IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal of New Materials for Electrochemical Systems
Vol. 27, No. 4, December 2024, pp. 301-313
Journal homepage: http://iieta.org/journals/jnmes

A KCP-DCNN Multimodal Biosensor Authentication Device with Two-Step Verification and QR Code Falsification

Jananee Vinayagam*, Golda Dilip

Department of Computer Science and Engineering, SRM Institute of Science & Technology Vadapalani Campus, Vadapalani, Chennai, Tamil Nadu 600026, India

Corresponding Author Email: jv9579@srmist.edu.in

https://doi.org/10.14447/jnmes.v27i4.a02

Received: March 15-2024
Accepted: December 18-2024

Keywords:
Biosensor,
Z-Score-based,
(GAN)Generative Adversarial Networks,
FDivergence AdaFactor
Snake Active Contour Model

ABSTRACT

Multi-biometric authentication systems have become a viable way to improve authentication performance in the current digital era. Several multi-biometric authentication studies have been carried out and published in the literature. The difficulties of separating real biometric information from fraudulent attempts and integrating biometric and non-biometric authentication methods in a "Deep Convolutional Neural Network (KCP-DCNN)" that makes use of Kernel Correlation Padding are highlighted in this paper. An efficient multimodal Biometric Authentication (BA) system that integrates fingerprint, signature, and face modalities is presented in the study. To get ready for picture improvement, the input images are first pre-processed using the "Radial Basis Function-centric Pixel Replication Technique (RBF-PRT)". This procedure uses" Log Z-Score-centric Generative Adversarial Networks (LZS-GAN)" to apply blurring, augmentation, and noise reduction techniques to improve the visual quality of photographs. Following this, Dlib's 68-point facial landmark extraction is performed using the enlarged signature, fingerprint, and enhanced face photos. Using a generative adversarial network (GAN) that generates new images using log Z-scores as feature representations, a Chaincode-centric method is used for minutia extraction. This is then used in the" FDivergence AdaFactor-centric Snake Active Contour Model (FDAF-SACM)" for contour extraction. Key features are then retrieved using KCP-DCNN for efficient classification. The user is authenticated if the categorization output is accurate after the Quick Response (QR) code produced from the retrieved points has been confirmed. A user identification recognition accuracy of 98.181% is attained by the created model. In order to improve the "Multimodal Biometric" (MB) system's authentication rate, the suggested approach makes use of a biosensor.

1. INTRODUCTION

One of the best methods for identifying and authenticating people based on their distinct biological characteristics is biometric identification using biosensors. Unimodal systems were widely utilized in biometrics in the past, but multibiometric (MB) systems are becoming more and more popular among academics. By collecting a variety of traits like fingerprints, face features, and iris patterns, MB systems are essential in offering security, affordability, precision, and dependability for speedy identification verification. Since a multibiometric authentication system uses several facets of an individual's identification, it is superior than conventional password-based techniques. This method lowers the possibility of spoofing attacks by making it more difficult for attackers to duplicate a number of biometric traits.

In order to prepare for their eventual broad use, numerous biometric services are currently being created and tested. Biometrics that have undergone multiple steps, such as preprocessing, feature detection, machine learning with extracted features, deep learning without feature engineering, and biosensor feature engineering, are the subject of numerous research articles. Because of their great accuracy in this area, neural networks are frequently used in computational approaches for recognition. Applications frequently demonstrate how scenario-based deep learning techniques enhance authentication performance when identifying the distinctive characteristics of each user. These approaches, however, typically overlook possible security issues brought up by the fusion process.

One major concern with neural networks is the risk of adversarial attacks, which use specially crafted input samples to trick the network into misclassifying data. These attacks take advantage of the network's learned non-linear decision boundaries, making them susceptible to minor input changes. This vulnerability raises important questions about the reliability and security of neural networks in critical areas like autonomous driving and medical diagnosis. Additionally, another challenge with neural networks is the potential for biases in training datasets. Demographic disparities related to biases can result in underrepresented or minority groups performing poorly. This issue has been observed in various applications, including facial recognition and criminal justice predictions.

Human physiological or behavioral biometrics were used in previous studies for identification or validation [9]. Whereas psychological biometrics deal with the internal signals generated by the human body that can be recorded by biosensors, behavioral biometrics deals with the distinct patterns of conduct that people form as a result of their deeply rooted habits [10]. However, these systems are limited since they only use readily created template data that is supplied during the authentication procedure. Interestingly, since physiological biometric traits—like fingerprints and faces—cannot be altered, updating the security system becomes impossible if an adversary manages to obtain them [11]. While extensive research has been done on the fusion of MBs, no

work has yet developed an effective method for combining biometrics and non biometrics for safe authentication.

The information that follows is a list of some of the disadvantages of current research approaches. Because security issues were ignored, the studies that were in place did not handle BA in the direction of combining biometric and nonbiometric features. Fingerprint-centric extraction feature techniques produce blurred features because of the input image's complexity and poor picture quality. BA depends on the "Artificial biometrics" that can be created based on the biometric template data provided during authentication.
It was a laborious procedure because localizing the optimal feature vector with an optimization technique required additional rounds.

The symmetric key encryption technique used by the present biometric system to encrypt features leaves it open to security flaws. Hash-based message authentication code (HMAC), which blends symmetric key cryptography and hash functions, is another alternate encryption method. This method hashes a message using a hash function and then encrypts the hash value using a symmetric key. This technique provides a secure and efficient way to confirm communications and halt tampering. Although symmetric key cryptography is widely used due to its simplicity and efficacy, a few systemic vulnerabilities could compromise security. By addressing the issues with key management and brute force attacks related to symmetric key cryptography, two alternative encryption methods that increase security are asymmetric key cryptography and HMAC.

The MB System Insufficient Motivation Offers Novelties:
• To increase overall efficiency, the proposed method integrates biometric and non-biometric authentication features.
• To prevent the creation of phony biometrics, the system employs a dual-step verification process.
Two techniques are utilized to extract accurate features: contrast enhancement through "contrast limited adaptive histogram equalization (CLAHE)" and minutia extraction via the chain code method. The CLAHE technique addresses the contrast enhancement issue, while the chain code method tackles rotation and scaling invariance by encoding an object's contour with a series of directional vectors. Additionally, the RBF-PRT technique resolves path planning and motion planning challenges by using radial basis function nodes to represent different regions of the image. By applying the RBF-PRT technique for image magnification, it becomes easier and faster to extract patterns of unique biometric traits, thereby accelerating the localization of feature vectors. Security vulnerabilities related to biometric attributes are mitigated through QR code generation and matrix transformation.
Forecoming Subdivision are represented as

Sub Division 2 BA Multimodal System Detailed Study,
Sub Division 3 Brief BA Proposed System,
Sub Division 4 Data Set Testing and Report Generation,
Sub Division 5: Analysis and Future Enhancement.

RELATED LITERATURE SURVEY

"Vhaduri et al. [12] explored the Hierarchical Implicit Authentication Model (HIAuth)", which combines heart rate, movement, and breathing biometrics as audio-based signals. The system utilized multiple classifiers along with a two-step feature selection process to authenticate users. Their comprehensive analysis yielded an F1 score, an actual rejection rate, and an average accuracy. The findings indicated that this technology could be applicable in the wearable industry. However, the model's performance was not as strong when independent biometric data were utilized. To develop 2 MB systems, Singh & Tiwari integrated unimodal sclera, ECG, and fingerprint-centric models.

Each unimodal system performed preprocessing, matching, feature extraction, both decision and score-level fusion methods for authentication [13].

According to the data, the system's" True Positive Rate (TPR)" and "False Positive Rate (FPR) " accuracy rates were the highest. However, the feature descriptors' low discrimination power and volatility affected the model's performance. A multimodal, multi-agent passenger authentication system that makes use of both fingerprint and face photographs was developed by Thenuwara et al. The gathered photos were mostly preprocessed before being employed as multiclassifiers acting as multiagents for authentication. Integrating the Multi-Agent System (MAS) negotiation with the confidence levels from different classifiers allowed for authentication. "The experimental results showed that the model outperformed previous models in the authentication process and was computationally efficient. Furthermore, the model did not evaluate biometric data security. Using biometric fingerprint and iris data, Tran et al. created a lightweight biometric authentication system that makes use of artificial intelligence (AI)." A composite feature was created in order to train the recognition model and verify the user's identification. The hash values were developed in order to preserve the biometric data's anonymity. The model's performance was encouraging. The hash function selection, however, affected recognition performance because a poorly chosen bit string slowed down the pattern-matching procedure. An ABA process that made use of an air signature verification method was presented by Behera et al. [16]. As the user signed in midair, this required recording their movements and thought processes. The "Random Forest (RF)" and "Hidden Markov Model" (HMM) classifiers were trained using features that were taken from the recorded data. In comparison to current techniques, experiments showed that the verification accuracy was increased and the "false positive rates (FPRs)" were considerably reduced. Although the model was capable of processing large amounts of data, it was not very quick. Joseph et al. investigated a multimodal biometric authentication approach that integrated fingerprint, palm print, and iris features in a cloud setting [17]. For every trait, the system used image processing methods such feature extraction, normalization, and preprocessing. To improve access control and data protection in the cloud environment, the characteristic points from each attribute were combined to create a secret key for authentication. Unfortunately, because all inputs were subjected to the same hash algorithm, the model's security was insufficient.

Purohit and Ajmera investigated biometric modalities such the palm, fingerprint, and ear for authentication [18]. "Oppositional Gray Wolf Optimization" (OGWO) was utilized to choose key features after features were extracted from each modality in order to achieve the optimal feature level fusion.

A Multi-Kernel Support Vector Machine (MKSVM) "was used for recognition. Although the approach produced improved results, it was susceptible to producing inaccurate

results due to its inability to learn from every image position. "El-Rahiem et al. developed a multimodal BA model using an electrocardiogram (ECG) and a finger vein [19]. The biometric data was pre-processed by the system using filtering techniques, and features were extracted using a deep convolution neural network (DCNN)."
Four machine learning classifiers were used for authentication by combining the feature points. The experiment's findings demonstrated an improvement in authentication effectiveness. The technology took longer to authenticate users initially, though.

The multimodal biometric identification approach used by Goh et al. [20] makes use of fingerprint, iris, finger vein, and facial biometric modalities. During the matching phase, this method entailed merging features and removing alignment problems. They used Index of Max (IoM) hashing to guarantee the security of biometric data. According to experimental findings, this procedure outperformed baseline approaches. However, the system's performance may be imprecise if each class is modeled using a large number of training samples. A multimodal biometric system that emphasizes arm and ear movements was created by Cherifi et al. [21].

Here, the modalities' characteristics were extracted using statistical metrics and local phase quantization (LPQ), and score-level fusion for authentication was achieved using a weighted sum. According to the results, the model demonstrated an improvement in equal error rate (EER); however, the system's accuracy was insufficient because the input images' quality was acceptable.

With BA systems, some classifiers and algorithms could work better than others. For example, decision trees assist identify the most crucial elements for reaching a certain result, making them ideal for forecasting and decision-making in BA systems. Another advantage of random forests is that they have a lower chance of overfitting. Individual decision trees are perfect for Bayesian analytic systems since they are especially helpful in managing complicated and noisy data. Furthermore, the ability of support vector machines (SVMs) to efficiently handle high-dimensional data—particularly when the number of features surpasses the number of samples—makes them essential components of Bayesian Analytics (BA) systems.

For Bayesian analytic systems, gradient boosting is especially advantageous because it can produce positive outcomes even when handling noisy data and missing values. In situations where the data is excessively skewed, noisy, or incomplete, it nevertheless works well. Because neural networks operate well with high-dimensional data and can manage intricate and nonlinear connections between input and output variables, they are particularly beneficial for Bayesian accounting systems. Systems that need to analyze massive amounts of data accurately are best suited for them. Before selecting a choice, it is crucial to thoroughly assess how well each algorithm performs on a particular dataset.

3.1 A PROPOSED SYSTEM FOR MULTIMODAL BIOMETRIC AUTHENTICATION

Improving performance is essential to overcoming constraints with regard to accuracy, robustness, and susceptibility to spoofing attacks in order to develop a trustworthy and secure authentication system. The many biometric characteristics of the user should therefore be included in an efficient biometric authentication system. Figure 1 shows the general flow of the proposed Biosensor method.

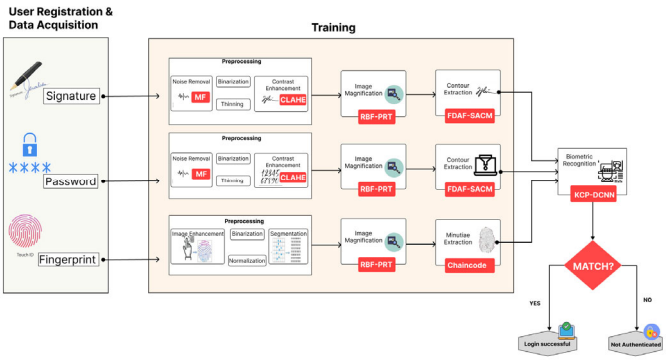


Figure 1. The projected multimodal biometric identification system's architecture

3.1 Enrolling Users and Compiling Information

During the system's registration process, users have the option to choose from three different types of biometric modalities, such as fingerprint, and provide their information, signature, and facial recognition data for authentication.

$$\Im_{m(i,j)} = \frac{L-1}{N} \sum_{k=1 to n} \partial_{m(i,j)} (U) \quad (1)$$

$\Im_{m(i,j)}$number of users is signified as U
$(\Im_{CE(FP,S,F)})$ referred as Registration center

3.2 Training Module

Initial step of User Registration process, the training of the user model should be adequately prepared for the verification process. Consequently, Biometric data train the recognition system in the following sections.
$\Im_{Bin(FP,S)} = \nabla_{binarize}(\Im_{CE(FP,S)})$collected at the user registration stage.

3.2.1 Pre-processing

The input photographs undergo pre-processing to generate unique patterns before they are utilized in the verification process. The methods used for preprocessing are detailed below.To eliminate the" salt-and-pepper noise" from the input photos, noise removal is used. The ∇_binarize technique is applied while minimizing the median filter's loss of important features. In order to successfully reduce noise, this median filter scans the image pixel by pixel, substituting the median value of each pixel with the values of the surrounding pixels from other categories. As a result, the images without noise $\Im_{Bin(FP,S)}$are acquired as,

$$\Im_{T(FP,S)} = \nabla_{Thin}(\Im_{Bin(FP,S)}) \quad (2)$$

The pixel at a given position acts as the median operator in this scenario. $\Im_{T(FP,S)}$in$(\Im_{T(FP,S)})$ is depicted in a way as $(\Im_{CE(F)})$ and $(\Im_{T(FP,S)})$ The coordinates represent the median values. Contrast Enhancement:

The "CLAHE" technique enhances the contrast of the noise-removed images.
$(\Im_{mag(FP,S)})$.

Histogram equalization is first applied after the image has been divided into smaller portions called tiles. This procedure

computes the histogram for every tile and controls the contrast using a clip limit.

If $(2wd-1)\times(2ht-1)$ is the histogram of $(\Im_{T(FP,S)})$ tile in$(wd\times ht)$, $(\Im_{bin(FP,S)})$ the clip limit is computed by,

$$\Im_{bin(FP,S)}=\begin{cases}1if\left(\beta<\Im_{T(FP,S)}(ii,jj)\right)\\0otherwise\end{cases},ii\to wd-1,jj\to ht-1 \quad (3)$$

Here, β represents the clip factor (ranging from 0 to 256), while $(\Im_{mag(n)})$ denotes the number of pixels and grey scales, and (2×2) indicates the maximum slope value. The surplus is trimmed and redistributed for each histogram that exceeds the clip limit. The "cumulative distribution function (CDF) "is computed after the distribution, and the "estimated CDF" is then scaled in accordance with the grayscale mapping. The following is the mapping equation.

$$\Im_{mag(FP,S)}=\sum_{n=0to255}(\Im_{mag(n)}). \quad (4)$$

The resulting tile after greyscale mapping is represented as (3×3), which corresponds to the pixel values of the mapping input image. Ultimately, the images produced exhibit improved contrast due to the interpolation of the generated tiles.

For binarization and thinning, just the "fingerprint and signature photos" are used. A black-and-white image with pixel values of 0 and 1 is produced by binarization. This can be given as $\left(UD(i,j)_{\Im_{mag(FP,S)}}\right)$ (5)

Binarize imaging technique is illustrated as follows.

$$UD(i,j)_{\Im_{mag(FP,S)}}=\begin{cases}min((i,j)_{hor})\,if\big((i,j)\in horizontal\big)\\min((i,j)_{ver})\,if\big((i,j)\in vertical\big)\\RBF\big((i,j)_{hor,ver}\big)if\big((i,j)\in central\big)\end{cases},$$

$$RBF\big((i,j)_{hor,ver}\big)=\Phi\left\|(i,j)_{hor,ver}-(i,j)_{central}\right\|.$$

Signified Binarized Output Images

Thinning is the technique used to simplify an image by eliminating contour points that are not essential to the skeleton. This process can be performed in various ways.

$$(i,j)\in horizontal \quad (6)$$

The final skeleton image following the thinning process is represented as (i,j) ∈central, whereas the technique for creating the skeletonized picture is explained above as (i,j) ∈vertical. After preprocessing, the face images (i,j)_ver are improved for different poses, and the fingerprint and signature images (i,j)_hor are magnified.

3.2.2 Image Magnification

Increasing the spatial resolution of previously processed images is the aim of picture magnification. Details in the photos can be seen more clearly thanks to this method. In this procedure, the Radial Basis Function-based PRT (RBF-PRT) is used. The PRT technique was chosen since it is easy to use when enlarging photos. Using minimum and maximum undefined central pixels for magnification, however, might lead to a significant mistake rate and extremely ambiguous results. Thus, in the conventional PRT framework, the magnification process incorporates the radial basis function."RBF-PRT" aims to create a zoomed image "RBF"

((i,j)_(hor,ver)) with a resolution of Φ for a given image $(\Im_{T(FP,S)})$ of $(\Im_{mag(FP,S)})$ resolution. To generate the enlarged images, "RBF-PRT" needs to estimate values for the new pixels that are created during the zooming process. Initially, the input images are threshold to produce a range of binary images $(\Im_{T(FP,S)})$ using binary decomposition.

$$2^4=16 \quad (7)$$

Here, the threshold parameter with values$(i<i_{max}())$ is given as $\left(\beta<\Im_{T(FP,S)}(i,j)\right)$.

The binary images are magnified to create a magnified image $\Im_{T(FP,S)}(i,j)=1$, dividing the image into distinct sections using the binary pattern interpolation method. In this approach, $\Im_{T(FP,S)}(i,j)=0$ represents patches, each containing 16 patterns. These (2×2) patches are then interpolated into high-resolution binary patterns while $\left(UD(i,j)_{\Im_{mag(FP,S)}}\right)$ preserving the accurate geometric shapes they represent.

$$\Im_{mag(FP,S)} \quad (8)$$

Thus, the final zoomed high-resolution image is drastically obtained as the sum of interpolated 256 high-resolution binary images.

$$(i,j)\in hor \quad (9)$$

The magnified images contain pixel values that are difficult to define, represented as (i,j)=min (i,j)_hor, and are combined with the known neighboring pixels.

$$(i,j)\in ver \quad (10)$$

$$(i,j)=min\quad(i,j)_{ver} \quad (11)$$

In this context, the undefined horizontal,central, vertical pixels are replaced with the neighboring pixels, where the horizontal direction is represented as

(i,j) ∈central,

the vertical direction is defined by "RBF ((i,j)_(hor,ver))", and both horizontal and vertical directions are denoted as $\Im_{mag(FP,S)}$ The terms $(\Im_{mag(FP,S)})$,$(\Im_{CE(F)})$ and $(\Re_G)$,$(\Re_D)$ refer to the radial basis function used to compute the central pixels, while the radial kernel is represented as $(\Im_{CE(F)})$. The zooming process that employs "RBF-PRT" is detailed in Algorithm 1.

Algorithm 1: Image magnification using RBF-PRT

"Input: Pre-processed images $(\Im_{tar(F)})$"

"Output: Magnified images $\left(\Im_{\Re_G(F)}(\alpha)\right)$"

Begin

Initialize input images$(\Im_{CE(F)})$, number of patterns $(\Im_{tar(F)})$

While$(\Re_G)$

Perform binary decomposition

If (α)

$\left(\aleph_\alpha(\alpha)\right)$

Else

$\left(\Im_{\Re_G(F)}(\alpha)\right)$

End if

"Extract $\left(\Im_{\Re_G(F)}(\alpha)\right)$patches

Perform binary interpolation

Sum each of 256 binary images.

For each $(\Im_{CE(F)})$in$\left(\aleph_\Im(\Im_{CE(F)})\right)$"

If $\lambda\left(\Re_G,\wp_G\right)=D_{\Im_{CE(F)}\sim\left(\aleph_\Im(\Im_{CE(F)})\right),\alpha\sim\aleph_\alpha(\alpha)}\left[-log\left(\Re_D\left(\Im_{\Re_G(F)}(\alpha),\Im_{tar(F)}\right)\right)\right]$

$$\alpha =$$

$$log\left(\frac{\aleph_{\Im}(\Im_{CE(F)})-\mu}{\phi}\right)$$

Otherwiseμ

ϕ

Otherwise.$\left(\Im_{CE(F)}\right)$

$\left(\Im_{\Re_G(F)}(\alpha)\right)$

End if

End

End while

Return $\lambda(\Re_D, \wp_D) =$

$$-D_{\Im_{CE(F)}\sim\left(\aleph_{\Im}(\Im_{CE(F)})\right)}\left[log\left(\Im_{\Re_D(F)}\right)\right]$$

$$-D_{\alpha\sim\aleph_\alpha(\alpha)}\left[log\left(1-\Re_D\left(\Im_{\Re_G(F)}(\alpha)\right),\Im_{tar(F)}\right)\right]$$

End

The final high-resolution image is used to extract distinctive patterns from the fingerprint and signature images, including contour points and minutiae points.

$\left(\wp_G, \wp_D\right)$

3.2.3 Efficient Augmentation

The preprocessed face images $D_{\Im_{CE(F)}\sim\left(\aleph_{\Im}(\Im_{CE(F)})\right)}$ are improved to generate different facial poses using "LZS − GAN". "A Generative Adversarial Network (GAN)"

The "LZS-GAN" consists of two neural networks: the functional "generator D (α~ℵ_α (α)) "and the discriminator ƛ. These networks operate within a two-player min-max game framework, utilizing a specific loss function. Let$\Im_{Aug(F)} = \underset{\Re_G}{min}\underset{\Re_G}{max}D_{\Im_{CE(F)}\sim\left(\aleph_{\Im}(\Im_{CE(F)})\right)}\, log\left(\Im_{\Re_D(F)}\right)$ $+D_{\alpha\sim\aleph_\alpha(\alpha)}\left[log\left(1-\Re_D\left(\Im_{\Re_G(F)}(\alpha),\Im_{tar(F)}\right)\right)\right]$ show the true picture, and $\Im_{Aug(F)}$ is used to extract the goal posture elements from the target image. The aim is to create new images $\left(1-\Re_D\left(\Im_{\Re_G(F)}(\alpha),\Im_{tar(F)}\right)\right)$ based on the extracted pose of $\Im_{\Re_D(F)}$ which is the generator's objective $\left(\Im_{Aug(F)}\right)$.

To achieve this, the generator $\left(\Im_{mag(S)}\right)$ utilizes a noise vector $\left(P_{i\left(\Im_{mag(S)}\right)}\right)$ with a prior distribution $\left(P_{i\left(\Im_{mag(S)}\right)}\right)$ producing $P_{i\left(\Im_{mag(S)}\right)} = \frac{\sigma.P_{i-1}+(1-\sigma)EF_p}{(1-\sigma)}.\Delta$, This is designed to trick the discriminator into aligning $\Delta = \frac{dEF_x}{dx}+\frac{dEF_y}{dy}+\frac{dEF_z}{dz}$ with the actual images that are part of the σ distribution EF_p. The output from the generator is then provided as.

$$(\Delta) \qquad (12)$$

This approach tackles the mode collapse challenge by employing the noise vector along with the "logarithmic Z-score" technique. Consequently, the generator can learn intricate representations by evaluating the likelihood that a score fits within the normal distribution.EF_x (13)

In this context, the mean and standard deviations of random variables are represented as EF_y and $\left(P_{i\left(\Im_{mag(S)}\right)}\right)$. Likewise, the discriminator evaluates both the real images (EF_p) and the "Generator's images $\left(EF_p\right)$" to differentiate between authentic and artificially generated images. The probability of discrimination is denoted as (x, y, z). (14)

In this case,

$(EF_{int}())$,(EF_{ext}) The distribution of duplicate samples from the generator is illustrated in $\left(EF_{img}\right)$, while the network parameters are indicated as and the loss function is expressed as

$EF_p =$

$$\int_0^{1\int}\left(EF\left(P_{i\left(\Im_{mag(S)}\right)}\right)_{img}\left(P_{i\left(\Im_{mag(S)}\right)}\right)_{ext}\left(P_{i\left(\Im_{mag(S)}\right)}\right)_{int}0\right)$$

(15). Ultimately, the objectives for both the discriminator and generator are achieved by solving the following loss function. Fresh face shots that match the attitude of the target images are referred to as $\left|P_{i\left(\Im_{mag(S)}\right)}\right|$, Fresh face shots that align with the attitude of the target images are denoted as $\left|P'_{i\left(\Im_{mag(S)}\right)}\right|$ The discriminator's goal is to maximize $\delta_1\left(\Im_{mag(S)}\right)$ to identify landmark points from facial photographs. The improved results are then utilized in $\delta_2\left(\Im_{mag(S)}\right)$

3.2.4 Contour extraction

The enlarged signature pictures $EF_{img}\left(P_{i\left(\Im_{mag(S)}\right)}\right) = \delta_l EF_l + \delta_e EF_e + \delta_t EF_t$" FDAF-SACM" are utilized to create the signature's contour map. It is advisable to use the standard version of the "Snake Active Contour Model (SACM)" due to its precision in feature identification and its adaptability to changes. However, the active contour point selection optimizer suffers from the decreasing gradient problem, which prevents the descent from achieving the optimal value, resulting in poor active contour point selection. Consequently, the proposed contour extraction model employs the optimizer "AdaFactor FDivergence".

To use the "FDAF-SACM" system, you first need to outline an initial contour around the feature you want to extract. After that, you should continuously adjust the feature's position towards the point with the lowest energy function, taking into consideration both internal and external characteristics.

The snake's initial estimate from this approach

The "FDAF-SACM" system begins by forming an initial contour around the point. Then, influenced by both internal and external stimuli, it continuously adjusts the feature's position around the point by utilizing the least energy function. It is crucial to select the initial estimate of the snake, EF_l, with care to avoid local minima of EF_e.

The local optima are selected based on the form of the signature, utilizing the "FDivergence AdaFactor" EF_t

$$\delta_l \quad (16)$$

$$\delta_e \quad (17)$$

The decay parameter is represented as δ_t, while the force applied to the snake is denoted as (EF_{ext}). The equations $\left(EF_{img}\right)$ and (EF_{con}), are also included, where $EF_{ext}\left(P_{i\left(\Im_{mag(S)}\right)}\right) = EF_{img}\left(P_{i\left(\Im_{mag(S)}\right)}\right) +$ $EF_{con}\left(P_{i\left(\Im_{mag(S)}\right)}\right)$ illustrates their individual contributions along the n-axis. By multiplying the position vector with the decay parameters derived from the "FDivergence", we can achieve the optimal value.

The energy function $\{P_i\}_{i=0,1,2,\ldots,n}$ is the sum of its internal forces $\left(\Im_{mag(FP)}\right)$, external forces (M_{IL}), and image

forces (M_{RE}), defined by the initial position of the snake (M_D), which can be expressed as (M_{EC}) (18)

Internal forces consist of continuity and contour smoothness to regulate snake deformations such as (M_{RB}) (19)

The first and second-order phrases are us are utilized to control the snake by adjusting its weights. (V_{in}) and(V) are specified as $(V_{out})$and$\left(V \in \Im_{mag(FP)}\right)$.

Image forces such as attract snakes to conspicuous features including lines, edges, and termination curves.

$$\left(V_{in} \in (x_n, y_n), V_{out} \in (x_{n+1}, y_{n+1})\right) \quad (20)$$

The many energy functions used to push snakes towards lines, edges, and terminations are presented as $(M_i \in \{M_{RE}, M_{RB}, M_{EC}, M_D, M_{IL}\})$, $M_i = \begin{cases} M_{RE} if \left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) > 0\right) \\ M_{RB} if \left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) < 0\right) \\ M_{EC} if \left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) = 0\right) \end{cases}$, and $S(V_{in}, V_{out}) = x_n y_{n+1} - x_{n+1} y_n$, and the weights modified to produce snake behaviour are shown as $S_{\Im_{mag(FP)}}(V_{in}, V_{out})$, $\left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) > 0\right)$, and M_{RE}.

In contrast, external influences guide the snake to migrate near the local minimum. The forces from the image itself contribute to this, as indicated by the condition where $\left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) < 0\right)$. M_{RB} and constraining forces are applied when $\left(S_{\Im_{mag(FP)}}(V_{in}, V_{out}) = 0\right)$.

(M_{EC}) (21)

Thus, the signature features are defined by the set of traced points from the M_D "FDAF-SACM" model's (M_{IL}) which generates the signature contours.

3.2.5 Wide Range of Minutia Extraction

The Enhanced fingerprint images"$\left(\Im_{Aug(F)}\right)$" are utilized to collect sufficient minutiae points, such as Ridge Island. $\left(\Im_{Aug(F)}\right)$, Ridge Ending $\nabla_h = \Im_{Aug(F)}(i, j+1) - \Im_{Aug(F)}(i, j-1)$, Ridge Dot $\nabla_v = \Im_{Aug(F)}(i-1, j) - \Im_{Aug(F)}(i+1, j)$, Ridge Enclosure$\nabla_h$, Ridge Bifurcation and other features are crucial for precise fingerprint matching. In this research, minutiae points are obtained through the Chain code technique, which involves tracking the ridge contour in a clockwise manner. The angles made during this tracking process, along with the number of coordinates from the start to the endpoint, help pinpoint the minutiae points.

Two vectors (i, j) approach the candidate point $(Mg)$from its previous contour points, while (A) extends out from $Mg = \sqrt{\nabla_h^2 + \nabla_v^2}$

Minutia points $A = \left|tan^{-1}\left(\frac{\nabla_h}{\nabla_y}\right)\right|$are determined by inserting these vectors into the Cartesian coordinate system.$\left(FL_{(i)}\right)$ as,

$$FL_{(i)} = \sum_{i=1}^{68} FL_i\left(\Im_{Aug(F)}\right) \quad (22)$$

$$\left(M_{(i)}\right) \quad (23)$$

Here, $\left(P_{(i)}\right)$ indicates the turning direction, with a left turn represented $\left(FL_{(i)}\right)$ as $\left(\Im_{mag(FP,M_{(i)})}, \Im_{mag(S,P_{(i)})}, \Im_{Aug(F,FL_{(i)})}\right)$, (ψ_{PF}) denotes a right turn to identify $\left(\Im_{mag(FP,M_{(i)})}, \Im_{mag(S,P_{(i)})}, \Im_{Aug(F,FL_{(i)})}\right)$, Additionally, the ridge splits and merges back at the same coordinates to determine $\left(\Im_{Aug(F)}\right)$ represented as $\left(\psi_{fea}\right)$.

The $\psi_{fea} = \begin{cases} \psi_{PF(k)} \leftarrow \psi_{PF} \in \left(\Im_{mag(FP,M_{(i)})}, \Im_{mag(S,P_{(i)})}, \Im_{Aug(F,FL_{(i)})}\right) \\ \psi_{FI(m)} \leftarrow \psi_{FI} \in \Im_{Aug(F)} \end{cases}$ is identified when the ridge begins and finishes at the same coordinate without any points in between. The ridges situated in the space between two primary ridges are referred to as ψ_{FI}.

3.2.6 Extraction of facial points

Face landmarks extracted from the enhanced images (m) represent various facial features. In this case, we utilize "Dlib's 68", a pre-trained "Facial landmark detector", to automatically pinpoint 68 specific locations on the face.

The input images $\Im_{Aug(F)}$ are first processed by the "Histogram of Oriented Gradients (HOG)" face detector. This detector analyzes the input photos by compiling the histogram of the magnitude and gradients of the pixel values, utilizing a "Biosensor"to create an outline of the facial features, which captures their shape and appearance.

$$\left(\psi_{fea}\right) \quad (24)$$

$$\xi_{con(x\times x)} = \Omega_{AF} \sum_{y,z}\left(\psi_{fea(y\times y)} * \varphi_{(z\times z)}\right) + \varepsilon \quad (25)$$

The gradients in this case, both horizontally and vertically, are represented as $\xi_{con(x\times x)}$ for rows, $(x \times x)$, for and $\psi_{fea(y\times y)}$are the rows and columns, correspondingly.

The gradients in this case, both horizontally and vertically, are represented as $(y \times y)$ and orientation$\varphi_{(z\times z)}$at each pixel is determined by

$$(z \times z) \quad (26)$$

$$\varepsilon \quad (27)$$

The histogram is created to analyze the magnitude and orientation of pixel values, helping to identify areas of interest within the face region of the image. Next, a landmark detector combined with a biosensor is used to track changes in appearance, allowing for the estimation of 68 coordinates that correspond to key facial points.

The facial landmark pointsΩ_{AF}detected are,

$$\xi_{KC(X\times X)} = \int \theta\left(\xi_{con(x\times x)}\right).\theta\left(\xi_{con(x+1\times x+1)}\right) d\xi \quad (28)$$

Lastly, $\xi_{KC(X\times X)}$ denotes the images containing the minutiaθ, contour $\left(\xi_{po(a\times b)}\right)$, and facial landmark $\xi_{po(a\times b)} = \Phi_{mp}\left(\xi_{KC(X\times X)}, \varphi_{(a\times b)}, f\right)$ for further processing.

3.2.7 Feature Extraction

After the extraction of unique patterns from the input images, we derive point features Φ_{mp} such as structural position, shape, feature vector, key point, "Kullback-Leibler (KL)" divergence matching, recognition tally, and distance between the horizontal and vertical points from the

obtained data $\varphi_{(a\times b)}$ Additionally, we utilize the "Local Binary Pattern (LBP)", HOG," Speeded Up Robust Features (SURF)", "Scale Invariant Feature Transform (SIFT)", and "Local Ternary Pattern (LTP)" from the previously processed facial images f. Hence, the retrieved characteristics are presented as follows $(\xi_{FC(j)})$are provided as,

(29)

Here, ${}^{(R,F)}G_{(\Im_{FP},\Im_S,\Im_F)} = \frac{exp(\xi_{FC(j)})}{\sum_j exp(\xi_{FC(j)})}$ consists of ${}^{(R,F)}G_{(\Im_{FP},\Im_S,\Im_F)}$local features retrieved from(ψ_{fea}).

3.2.8 Superficial Biometric Recognition

Biometric information is categorized as either authentic or fraudulent with the help of "KCP-DCNN." The conventional "DCNN" is selected due to its proficiency in handling extensive data sets and delivering precise predictions. Nonetheless, a significant challenge arises when decreasing the spatial resolution of feature maps, as this results in the loss of crucial details, like the object's position and orientation. To address this challenge, "DCNN" utilizes kernel correlation-centric padding.

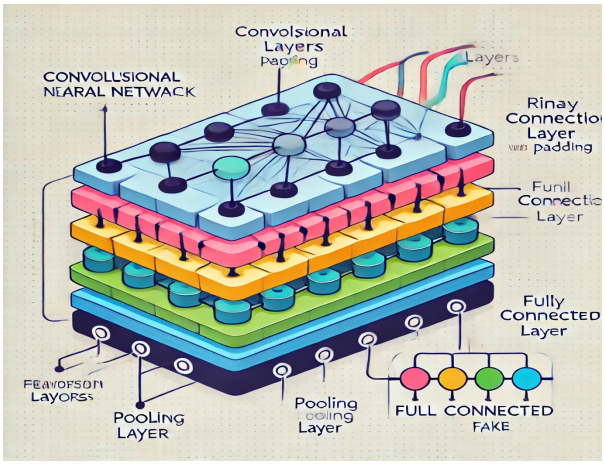


Figure 2. Architecture of "KCP-DCNN"

The output feature matrix, represented as ε, has a size of $\varphi_{(z\times z)}$, The input features are organized into a matrix of size $\psi_{fea(y\times y)}$, $(\xi_{con(x\times x)})$.The notation $(\psi_{fea(y\times y)})$ depicts the filters, $(\xi_{KC(X\times X)})$, while $\xi_{po(a\times b)}$ indicates the bias vector, Lastly $(\xi_{FC(j)})$ signifies the activation function used to standardize the output.

Kernel "correlation-centric" padding is applied after convolution to enhance the pixel contributions at the edges of the input image. This approach helps preserve position and orientation information during the pooling operation by shifting this information towards the center of the images.

$\left({}^{(R,F)}G_{(\Im_{FP},\Im_S,\Im_F)}\right)$ (31)

The output feature map after padding is denoted as(R,F), hile the kernel function is represented as $(M_{(i)})$.

The pooling layer reduces the dimensions of the feature maps created by a convolutional layer. The pooling feature maps $(P_{(i)})$ are generated as follows

$(FL_{(i)})$

The process of pooling to select various features from the covered region by the filter $\left(\Im_{mag(FP,M_{(i)})},\Im_{mag(S,P_{(i)})},\Im_{Aug(F,FL_{(i)})}\right)$ is described as$(M_{(i)})$, and$(P_{(i)})$ indicates the number of pixels that are converted into the input matrix.

The resulting feature maps are converted into a one-dimensional feature vector $(FL_{(i)})$ following the convolution and grouping layers. This transformation allows us to obtain output classification probabilities through the "SoftMax" layer in the fully connected layer. The output can be derived as follows. $(\hbar_{l(T\times T)})$ (33)

The "SoftMax function" is defined to predict whether the classes are genuine or fake.

$\hbar_{l(T\times T)} = \eta_{trfm}\left(\left(\Im_{mag(FP,M_{(i)})},\Im_{mag(S,P_{(i)})},\Im_{Aug(F,FL_{(i)})}\right),\tau\right)$.

Algorithm 2 explains the recognition procedure using "KCP-DCNN".

Algorithm 2: Biometric Recognition utilizing KCP-DCNN with Biosensor

Input: Input Features$(l=3)$
Output: Recognized output θ

Begin
  Initialize input dataη_{trfm}, parameters$(\hbar_{dist})$, $\hbar_{dist} = \varpi_{dis\_mat}(\hbar_{bin(r,c)},\hbar_{bin(r+1,c+1)})$, and number of layers
  Construct the feature matrix ϖ_{dis_mat}
  For $\hbar_{bin}$do
  Extract (r,c)
  Apply KC padding
For$\Theta_{QR} = \lambda(\hbar_{dist})$ do
Reduce dimensionality
ObtainΘ_{QR}
End
Construct λ
Perform classification using$(\Im_{FP})$
End
Return classified output$(\Im_S)$
End

The "KCP-DCNN" model assesses whether biometric data is genuine or fake. This enhances confidence levels, enabling a person to be identified and verified based on specific criteria.

3.2.9 "QR" codes

In order to improve the authenticity process, the subsequent stage of the recognition system uses the distinctive patterns produced by the input photographs to form the QR code. The positions of facial landmarks, curves, and minutiae are converted into a matrix to create the QR code.

In this process, by utilizing the position of minutia $(\Im_F)$, contour$U_n \xrightarrow{\{\Im_{FP},\Im_S,\Im_F\}} RC$, and facial landmark U_n we can generate the QR code by converting these elements into a matrix. Let (n)be the input images containing the minutiaRC, contour $(\Im_{FP},\Im_S,\Im_F)$, and facial landmark $(\Im_{FP},\Im_S,\Im_F)$ points situated at various locations, Additionally, $(\Im_{NR(FP,S,F)})$ denote the size defined for the transformation matrix. The transformed matrices$\Im_{NR(FP,S,F)} = \{\Im_{NR}(i,j)|(i,j) = med(\Im(i,j))\}$ are derived for the median biometric images, represented as

$$\Im(i,j) \quad (34)$$

The function used for transforming the image matrix is defined by (i,j).

The transformation matrices blend the matrices that are utilized for matrix binding. Potential pixel values from other transformation matrices are inserted into the specific areas where pixel values are absent during the matrix binding process. After matrix binding, a distance matrix $\Im$ is created, showing the distance between pairs of values in each row and column.

$$\Im_{NR}(i,j) \quad (35)$$

The technique for computing the distance matrix is represented as $\left(\Im_{NR(FP,S,F)}\right)$, The matrix obtained after binding is denoted as $\left(\partial_{m(i,j)}\right)$, where m^{th} refers to the corresponding row and column parameters used to calculate the distance between pixel values.

The proposed system facilitates the generation of a" QR code" by utilizing the safe distance matrix, which can be represented as $\left(\Im_{NR(FP,S,F)}\right)$ (36)

The "QR code" produced by the generator is defined as $\partial_{cl} = \frac{L}{N}\left(1 + \frac{cf}{100}(sl_{max}())()\right)$. This QR code serves as a two-dimensional matrix code for authentication in the proposed system. Once registered, users try to log in using their fingerprint, signature, and facial images. The model employs a two-step verification process to validate the user's identity.

• The initial phase assesses whether the input is genuine or forged by analyzing its features and comparing them against various verification units in the databases, such as fingerprints, facial recognition, and signatures.

• Once the inputs are verified as authentic, users can proceed to the next step, where they log in by scanning the QR code generated during registration. By matching the QR code, the system determines whether to authenticate the user or flag them as unauthorized.

The accuracy of the proposed model is increased by this extra verification unit, which improves convenience and security in biometrics-based systems that make use of biosensors. We can develop a novel method of user authentication and identity verification by utilizing technologies for handwritten character recognition, biometric data, and facial recognition. Using distinctive bodily characteristics, such as fingerprints, handwriting patterns, or facial features, to identify someone is known as biometric authentication. To match the findings to a user's identification by looking at their facial features, sophisticated algorithms in face recognition technology examine saved images or video feeds. Additionally, handwritten character recognition technology can be used to identify and authenticate users based on their unique handwriting styles.

3.3 Experimental Hypothesis

Accuracy, specificity, F-measure, precision, and recall, the proposed "KCP-DCNN" performs better than alternative techniques. Notably, it attains the best precision, recall, and "F-measure" values at 98.529%, as well as the highest accuracy and specificity at 98.181% and 97.619%, respectively. The CNN comes in second for accuracy and specificity, while the "KCP-DCNN" is superior in precision, recall, and F-measure. However, when compared to the "KCP-DCNN" and CNN, the RNN and DBN perform worse in terms of accuracy, specificity, precision, recall, and F-measure. These findings imply that the KCP-DCNN is a very successful strategy for this particular issue.

Multiple convolutional and pooling layers are incorporated into the KCP-DCNN approach, which is followed by dense layers for classification. This method can be very computationally demanding, particularly when dealing with huge input photos. However, because it makes use of the KCP (Knowledge Consolidation and Pruning) technique, which helps to reduce computational complexity and the number of parameters, it is more efficient than typical DCNNs. Furthermore, the particular hardware and software utilized determine the KCP-DCNN method's real-time processing capabilities. For instance, it might be able to process smaller input images in real time if it is implemented on a high-performance GPU with code that is optimized.

The KCP-DCNN technique employs multiple convolutional and pooling layers prior to the addition of dense layers for classification. This approach can lead to a considerable computational load, particularly when processing large sets of input images. However, the use of the KCP (Knowledge Consolidation and Pruning) technique in this methodology helps to minimize the number of parameters and reduce computational complexity, making it more efficient compared to traditional DCNNs.

The KCP-DCNN methodology's ability to process data in real time is influenced by the hardware and software in use. For example, utilizing a high-performance GPU with optimized coding can enable real-time processing of input images. This technique demands considerable processing power, requiring a robust CPU, GPU, or TPU (Tensor Processing Unit). A good illustration is the NVIDIA GeForce RTX 3090 GPU, which comes with 24 GB of RAM and can effectively handle the training and inference of KCP-DCNN models with large input images. The process may demand a considerable amount of RAM and storage to hold the trained models and input data. Especially in critical applications, it is essential to ensure scalability and robustness to maintain the system's availability, reliability, and security. Systems should be built with scalability and resilience as primary focuses to adapt to evolving user requirements and defend against potential attacks.

4. RESULTS AND DISCUSSION

The numerous tests conducted on the Python working platform to confirm and validate the suggested MB system are presented in this part.

4.1 Dataset Description

The biometric photos collected from many sources are subjected to trials aimed at validating the proposed system at different significant levels. The system collected fingerprint and face image data from the FVC2000_DB4_B, Face recognition, and "Sokoto Coventry Fingerprint Data Set (SOCOFing)".

Eleven hundred thirty-two photos in all were selected to act as training examples for the suggested method. Real-time signature collecting was used to create the system's training samples, yielding 1013 samples. Ten thousand samples make up the dataset, of which 80% is used for training and 20% is

used for testing. The total number of photos collected to create the Biosensor training samples is shown in Table 1.

Table 1. Biometric pictures gathered from different databases

Data gathering biometric	Images count
Biometric	Fingerprint-1500
	Face-1000
Total pictures gathered	1132
quantity of produced training	1013
Real-time samples of signatures produced	1013
Training images	810
Testing images	203

Complete sample of DataSet Acquired to Train the model and acquire results

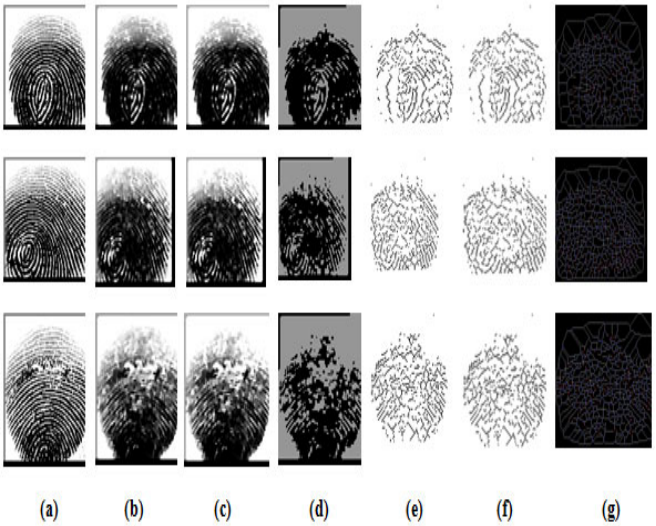


Figure 3 "Representative fingerprint images gathered from publicly accessible sources (a) Images used as input; (b) Images with noise removed (c) pictures with more contrast (d)Image binarization, (e) the output image following thinning. (f) Magnified pictures; (g) Extracted minutia points"

Figure 4 displays the outcomes of the obtained sample photos in signature. Figure 5 presents the results of the sample photos taken in the face using Biosensor.

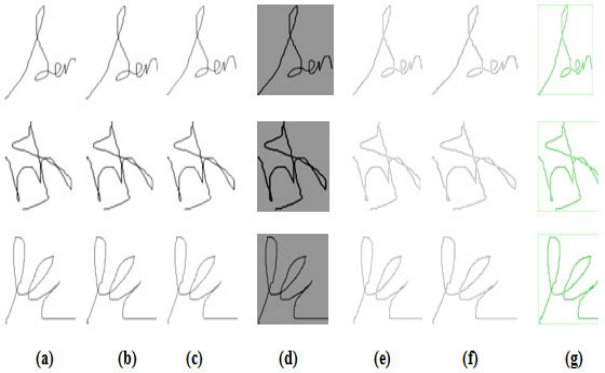


Figure 4. "Gathering sample signature photographs in real time (a) Input images; (b) Noise-removed images; (c) Contrast-boosted images; (d) Binarized images; (e) Output image after thinning; (f) Magnified images; and (g) Contour Points"

Figure 5. Facial points are recovered from (a) input photographs, (b) noise-free images, (c) contrast-optimized images, and (d) example face shots.

4.2 Performance analysis

This section compares the performance of the "RBF-PRT" and "KCP-DCNN" approaches with the existing methods in order to evaluate the efficacy of the proposed system.

Table 2. Comparison of the Proposed "KCP-DCNN's " Performance

Methods/ Metrics	Precision (%)	Recall (%)	F-measure (%)	Accuracy (%)	Specificity (%)
Proposed KCP-DCNN	98.529	98.529	98.529	98.181	97.619
CNN	96.648	96.052	97.333	96.363	97.058
RNN	96.25	95.061	95.652	93.636	89.655
DBN	94.202	91.549	92.857	90.909	89.743
DNN	92.187	88.059	90.076	88.181	88.372

The KCP-DCNN's" performance metrics are evaluated against the CNN, Deep Belief Network (DBN), Recurrent Neural Network (RNN), and Deep Neural Network (DNN) as they are currently available in Table 2. Performance metrics include precision, F measure, recall, accuracy, and specificity. Increased measurement precision could be indicated by elevated values from these markers. Consequently, the collected data demonstrated that the proposed method enhanced accuracy, recall, and F measure by 1.88%, 2.47%, and 1.19%, respectively, as compared to the industry standard "CNN". Furthermore, the accuracy and specificity of the proposed method were at their peak. Thus, the "KCP" technique reduced the amount of crucial data lost while

improving the high projected accuracy by learning a vast amount of data using Biosensor.

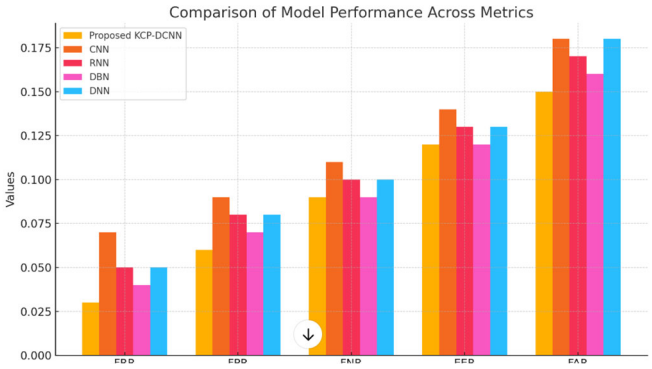


Figure 6. Comparing the effectiveness of various techniques

Recurrent Neural Network (RNN), Deep Neural Network (DNN), Deep Belief Network (DBN), and the present "CNN" are compared with the KCP-DCNN's performance metrics in "Table 2. Precision, F measure, recall, accuracy, and specificity are some of the performance metrics." Increased measurement precision may be indicated by high results from these indicators. In comparison to the industry standard "CNN", the gathered data showed that the suggested method improved accuracy, recall, and F measure by 1.90%, 3.01%, and 1%, respectively. Additionally, the suggested technique's accuracy and specificity were at their highest points. Thus, the "KCP" technique improved the high projected accuracy while avoiding the loss of important information by learning a sizable amount of data using a biosensor.

Table 3. Examination of Training Duration

Methodologies	Duration of Training (ms)
Method 1:"KCP-DCNN" [Proposed]	27003
Method 2:CNN	32002
Method 3:RNN	37003
Method 4:DBN	43014
Method 5:DNN	48006

Table 3 provides an analogy of the training times for the suggested and existing recognition systems. Compared to the current "CNN", the suggested approach requires a training time that is substantially less, 4999 ms. This shows that, in comparison to the existing techniques, the "KCP" methodology offers an effective learning route to reduce training time, allowing the recommended system to learn more rapidly and correctly.

The performance of the proposed "RBF-PRT" is compared with the already used picture magnification techniques, including "bilinear interpolation (BI)", "closest neighbor interpolation (NNI)", "intelligent pixel replication (IPR)", and "bi-cubic interpolation (BCI)", as illustrated in Figure 7. Based on quality metrics including "Mean Square Error (MSE)", "Mean Absolute Error (MAE)", "Root Mean Square Error (RMSE)", and "Mean Absolute Percentage Error (MAPE)", the techniques are evaluated independently for fingerprint and signature images.

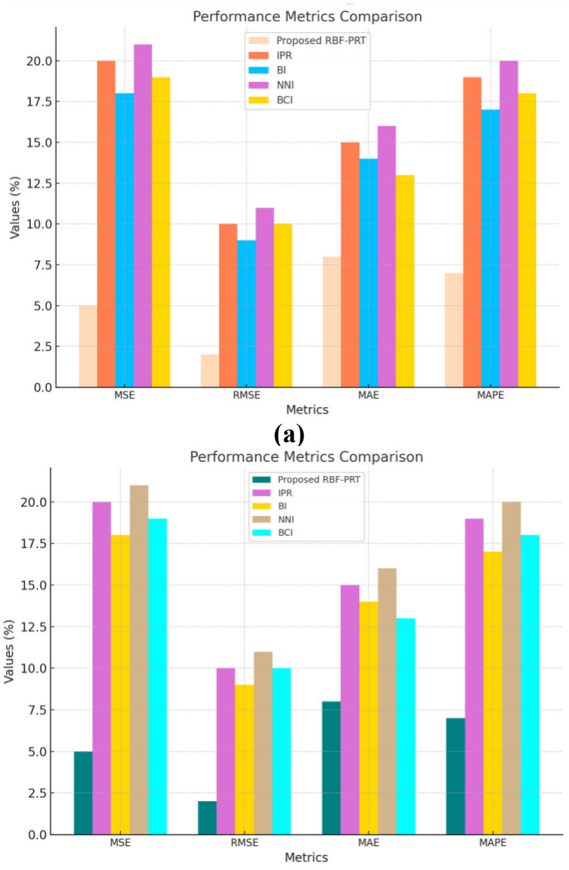
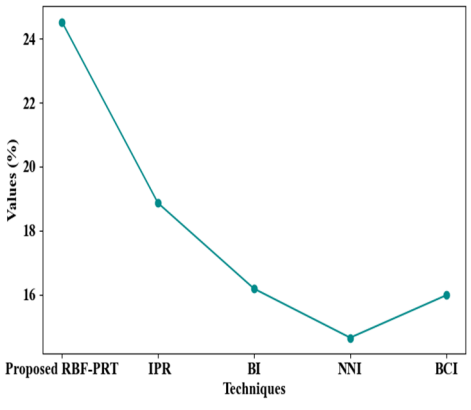
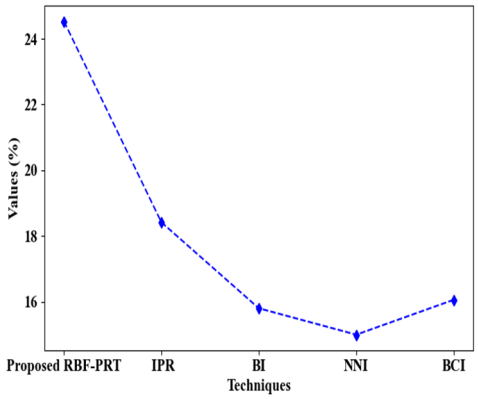


Figure 7. Performance Assessment of the Proposed "RBF-PRT" in Connection with (a) Fingerprint and (b) Signature Images

A high-quality magnification is shown by obtaining the lowest values of these metrics between the original and reconstructed pictures. Figures 8(a) and 8(b) demonstrate that the recommended approach yielded the lowest "MSE" and "RMSE" values for fingerprint images (5.0324 and 2.859) and signature images (4.918 and 2.996). The suggested method also produced minimum values for "MAE" and "MAPE" that were higher than those of the existing procedures. Thus, the study concludes that the center pixel value may be updated using an "RBF-centric method to provide high-quality magnification while simultaneously lowering the error rate.

The peak signal-to-noise ratio (PSNR) of the commonly used and advised image magnification methods for fingerprints and signatures.





(b)

Figure 8 Performance analysis categorization using PSNR for (a) fingerprint and (b) signature images

According to the results, the proposed method outperforms the existing approaches in this area, producing fingerprint and signature images with "PSNRs" of 24.5236% and 24.5320%, respectively. Consequently, the study shows that the RBF strategy aids the suggested technique in generating high-quality enlarged images with improved "PSNR" values.

4.3Analyzing things in comparison

The suggested "KCP-DCNN" model is contrasted with existing biosensor-based approach systems.

Table 4 presents a comparison between the proposed system and the top MB systems in terms of precision, specificity, FPR, and EER. Using SOCOF principles, FVC2000_DB4_B, and face recognition datasets, Vyas et al. employed a KCP-DCNN model for score-level fusion of fingerprint, signature, and face biometrics [22].Their proposed model achieved high accuracy (98.529%), low equal error rate (EER) (0.019%), low false positive rate (FPR) (0.023%), and good specificity (97.619%). Purohit and Ajmera created an LCNN-Salp swarm optimization model for biometrics employing fingerprints, faces, and keystrokes using the ORL, Yale face, FASSEG, KEY STROKE, and fingerprint datasets [23].

Table 4. Analysis of Comparations

Author's Name and Year	Method utilized	Utilizing a biometer	Dataset	Metrics for Results			
				Accuracy (%)	Degree of Specificity	False Positive Rate (%)	Expected Error Rate (%)
Proposed Model	Method KCP-DCNN	Face, fingerprint, and signature	SOCOFing, FVC2000_DB4_B, and Face recognition datasets	98.529	97.619	0.023	0.019
(Vyas et al., 2022) [22]	Score-level fusion	Iris & Palmprint	MMDB1, MMDB2, and IITD iris database	-	-	0.5	9.61
(Purohit&Ajmera, 2022) [18]	[Salp swarm optimization] LCNN-	Fingerprint, face, and keystroke.	FASSEG, KEY STROKE,ORL, Yale face, and Fingerprint	97.5	95.78	4.22	-
(Iula&Micucci, 2022) [9]	Score-level fusion	Palm-print & hand geometry	home–made database	-	-	0.044	0.08
(Vijay &Indumathi, 2021) [24]	Multi-SVNN classifier	Iris, ear, and Finger vein	SDUMLAHMT database and AMI	92.684	95.468	-	-
(Sarangi et al., 2022) [25]	kNN classifier	Ear & profile face	UND-E database and UND-J2 database	-	-	0.12	2.3928

High specificity (95.78%) and accuracy (97.5%) were attained by their suggested model, but its false positive rate (FPR) was higher (4.22%). For EER, no results were given in this investigation. Using a homemade database, Iula and Micucci employed score-level fusion for palm print and hand geometry biometrics [9]. Low false rejection rates (FRR) (0.08%) and low false acceptance rates (FAR) (0.044%) were attained by their suggested model. For this investigation, there were no findings available for FPR, EER, precision, or specificity.

Using the SDUMLAHMT database and AMI, Vijay and Indumathi employed a multi-SVNN classifier for biometrics involving the iris, ear, and finger veins [24]. High specificity (95.468%) and precision (92.684%) were attained by their suggested model; however, FPR and EER data were not presented in this investigation. Sarangi et al. used a KNN classifier for face and ear biometrics using the UND E and UND J2 datasets [25]. Low false rejection rates (FRR) (2.3928%) and low false acceptance rates (FAR) (0.12%) were attained by their suggested model. For this investigation, there were no findings available for FPR, EER, precision, or specificity.

Results demonstrated that, in comparison to the current procedures, the suggested technique yields better outcomes. Compared to the current methods using Biosensor, the suggested KCP-DCNN model decreased EER by 9.591% and increased accuracy by 1.029%. Additionally, the suggested system performed better in terms of FPR and specificity. Despite their good performance, the existing methods required a lot of time because they extracted low-level features from the intricate structures of the images. Furthermore, they rely solely on the biometric template data that is provided for authentication. As a result, the system becomes open to security breaches wherein hackers might use fake biometric information to gain access. This has been fixed in the proposed method by utilizing biosensor authentication with a combination of non-biometric and biometric features. The suggested technique produced distinct patterns of biometric data and detailed copies of enlarged photographs to enable accurate and quick authentication performance. Moreover, the use of falsified biometric data for authentication has been prevented by the two-step verification procedure. This is the primary cause of the suggested methodologies exceptional performance.

5. CONCLUSION

This research proposes an effective multimodal Biosensor-assisted identity identification system that integrates fingerprint and signature modalities. The creation of distinctive patterns, such as minutiae, contours, and facial landmark points, and the RBF-PRT-centered picture magnification are crucial stages of the suggested authentication system. Furthermore, several experiments are conducted in which the suggested RBF-PRT and KCP-DCNN algorithms perform similarly to the conventional methods. When compared to the existing methodologies, the experimental results demonstrated that the proposed methodology achieved a low EER (0.0192) and an enhanced recognition rate (98.529%). Therefore, the suggested system can function well for multimodal BA. The main drawback of the suggested approach is its ignorance of feature selection, which means that biometric features may contain noisy, redundant, or irrelevant features that degrade performance. Future research into a variety of aspects in conjunction with a feature selection method may lead to the development of a more effective MB system for the precise identification of an individual. The suggested solution offers secure payment together with two-factor authentication and can be integrated with Biosensor.

REFERENCES

[1] Almomani, I., El-Shafai, W., AlKhayer, A., Alsumayt,A., Aljameel, S. S., & Alissa, K. (2023). Proposed Biometric security system based on deep learning and chaos algorithms. Computers, Materials and Continua, 74(2),3515–3537. https://doi.org/10.32604/cmc.2023.033765

[2] Bedari, A., Wang, S., & Yang, W. (2022). A secure online fingerprint authentication system for industrial IoT devices over 5G networks. Sensors, 22(19), 1–16. https://doi.org/10.3390/s22197609

[3] Rajendran, S., Sundarapandi, A.M.S., Krishnamurthy, A. and Thanarajan, T., 2022. An Intelligent Face Recognition Technology for IoT-Based Smart City Application Using Condition-CNN with Foraging Learning PSO Model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), p.2256018. https://doi.org/10.1142/s0218001422560183

[4] Bordel, B., Alcarria, R., & Robles, T. (2022). Lightweight encryption for short-range wireless biometric authentication systems in Industry 4.0. Integrated Computer-Aided Engineering, 29(2), 153–173. https://doi.org/10.3233/ICA-210673

[5] Chen, Y., Xue, M., Zhang, J., Guan, Q., Wang, Z., Zhang, Q., & Wang, W. (2021). ChestLive: Fortifying voice-based authentication with chest motion biometrics on smart devices. ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 5(4), 1–25. https://doi.org/10.1145/3494962

[6] Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Acharya, S. and Kim, H., 2023. Blockchain Assisted Data Edge Verification with Consensus Algorithm for Machine Learning Assisted IoT. IEEE Access. DOI:10.1109/ACCESS.2023.3280798

[7] Riya, K.S., Surendran, R., Tavera Romero, C.A. and Sendil, M.S., 2023. Encryption with User Authentication Model for Internet of Medical Things Environment. Intelligent Automation & Soft Computing, 35(1). DOI:10.32604/iasc.2023.027779

[8] Thanarajan, T., Alotaibi, Y., Rajendran, S. and Nagappan, K., 2023. Improved wolf swarm optimization with deep-learning-based movement analysis and self-regulated human activity recognition. AIMS Mathematics, 8(5), pp.12520-12539. doi: 10.3934/math.2023629

[9] Iula, A., &Micucci, M. (2022). Multimodal biometric recognition based on 3d ultrasound palmprint-hand geometry fusion. IEEE Access, 10, 7914–7925. https://doi.org/10.1109/ACCESS.2022.3143433

[10] Gowri, S., Appathurai, K., Gomathi, R.M. and Surendran, R., 2023, August. Securing Files on Cloud Storage with Group Key Management Protocol. In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1317-1321). IEEE. **DOI:** 10.1109/ICIRCA57980.2023.10220871

[11] Kumar, T., Bhushan, S., &Jangra, S. (2021). An improved biometric fusion system of fingerprint and face using whale optimization. International Journal of Advanced Computer Science and Applications, 12(1), 664–671. https://doi.org/10.14569/IJACSA.2021.0120176

[12] Vhaduri, S., Dibbo, S. V., & Cheung, W. (2021). HIAuth: A hierarchical implicit authentication system for IoT wearables using multiple biometrics. IEEE Access, 9, 116395–116406. https://doi.org/10.1109/ACCESS.2021.3105481

[13] Singh, S. P., & Tiwari, S. (2023). A dual multimodal biometric authentication system based on WOA-ANN and SSA-DBN Techniques. Sci, 5(1), 1–28. https://doi.org/10.3390/sci5010010

[14] Thenuwara, S. S., Premachandra, C., &Kawanaka, H. (2022). A multi-agent based enhancement for the multimodal biometric system at border control. Array, 14, 1–11. https://doi.org/10.1016/j.array.2022.100171

[15] Tran, Q. N., Turnbull, B. P., Wang, M., & Hu, J. (2021). A Privacy-preserving biometric authentication system with binary classification in a zero knowledge proof protocol. IEEE Open Journal of the Computer Society,3,1–10. https://doi.org/10.1109/ojcs.2021.3138332

[16] Behera, S. K., Kumar, P., Dogra, D. P., & Roy, P. P. (2021). A robust biometric authentication system for handheld electronic devices by intelligently combining 3D Finger motions and cerebral responses. IEEE Transactions on Consumer Electronics, 67(1), 58–67. https://doi.org/10.1109/TCE.2021.3055419

[17] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., &Shamna, A. R. (2021). A multimodal biometric authentication scheme based on feature fusion for improving security in the cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6141–6149. https://doi.org/10.1007/s12652-020-02184-8

[18] Purohit, H., &Ajmera, P. K. (2021). Optimal feature level fusion for secured human authentication in the multimodal biometric system. Machine Vision and Applications,32(1),1–12. https://doi.org/10.1007/s00138-020-01146-6

[19] El-Rahiem, B. A., El-Samie, F. E. A., & Amin, M. (2022). Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. Multimedia Systems, 28(4), 1325–1337. https://doi.org/10.1007/s00530-021-00810-9

[20] Goh, Z. H., Wang, Y., Leng, L., Liang, S. N., Jin, Z., Lai, Y. L., & Wang, X. (2022). A framework for multimodal biometric authentication systems with template protection. IEEE Access, 10, 96388–96402. https://doi.org/10.1109/ACCESS.2022.3205413

[21] Cherifi, F., Amroun, K., & Omar, M. (2021). Robust multimodal biometric authentication on IoT device through ear shape and arm gesture. Multimedia Tools and Applications, 80(10), 14807–14827. https://doi.org/10.1007/s11042-021-10524-9

[22] Vyas, R., Kanumuri, T., Sheoran, G., & Dubey, P. (2022). Accurate feature extraction for multimodal biometrics combining iris and palmprint. Journal of Ambient Intelligence and Humanized Computing, 13(12), 5581–5589. https://doi.org/10.1007/s12652-021-03190-0

[23] Purohit, H., &Ajmera, P. K. (2022). Multi-modal biometric fusion based continuous user authentication for E-proctoring using hybrid LCNN-Salp swarm optimization. Cluster Computing, 25(2), 827–846. https://doi.org/10.1007/s10586-021-03450-w

[24] Vijay, M., &Indumathi, G. (2021). Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications. Journal of Information Security and Applications, 58, 1–14. https://doi.org/10.1016/j.jisa.2020.102707

[25] Sarangi, P. P., Nayak, D. R., Panda, M., &Majhi, B. (2022). A feature-level fusion-based improved multimodal biometric recognition system using ear and profile face. In Journal of Ambient Intelligence and Humanized Computing. Springer Berlin Heidelberg. https://doi.org/10.1007/s12652-021-02952-0