15}$$

Where,

SF_t, SF_{nt} represents scaling with transformation and non-transformations.

Eq. (15) indicates that throughout each time period, both transforming and non-transforming biometric symbols are processed, with only essential indications provided at each stage. The existence of noise must be monitored at this stage, as transformations require a longer duration for processing the relevant data.

2.8. Composite objective functions

The aforementioned parametric determinations are evaluated using min-max processes, thereby presenting a multi-objective case study in the suggested technique for biometric indicators. Consequently, individual composite functions are articulated as follows.

$$f_1(x) = max \sum_{i=1}^{n} I_i \tag{16}$$

$$f_2(x) = min \sum_{i=1}^{n} SG_i \tag{17}$$

$$f_3(x) = max \sum_{i=1}^{n} BF_i \tag{18}$$

$$f_4(x) = max \sum_{i=1}^{n} DG_i \tag{19}$$

$$f_5(x) = max \sum_{i=1}^{n} F_p(i) \tag{20}$$

$$f_6(x) = max \sum_{i=1}^{n} DD_i \tag{21}$$

$$f_7(x) = min \sum_{i=1}^{n} TS_i \tag{22}$$

The different composite functions are amalgamated and articulated as total objective functions, as demonstrated in Eq. (23).

$$obj_t = f_1(x) + f_2(x) + f_3(x) + f_4(x) + f_5(x) + f_6(x) + f_7(x) \tag{23}$$

The overall objective functions must be processed utilizing automated principles through explainable artificial intelligence optimization to enhance the efficiency of biometric symbol recognition. A comprehensive description of explainable artificial intelligence is as follows.

3. Explainable artificial intelligence

Explainable artificial intelligence in biometrics is employed to enhance speed, accuracy, and scalability during autonomous operations. In the implementation of explainable artificial intelligence, it is essential to consider two categories of data that pertain to both natural and behavioral aspects. When both features are observed, an increase in transparency is attained, allowing for the rapid identification of each recorded pattern. The primary benefit of transparent operation in biometrics is the ability to accept and store new data patterns for both recognition and verification. As compared to other optimization procedures explainable artificial intelligence provides a clear way for accurate analysis thereby trust in captured signals can be improved. In addition explainable artificial intelligence provides a quick path for identifying errors and it can be diagnosed in a easy way if inaccurate biometric signals are processed. To process data obtained by biometric indicators, explainable artificial intelligence employs four processing steps: feature extraction, input–output mapping, simplification of the biometric signal model, and local interrupt features. Furthermore, in instances of inequitable limits in collected biometrics manifested in many forms, a definitive equilibrium between accuracy and trust is essential in explainable artificial intelligence [20]. The biometric processing system is sent to end users only after meticulous fine-tuning, ensuring precise decision-making as a result of achieving optimal balance circumstances. Moreover, enhanced support is offered through

explainable artificial intelligence following the resolution of identified issues, alongside ongoing advancements facilitated by freshly acquired biometrics with minimal error rates.

3.1. Biometric interpretability model

To generate output from biometric collected signals, a predictive decision model must be integrated with an interpretability model, wherein the significance of feature extraction is processed transparently. The interpretability model will monitor comprehensive alterations in biometric processing pathways and promptly notify these changes to authorized users, enabling timely steps to enhance security. Conversely, the aforementioned scenario demonstrates that interpretability facilitates the straightforward observation of accuracy changes, hence enabling the timely removal of biometric symbols with low accuracy. One of the major advantage of interpretability model is that image set at input units are analyzed in a clear way irrespective of included types thus predictions are directly made at output with successive decision making mechanisms. Further the possibility of using interpretability in artificial intelligence is that the difference between individuals or objects are found by following critical mapping procedures. In the initial state, interpretability monitors and identifies gradual alterations in the examined input patterns, after which these changes are correlated with the original functions where activation segments are supplied. While mapping input and output functions, features such as biometric points or edges with varying degrees are delineated, hence preserving the inherent characteristics of intelligent procedures. Likewise, boundary constraints are taken into account in interpretability models, signifying that specific conventions are derived from internal processing units. Moreover, both sensitivity and interpretability are enhanced in low-complexity artificial intelligence systems, resulting in practical real-time solutions compared to other methods. The mathematical implications of interpretability optimizations are as follows.

3.1.1. Occurrence approximations

It is essential to offer meaningful approximations for all occurrences in biometrics to conserve the substantial amount of symbolic data created during a specific time period. Therefore, an equivalent quantity of approximations must be supplied in this instance by circumventing the intricacies of symbolic units as specified in Eq. (24).

$$OA_i = \sum_{i=1}^{n} \varrho_i \rightarrow \varsigma_i \tag{24}$$

Where,

ϱ_i denotes original biometric units.

ς_i represents equalized approximate units.

Eq. (24) stipulates that within designated time intervals, it is important to furnish indicators with uniform approximations. However, in the event of extended time periods, it becomes challenging to offer localized solutions, since approximations are computed to attain significant complexities due to the proximity of point symbols.

3.1.2. Robust approximations

In explainable artificial intelligence, the potential for symbol detection must converge at a specific point, therefore diminishing the resilience of the predictive model. Consequently, comprehensive approximations with resilience in intricate variations must be minimized, allowing the specified symbol after certain approximations to be simplified as articulated in Eq. (25) as follows.

$$RA_i = \sum_{i=1}^{n} \varpi_i(\mathrm{K}_i - \Upsilon_i) \tag{25}$$

Where,

K_i represents complex model.

Υ_i denotes simplified models.

Eq. (25) demonstrates that the disparity between complicated and equalized approximations yields precise symbolic deviation; hence, appropriate linear models must be fitted, even in the presence of a greater number of symbols. The deviating value must not exceed the crucial symbolic unit; thus, complete fit can be attained in this instance.

3.1.3. Interpretable formations

To measure the interpretable distance with uniform symbolic representations, it is crucial to give a scaling factor; thus, the bandwidth of symbols can be transmitted to the relevant end users for identifying purposes. Therefore, this form of distance measurement must be conducted as delineated in Eq. (26).

$$IF_i = \sum_{i=1}^{n} \zeta_d(i-n) \tag{26}$$

Where,

ζ_d indicates distance variations.

Eq. (26) indicates that, based on the fluctuations in distance between two biometric symbols in the specified forms, the end user can select the optimal representative indicators, so attaining the optimum fit over subsequent time intervals.

Algorithm 1. Biometric interpretability model.

Begin PROCEDURE BIM
  Given
  ϱ_i : Number of original biometric unit
  ς_i: Indicated approximate units
  for i=1:n **do**
    1. OA_i for occurrence approximations at reduced complexities
    2. RA_i for performing robust approximations with simplified models
  end for
  else
  for all i=1:n **do**
    3. IF_i to provide interpretable formations at varying distance
  end for all
end PROCEDURE

The block representations of interpretability optimization are illustrated in Figs. 2 and 3, with the following step indications. The block representation that are indicated in Fig. 2 provides the connectivity on interpretations that are used in explainable artificial intelligence where at initial state original biometric units are observed and only symbolized authentications are provided.

Further only required amount of symbols are transmitted

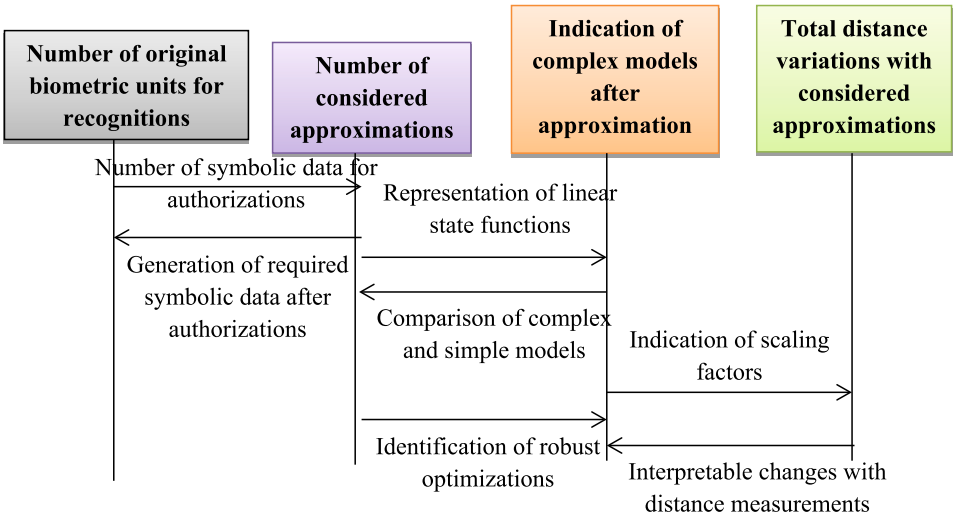

Fig. 2. Block representations of biometric interpretability.

unidentified symbols are removed from the connected systems hence a linear state representation is provided which approximates the complex models. Thereafter due to approximations complex problems are handled in an effective way by using various scaling factors at indicated distance measurements.

3.2. Decision processing units

Alongside the comprehensive interpretability inherent in artificial intelligence techniques, it is essential to analyze each unit for individualized judgments, enabling the attainment of intelligent outputs within anticipated timeframes. Consequently, to make judgments in integrated biometrics, it is essential to amalgamate whole units, thereby maximizing the accuracy of each processing unit. Additionally, for each feature, magnitude indicators are represented with symbols, where absolute values are verified to enhance the security of all specified symbols. In addition to complete interpretability that is present in artificial intelligence technique it is necessary to process each unit for individual decisions where intelligence outcomes can be achieved within expected time periods. Therefore to choose decisions in connected biometrics it is necessary to mix up entire units where accuracy of each processing units are increased to maximum extent. Further for each feature the magnitude indications are made with each symbols where absolute values are checked to improve the security of all indicated symbols. However in decision processing units unified parametric measures are made for each symbol thus individual predictions are provided for each stored symbols. Furthermore, score-based decisions are made as unrecognized symbols introduce complexity and compromise the database in pertinent applications. Each user is permitted to respond to inaccurate biometric symbols, and the process of storing these responses occurs independently of the end users. From the aforementioned scenario, a user can ascertain whether robust decisions can be made regarding input features, hence facilitating the sharing of the database among various user groups. The mathematical depiction of the decision-making process, wherein biometric signals are categorized into distinct user groups, is as follows.

3.2.1. Partial decisive system

To analyze the feature importance system for biometric units, it is crucial to supply partial derivatives for informed decision-making. Therefore, each option in this situation must be elucidated concerning the observation of prospective differences, since the calculative units are of larger significance, as indicated in Eq. (27).

$$DS_i = \sum_{i=1}^{n} CU(i-n) \tag{27}$$

Where,

CU denotes calculative units.

$i-n$ represents the difference with calculative units.

Eq. (27) stipulates that the disparity between each calculative unit must be minimized, as alterations in each biometric symbol should be less significant than the original representations. Consequently, in instances of significant difference patterns, a greater quantity of extraneous biological symbols is present that must be modified prior to processing the subsequent biometric unit.

3.2.2. Sequenced decision

With the provision of synthetic data, judgments can be made based on the available sequence, wherein biometric symbols are seen solely through a split representation. Splitting units introduces additional biometric units, enabling the execution of complex judgments within specified time intervals, as demonstrated in Eq. (28).

$$seq_i = \sum_{i=1}^{n} \eta_i(\iota_1 + .. + \iota_i) \tag{28}$$

Where,

η_i denotes possibility of separation.

$\iota_1 + .. + \iota_i$ represents sequential units.

Eq. (28) suggests that if successive units are segregated, it becomes significantly more challenging to detect the existence of symbols hence, complete user identification is achieved within the stipulated time frame. The aforementioned sequential steps effectively mitigate the risk associated with data represented in multiple formats.

3.2.3. Local indications

Sequence representation indicators for each local unit in biometrics are taken into account, allowing for comprehensive mapping to be executed without external drawbacks. Therefore, the suggested strategy utilizes local signals with distinct scores as specified in Eq. (29).

$$LI_i = \sum_{i=1}^{n} ft_{in} \times pt_f(i) \tag{29}$$

Algorithm 2. Decision processing units.

Begin PROCEDURE DPU
  Given
  CU : Number of cumulative units
  η_i: Possibility of separations
  for i=1:n **do**
    1. DS_i for providing partial decisive systems at required time factors
    2. seq_i for sequenced symbolic units with increased separations
  end for
  else
  for all i=1:n **do**
    3. LI_i for indicating input and feature value representations
  end for all
end PROCEDURE

Where,
ft_{in} denotes input features.
$pt_f(i)$ represents predicted feature values.

Eq. (29) establishes that the ultimate secured decisions will rely on feature indications, necessitating inputs concerning evolving representations. The block representations of interpretability optimization are illustrated in Figs. 4 and 5, with the following step indications. Table 2 provides the definition of variables in proposed system model and optimization algorithms.

4. Results

In this section real time outcomes are discussed for captured biometric units thus complete solutions are provided for increasing security constraints with respect to captured data. Since synthetic data is considered most of the artificial cases are also taken into account thereby appropriate training rates are increased. In order to provide real time outcomes the captured images are defined with actual pixel values where appropriate filters are connected to prevent unauthorized access. Further to avoid complexities both original and corrected cases are considered hence the possibility of appropriate decision making is increased at reduced interpretabilities. Moreover each biometric patterns are arranged in sequential order hence output units are simplified where low complexities are present thereby each sample is generated at particular time period. In addition number of reconstructions are avoided in proposed method as it reduces the security of biometric patterns thus at varying ranges it is possible to achieve equivalent values. The hardware representations are connected by recognizing the finger prints and images by using detection principles that are applied at input units where images are pre-processed. At this state of operation complete training is provided to each image and corresponding models are saved for future use where at later case batch size of biometric units can be increased. Conversely for each saved biometric units the generated patterns are rescaled and target size is increased in order to process sequential order thereby avoiding half characteristic nature. To validate the outcomes it is necessary to consider each parameter therefore in proposed method four scenarios are considered with min-max objective functions and the importance of four scenarios are listed in Table 3.

Scenario 1: Biometric image set and flows.
Scenario 2: Number of data generations.
Scenario 3: Possibility of transformations.
Scenario 4: Distributive data set.

5. Discussions

The real time outcomes that are observed from each hardware interface is converted to equivalent simulation units with representation of parametric units. Hence in this section the discussions are made by considering necessary simulation units that increases the security of captured biometric patterns. Since explainable artificial intelligence is integrated for creating synthetic data a partial decisive mechanism is involved hence sequenced decisions are made with possibility of indicating local units. In order to observe the outcomes with equivalent simulation setup at initial state total number of samples that are used for evaluating biometric patterns are observed with characteristic measurement and conditions involved in environmental cases. Moreover individual structure for each data is provided hence identification process is carried out in presence of correct labelling units.

Table 4 provides the information on simulation parameters that are used for integrating the necessary data units with generation process. Since individual biometric patterns are analyzed it is necessary to provide a visualization framework and to map all biometric patterns in a sequence order. Therefore all original representations can be determined at maximized efficiency and indications can also be made with local model without any interpretations. Additionally two types of approximations are made with original representative values therefore the possibility of robustness can also be reduced at earlier states. Conversely the major challenge on data changing patterns that is considered as major challenge in each real time applications is also solved with proposed method.

5.1. Scenario 1: Biometric image set and flows

In the proposed method, biometric patterns are collected through image representations, necessitating the provision of a collection of units arranged in sequential order. Therefore, the flow patterns of biometric units must be properly defined so that only designated pixel values can be utilized for input units. In all instances, only complete biometric symbols are processed; hence, partial recognition systems are disregarded, resulting in optimized approximations. To analyze the biometric image collection, the maximum pixel values treated with convoluted filters eliminate all extraneous biometric patterns, enabling detection within specific ranges. Additionally, biometric pattern orientations at each level are altered to distinguish them from end users, hence enhancing the privacy of the data kept in the complete database. Random distributions can similarly be generated without disrupting the continuity of biometric patterns, provided that the preceding sequence is sanctioned.

Fig. 6 illustrates the comparing results for the image collection and the recognized flows in biometric patterns. Fig. 6 demonstrates that the suggested method can achieve maximum flow with the input image set, in contrast to the previous methodology. The primary reason for the

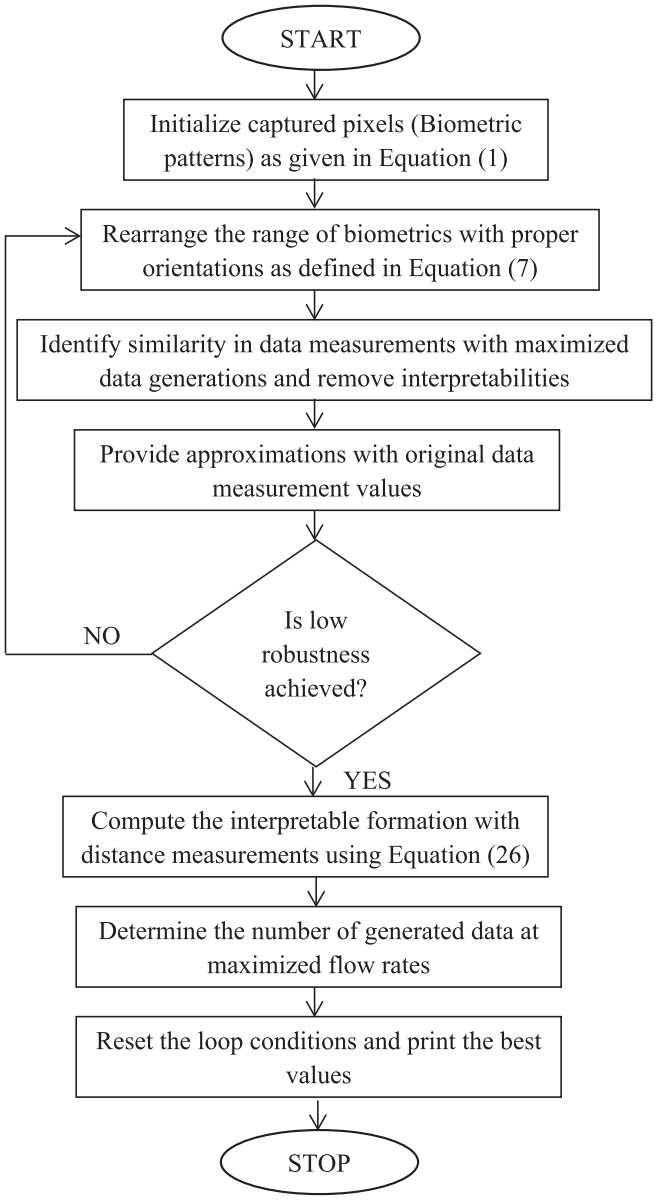

Fig. 3. Flow chart of data generations with interpretable identifications.

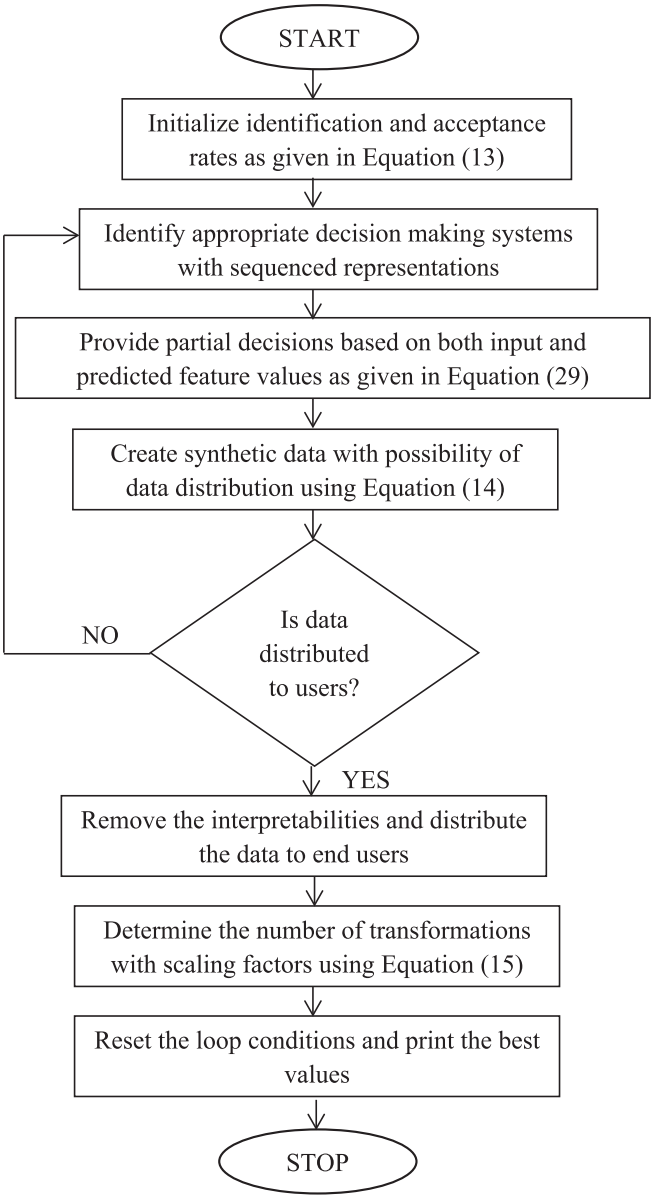

Fig. 5. Flow chart of data distributions and transformations with decisive strategy.

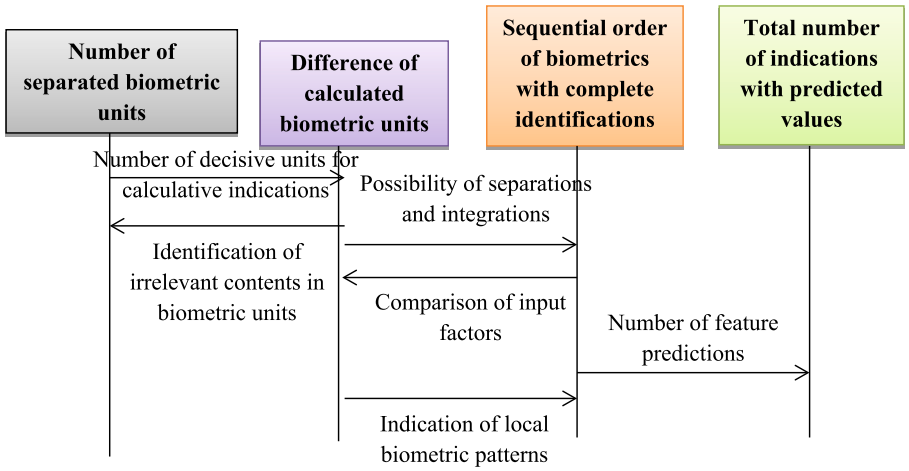

Fig. 4. Block representations of decisive units

Table 2
Description of variables.

Variables	Definition
$P_l(i,n)$	Captured pixel values of biometrics
ρ_i	Indicated filters
$r_l(i)$	Likelihood of reconstruction
z_i	Variable for reconstruction
β_{in}	Ranges of biometrics
O_i	Equivalent orientations
$\begin{bmatrix} DT_1 & \cdots & DT_i \\ \vdots & \ddots & \vdots \\ DT_i & \cdots & DT_n \end{bmatrix}$	Original biometric data matrix
λ_{in}	Data similarity
$\aleph_f(i,n)$	False identification rates
$\vartheta_a(i)$	Incorrect acceptance
OD_i	Original data
ΔD_i	Distributed data
SF_t, SF_{nt}	Scaling with transformation and non-transformations
ϱ_i	Original biometric units
ς_i	Equalized approximate units
K_i	Complex model
Υ_i	Simplified models
ζ_d	Distance variations
CU	Calculative units
$i-n$	Difference with calculative units
η_i	Possibility of separation
$\iota_1 + .. + \iota_i$	Sequential units
ft_{in}	Input features
$pt_f(i)$	Predicted feature values

Table 3
Importance of scenarios.

Scenarios	Significance
Biometric image set and flows	To identify the flow of images at capturing units
Number of data generations	To generate equivalent synthetic data with captured biometric patterns
Possibility of transformations	To transform the patterns in to equivalent representations at reduced robustness
Distributive data set	To distribute each data set to users in appropriate formats

Table 4
Simulation parameters.

Bounds	Requirements
Operating systems	Windows 7 and above
Platform	MATLAB, data generation tools and visualization framework
Version (MATLAB)	2018 and above
Version (Data generation tools)	1.3 and above
Applications	Data creation, observation and accumulation
Implemented data sets	Number of samples, images, reconstructions, interpretabilities, training and testing phases

enhanced flow in the proposed system is that only complete unit representations are permitted, hence eliminating any comparable indications. Furthermore, with explainable artificial intelligence, the generated data is validated, and biometric patterns are systematically organized, referred to as the pre-processing stage in this context. To validate the results, the quantities of collected photos are 23, 26, 31, 37, and 42, corresponding to a singular biometric range of 78, 84, 89, 92, and 97. In the aforementioned image set and biometric patterns, the observed flows for the suggested technique are 59%, 68%, 75%, 84%, and 89%. The current approach results in flow reductions of 36%, 38%, 41%, 44%, and 48%, respectively; hence, even if biometric patterns are processed sequentially, it remains challenging to achieve equal data processing flow.

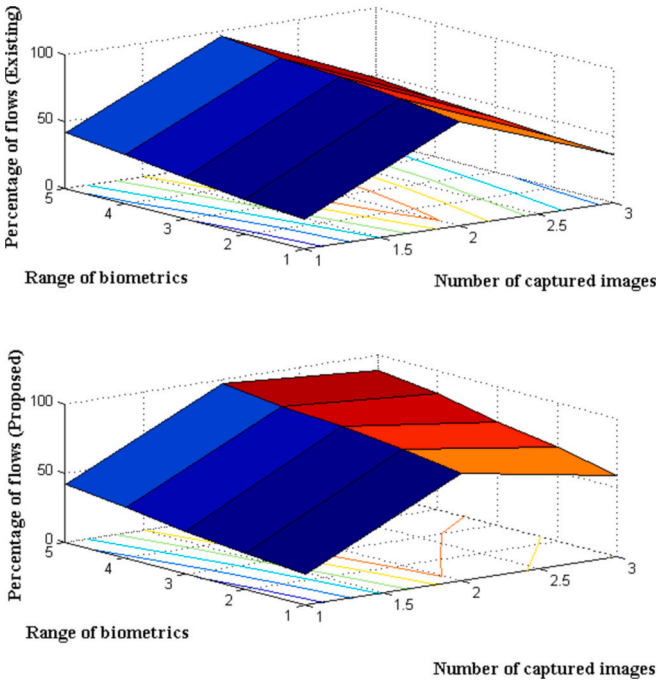

Fig. 6. Maximized flows for proposed and existing approach with varying range of biometric patterns.

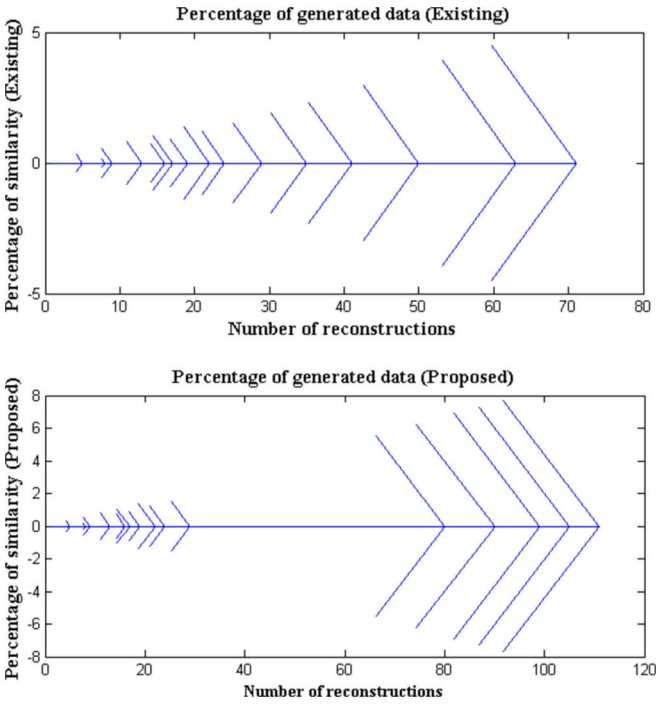

Fig. 7. Number of generated data for similarity rate identifications at reduced reconstruction rate.

5.2. Scenario 2: Number of data generations

This scenario identifies the complete quantity of data that can be artificially generated using collected biometric patterns. Therefore, to ascertain the entire data required for any user request, it is essential to minimize the number of reconstructions at the initial step. In each data processing condition, the likelihood of reconstructions will be significantly elevated due to the lack of regularization measures, as total

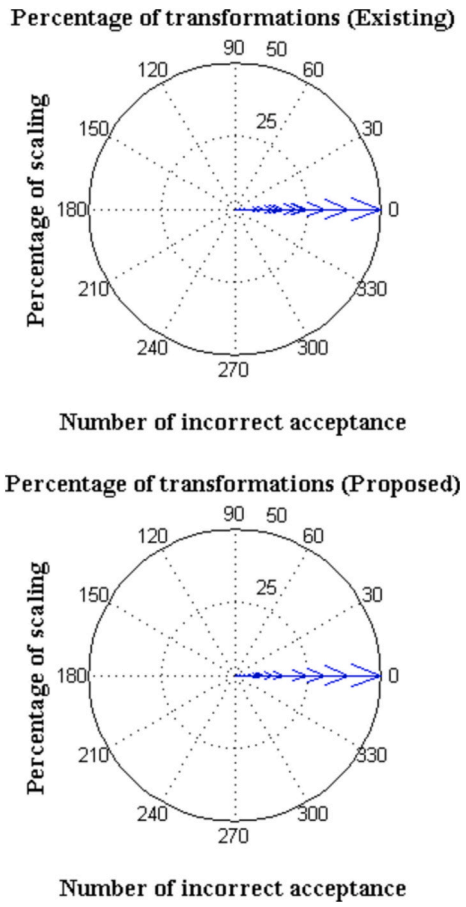

Fig. 8. Scaling factor representations for data transformations and incorrect acceptance.

equilibrium across diverse patterns and data is unattainable. Therefore, it is essential that only pertinent data is collected and securely stored, in contrast to the utilization of extraneous data. Furthermore, the collection of requisite data facilitates the identification of similarities between biometric patterns and datasets, hence diminishing the visibility of conditions to unidentified users. Due to diminished visibility, the synthetic data can be retained within the original data-generated matrix, allowing for partial decisions to be made.

Fig. 7 depicts the quantity of data generated for both the current and suggested methodologies. Fig. 7 demonstrates that the predicted model generates just needed data, in contrast to the existing approach. Essential data generation is contingent upon supplying samples to end users, where specified biometric units are recognized and a sequential order is adhered to for informed decision-making. To validate the results of data production, the number of reconstructions considered are 4, 7, 10, 13, and 17, with similarity indicators at 2%, 9%, 11%, 15%, and 19%. Consequently, for this form of reconstruction, the proportion of created data is observed to be 24%, 29%, 37%, 49%, and 56% in the case of the existing approach [7]. However, the proposed method generates only required data, with maximized generation rates of 69%, 78%, 86%, 91%, and 96%. Consequently, given comprehensive data, equilibrium can be attained, enabling all users to make informed sequential judgments.

5.3. Scenario 3: Possibility of transformations

This scenario examines all potential transformations of biometric patterns to minimize the total number of mistakes at input units. As a greater number of biometric patterns are saved, it becomes feasible to

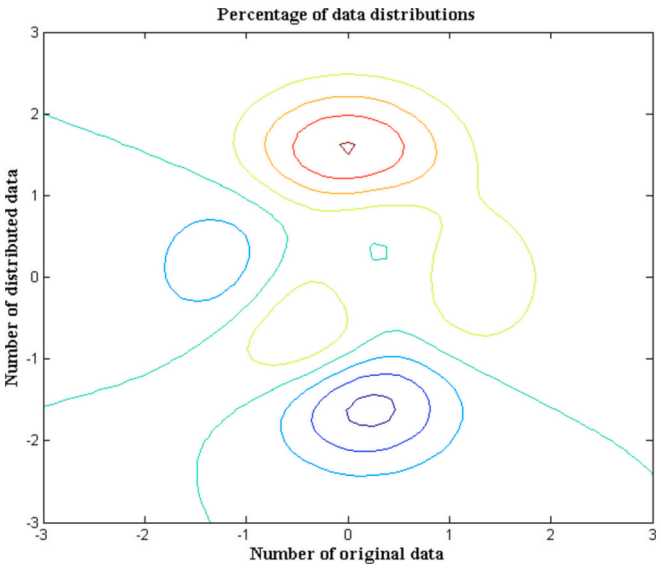

Fig. 9. Distributed data vs. original data representations for changing biometric patterns.

decode the biometric units, allowing for the generation of artificial data corresponding to altered biometric patterns. Consequently, to address the aforementioned issue, the created pattern can be altered using synthetic data, ensuring that unknown users are incapable of decoding any biometric pattern. The changes decrease false acceptance rates, ensuring that only legitimate attempts are performed, hence minimizing inaccuracies in the process. The biometric patterns can be modified using scaling factors, with only projected input values being processed in this scenario, devoid of any equality requirements. This scaling method enhances the stability of input biometric units relative to the original biometric symbols without any changes.

Fig. 8 illustrates the simulation analysis regarding the potential changes in both the proposed and existing methodologies. Fig. 8 indicates that biometric transformations are diminished, resulting in a decrease in artificial biometric units and thereby reducing the erroneous production of biometric patterns for data access. The primary rationale for these reductions in transformations is that uniform approximations are offered at specified time intervals, hence minimizing inaccuracies in detections. The verification of transformation outcomes reveals an inaccurate acceptance count of 17, 25, 31, 39, and 50, corresponding to scaling percentages of 2, 4, 8, 10, and 13. Consequently, in the aforementioned situation, the transformation percentages for the suggested approach are restricted to 9, 6, 4, 2, and 1%, while the transformation percentages for the present approach [7] are 24, 21, 17, 15, and 13%, respectively. Consequently, with few alterations, it is feasible to attain elevated privacy for all examined data.

5.4. Scenario 4: Distributive data set

The generated data set must be disseminated to all end users only following specific authentication procedures. Therefore, in this context, the likelihood of distributions is analyzed to facilitate informed decision-making prior to data transmissions. Initially, the volume of original data will be assessed, and subsequent modifications resulting from data availability will be monitored. Furthermore, for distributions, all interpretabilities are diminished, and solely local models are employed, hence enhancing data privacy. In other instances, data quality is assessed using the Smirnov dataset. The necessity of data distribution must remain separate from recognized patterns, since individual biometric units might be considered, resulting in a sequential decision-making process. Once the data is disseminated, the other user can

develop synthetic data representations that incorporate additional biometric patterns for matching with end users.

Fig. 9 presents a comparative examination of data distributions for both the proposed and existing methodologies. Fig. 9 demonstrates that the suggested strategy maximizes distributive data sets with enhanced security compared to the previous methodology [7]. The primary rationale for attaining optimized distributed data is that the suggested method exhibits a less discrepancy between the original and anticipated data compared to previous approaches, due to the high accuracy of the collected biometric unit. To validate the results of the proposed method, the original dataset comprises 1235, 1789, 2391, 2945, and 3500, whereas the dispersed dataset consists of 768, 1342, 1758, 2367, and 2790. In the original and distributed data scenarios, the outcomes of the suggested method are seen to be 79%, 84%, 88%, 93%, and 96%, while the existing strategy yields percentages of 65%, 68%, 71%, 74%, and 77% for distributed data, respectively.

6. Performance metrics

The performance metrics offer a definitive means of comprehending the biometric acceptance ratio, hence decreasing the risk of erroneous readings in this context. The storage of an increased quantity of biometric patterns allows for performance evaluations of the complete biometric system using artificial data, hence resulting in diminished error rates. Moreover, the performance metric is employed to assess variety, allowing for the observation of comprehensive fluctuations in relation to real-time analysis. Consequently, the subsequent case studies are included to evaluate the efficacy of the proposed strategy.

Case study 1: Robustness characteristics
Case study 2: Space complexity
Case study 3: Time complexity

6.1. Case study 1: Robustness characteristics

This case study assesses the robustness of biometric patterns about variations in repeated values. As the quantity of biometric patterns increases, it is essential to optimize them using original representations, hence eliminating full local interpretations. Initially, it is essential to delineate all metrics pertinent to robustness, including precise indicators, interpretative possibilities, and the quantity of biometric fluctuations. Reducing the aforementioned elements can diminish the resilience of synthetic data; nonetheless, in the proposed method, synthetic noise is introduced to assess overall robustness. The initial criterion for robustness is established just when this type of noise is incorporated into the proposed system. In a similar manner, both testing and training examples are analyzed for robustness features, resulting in modifications during iterations at both points, where total degradation can be noticed.

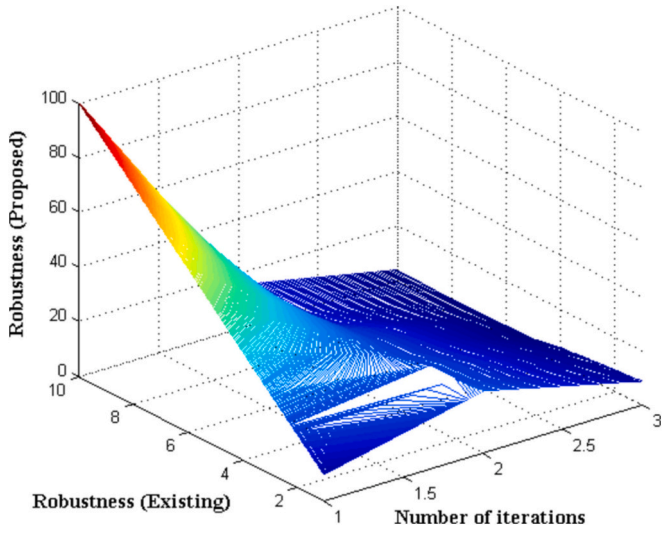

Fig. 10. Comparison of robustness for varying number of iterations.

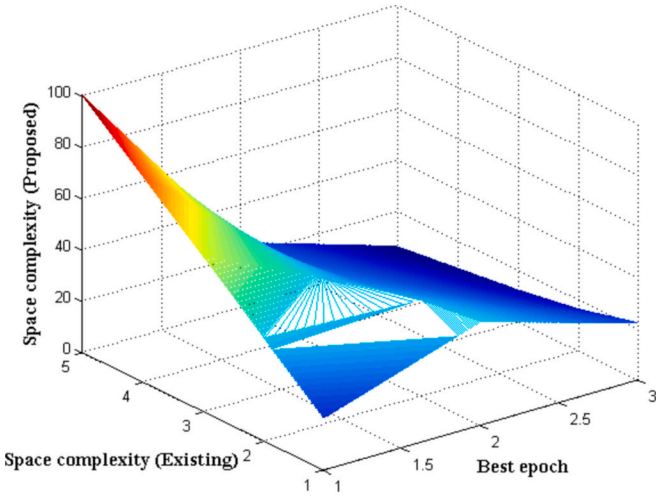

Fig. 11. Space complexity reductions with best epoch conditions.

Fig. 10 presents a comparative examination of robustness between the existing and proposed approaches. Fig. 10 indicates that total robustness is diminished in the planned approach relative to existing models [7]. Due to diminished robustness, the level of security is heightened, allowing the entire biometric system to adapt to changes while enhancing confidence among diverse users. To validate the results of robustness, the number of iterations studied are 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100, during which interpretable forms are progressively diminished until a constant value is attained. In the proposed method, robustness is diminished to 9, 8, 7, 6, and 4, after which constant values are attained; conversely, in the existing approach, robustness persists at 23, 22, 22, 21, 21, 20, 17, and 16, thereafter obtaining constant values. Consequently, when interpretable data forms diminish, it becomes feasible to offer low robustness for all fabricated data at minimal repetitions.

6.2. Case study 2: Space complexity

This case study examines and discusses the complexity representations for the storage of biometric patterns. As each input pattern is associated with image representations, a greater quantity of storage is required, resulting in an increase in the time taken for each input state. Therefore, to diminish complexity, the input pixels for biometric patterns must be minimized; concurrently, the recognition instances must be increased to ensure data privacy is upheld. Furthermore, the computational complexities must be examined in this context, where substantial quantities of intermediate biometric patterns can be retained without failure, hence facilitating feature reduction scenarios. Utilizing the proposed method for data processing results in reduced storage requirements compared to raw data, while simultaneously preserving the dimensionality of the data without alterations.

Fig. 11 depicts the results of space complexity for both the proposed and existing methodologies. Fig. 11 demonstrates that the proposed strategy significantly reduces space complexity in comparison to the existing model. The primary reason for the decrease in complexity is that the suggested method facilitates both training and inference for synthetic data while simultaneously minimizing model size. To validate the results of space complexity, only the optimal epoch is taken into account from the total iterations, with step sizes modified to 20, 40, 60, 80, and 100. Additionally, both peak and average memory capacities are specified to inform users about the quantity of generated biometric patterns

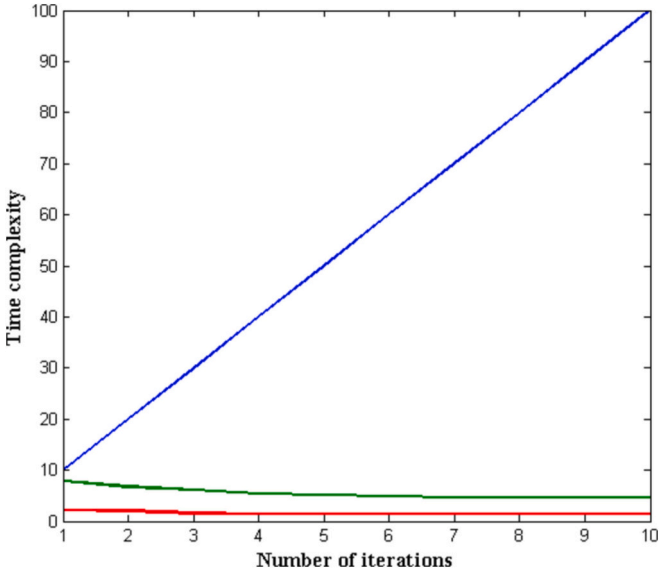

Fig. 12. Comparison of time complexity with changing iteration periods.

and synthetic data. Thus, for the specified era, the suggested method demonstrates a low space complexity of 22%, 16%, 12%, 9%, and 6%, while the present methodology exhibits a space complexity of 40%, 37%, 32%, 28%, and 25%, respectively.

6.3. Case study 3: Time complexity

As more amount of data needs to be processed after recognizing the biometric patterns it is necessary to observe variations in time as complex patterns requires more time for carrying out certain transmissions. In real time whenever the patterns are simple then at the input side it is possible to connect each data transmissions at reduced time period. But in case if the biometric pattern changes and if complex patterns are provided then the time for input unit recognition will be much higher therefore the process of data transmission faces more amount of delay. Moreover the interface units in the process of biometric recognition is highly complex and it is possible to create internal delays as the process of visualization changes with respect to complex time periods. In addition the upper bound of explainable artificial intelligence must be reduced to prevent all complex cases thereby recognizing individual data at corresponding time periods thus it is possible to reduce delays for changing input size patterns.

Fig. 12 illustrates the comparison of time complexity for proposed and existing approaches. From Fig. 12 it is pragmatic that time complexity is reduced in projected approach with explainable artificial intelligence as compared to existing technique that process the data with only learning models that directly provides the task to end users. The major reason for reduced complexity is that same number of biometric operations are reduced that includes different symbols and in case of processing unit if same symbols are recognized then it is completely removed. To verify the outcomes of time complexity total number of iterations are considered as 10,20,30,40,50,60,70,80,90 and 100 where all iteration period corresponds to different complexity metrics. Hence for the above mentioned iterations time complexity is observed to be 7.9,6.7,6.1,5.4,5.1,4.9,4.7 and 4.6 s for existing method whereas in projected approach with explainable artificial intelligence the complexity of biometric pattern recognitions are reduced to 2.2,2,1.6 and 1.4 s respectively. Therefore the complexity remains constant at initial iteration period in proposed model but in existing approach due to learning tasks that are directly connected with output unit it is observe that only after 80th iteration constant observations are reached.

7. Conclusions

The security framework essential for the development and storage of data units exists in many configurations and must remain inaccessible to unauthorized users. The biometric patterns can be supplied with comprehensive recognition, allowing for complete orientation when the input units are processed for data access. The suggested method captures biometric patterns by utilizing diverse image sets and employs texture representations for data access by end users. Upon accessing the biometric patterns, artificial data is generated via explainable artificial intelligence, hence optimizing the conversion of original data. Furthermore, all interpretable formations that hinder access to biometric patterns are monitored by distance representations, hence enabling the provision of comparable decisions at output units. Conversely, additional parametric optimizations are conducted by creating requisite samples, hence minimizing the potential for reconstructions, ensuring that the original biometric patterns remain unaltered. Similarly, the spectrum of biometrics can be expanded to facilitate additional flows, so enabling each user to access requisite data within appropriate time intervals. If the biometric patterns match, comprehensive data will be created, allowing for easier identification of similarity compared to other systems that process data without synthetic input.

To observe the outcomes in real time for considered biometric patterns with synthetic data four scenarios and three case studies are implemented. For all scenarios a real time (equivalent) simulation setup is considered where for maximum number of captured images percentage of flows are increased to 89% in proposed approach. Similarly for subsequent scenarios due to reduced reconstructions percentage of generated data is increased to 96% and additionally with the number of incorrect processing systems number of data transmission is minimized to 1% which makes 96% of data to be distributed with correct patterns. In future the proposed method can be extended with advanced data generation techniques by following mitigation strategies where cross domain transferability will be provided.

7.1. Policy implications

In various industries the data analytics plays an important role by introducing privacy preserving innovations where all regulatory and ethical policies must be followed in securing more amount of data. Moreover in real time the industries can train all critical data with synthetic data representations as artificial intelligence technique is involved without any risk to exposure of data that is present in various application platforms.

CRediT authorship contribution statement

Achyut Shankar: Formal analysis, Data curation, Conceptualization. **Hariprasath Manoharan:** Writing – review & editing, Writing – original draft, Supervision, Project administration. **Adil O. Khadidos:** Visualization, Validation, Software, Resources. **Alaa O. Khadidos:** Visualization, Validation, Software, Resources. **Shitharth Selvarajan:** Writing – review & editing, Writing – original draft, Supervision, Project administration. **S.B. Goyal:** Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. (GPIP: 958-611-2024). The authors, therefore, acknowledge with thanks DSR for technical and financial support.

Data availability

Data will be made available on request.

References

[1] M. Stippinger, D. Hanák, M.T. Kurbucz, G. Hanczár, O.M. Törteli, Z. Somogyvári, BiometricBlender: ultra-high dimensional, multi-class synthetic data generator to imitate biometric feature space, SoftwareX 22 (2023) 101366, https://doi.org/10.1016/j.softx.2023.101366.

[2] A. Makrushin, V.S. Mannam, J. Dittmann, Privacy-friendly datasets of synthetic fingerprints for evaluation of biometric algorithms, Appl. Sci. 13 (2023), https://doi.org/10.3390/app131810000.

[3] E. Blümel, M. Schulz, R. Breithaupt, N. Jung, R. Lange, Enhancing resilience in biometric research: generation of 3D synthetic face data using advanced 3D character creation techniques from high-fidelity video games and animation, Sensors 24 (2024), https://doi.org/10.3390/s24092750.

[4] J. Jenkins, K. Roy, Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study, Discov. Artif. Intell. 4 (2024), https://doi.org/10.1007/s44163-024-00138-z.

[5] S. James, C. Harbron, J. Branson, M. Sundler, Synthetic data use: exploring use cases to optimise data utility, Discov. Artif. Intell. 1 (2021), https://doi.org/10.1007/s44163-021-00016-y.

[6] S. Selvarajan, H. Manoharan, A.O. Khadidos, A.O. Khadidos, A. Shankar, C. Maple, S. Singh, Generative artificial intelligence and adversarial network for fraud detections in current evolutional systems, Expert. Syst. (2024) 1–25, https://doi.org/10.1111/exsy.13740.

[7] S. Selvarajan, H. Manoharan, A. Shankar, A.O. Khadidos, A.O. Khadidos, A. Galletta, PUDT: plummeting uncertainties in digital twins for aerospace applications using deep learning algorithms, Futur. Gener. Comput. Syst. 153 (2024) 575–586, https://doi.org/10.1016/j.future.2023.11.034.

[8] S.S. Gornale, S. Kumar, A. Patil, P.S. Hiremath, Behavioral biometric data analysis for gender classification using feature fusion and machine learning, Front. Robot. AI. 8 (2021) 1–9, https://doi.org/10.3389/frobt.2021.685966.

[9] B.N. Jacobsen, Machine learning and the politics of synthetic data, Big Data Soc. 10 (2023), https://doi.org/10.1177/20539517221145372.

[10] T. Gu, J.M.G. Taylor, B. Mukherjee, A synthetic data integration framework to leverage external summary-level information from heterogeneous populations, Biometrics 79 (2023) 3831–3845, https://doi.org/10.1111/biom.13852.

[11] M. Meiser, I. Zinnikus, A survey on the use of synthetic data for enhancing key aspects of trustworthy AI in the energy domain: challenges and opportunities, Energies 17 (2024), https://doi.org/10.3390/en17091992.

[12] J.J. Bird, A. Lotfi, CIFAKE: image classification and explainable identification of AI-generated synthetic images, IEEE Access. 12 (2024) 15642–15650, https://doi.org/10.1109/ACCESS.2024.3356122.

[13] A. Singh, A. Arora, A. Nigam, Cancelable Iris template generation by aggregating patch level ordinal relations with its holistically extended performance and security analysis, Image Vis. Comput. 104 (2020) 104017, https://doi.org/10.1016/j.imavis.2020.104017.

[14] H.O. Shahreza, S. Marcel, Inversion of deep facial templates using synthetic data, 2023 IEEE Int. Jt. Conf. Biometrics, IJCB 2023 (2023) 1–8, https://doi.org/10.1109/IJCB57857.2023.10449033.

[15] A. Makrushin, C. Kauba, S. Kirchgasser, S. Seidlitz, C. Kraetzer, A. Uhl, J. Dittmann, General requirements on synthetic fingerprint images for biometric authentication and forensic investigations, in: IH MMSec 2021 - Proc. 2021 ACM Work. Inf. Hiding Multimed. Secur, 2021, pp. 93–104, https://doi.org/10.1145/3437880.3460410.

[16] B. Mieth, A. Rozier, J.A. Rodriguez, M.M.C. Höhne, N. Görnitz, K.R. Müller, DeepCOMBI: explainable artificial intelligence for the analysis and discovery in genome-wide association studies, NAR Genom. Bioinforma. 3 (2021) 1–21, https://doi.org/10.1093/nargab/lqab065.

[17] Z. Xiang, Z. Huang, K. Khoshelham, Synthetic lidar point cloud generation using deep generative models for improved driving scene object recognition, Image Vis. Comput. 150 (2024) 105207, https://doi.org/10.1016/j.imavis.2024.105207.

[18] A. Kerim, U. Celikcan, E. Erdem, A. Erdem, Using synthetic data for person tracking under adverse weather conditions, Image Vis. Comput. 111 (2021) 104187, https://doi.org/10.1016/j.imavis.2021.104187.

[19] L. Cascone, C. Pero, H. Proença, Visual and textual explainability for a biometric verification system based on piecewise facial attribute analysis, Image Vis. Comput. 132 (2023), https://doi.org/10.1016/j.imavis.2023.104645.

[20] J.M. Górriz, I, et al., Computational approaches to explainable artificial intelligence: advances in theory, applications and trends, Inf. Fusion. 100 (2023) 101945, https://doi.org/10.1016/j.inffus.2023.101945.