A Human Gait Recognition Against Information Theft in Smartphone using Residual Convolutional Neural Network

Gogineni Krishna Chaitanya[1], Dr. Krovi.Raja Sekhar[2]
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, 522502, Andhra Pradesh, India

***Abstract*—The genuine user of the smartphone is identified and information theft is prevented by continuous authentication, which is one of the most emerging features in biometrics application. A person is recognized by analysing the physiological or behavioural attributes is defined as biometrics. The physiological qualities include iris acknowledgment, impression of finger, palm and face geometry are used in the biometric validation frameworks. In the existing entry-point authentication techniques, a confidential information is lost because of internal attacks, while identifying the genuine user of the smartphone. Therefore, a biometric validation framework is designed in this research study to differentiate an authorized user by recognizing the gait. In order to identify the unauthorized smartphone access, a human gait recognition is carried out by implementing a Residual Convolutional Neural Network (RCNN) approach. A personal information of end user in smartphone is secured and presented a better solution from unauthorized access by proposed architecture. The performance of RCNN method is compared with the existing Deep Neural Network (DNN) in terms of classification accuracy. The simulation results showed that the RCNN method achieved 98.15% accuracy, where DNN achieved 95.67% accuracy on OU-ISIR dataset.**

Keywords—Authentication; biometric analysis; genuine user; information loss; residual convolutional neural network; smartphone

I. Introduction

In the past few years, the researchers considered reliable authentication of users as most significant technique in various applications namely smart phone unlocking or online banking system, because the verification provides security to credential information of end users [1]. According to every access control framework, identification has three different strategies to verify the possessions. A person's keys, badges and cards are considered as first strategy, where secret password, Personal Identification Number (PIN), client id are presented in second strategy and the final strategy is biometrics such as ear, face, fingerprint, etc. [2]. The individual's identification is verified by biometric verification techniques straightforwardly, when compared with first and second techniques [3]. The existing algorithms uses the physiological biometrics such as retina, unique mark, and palm prints for characterizing the human personality on the basis of information collected from the human body [4]. A particular activity of a man is characterized by using behavioural biometrics such as keystroke elements, voice ID, signature elements and movements of human [5]. In biometrics frameworks, the existing techniques widely used the human's face, fingerprint impression and iris [6,7]. But, there are some major drawbacks presented in the existing techniques, where the health conditions, age, external appearances influence the human face and ink, drugs or burns on fingers influences the finger impression. Therefore, gait behavioural analysis is introduced by the researchers as new innovation, because a novel element of an individual is described by human gait [8,9].

The personal information of user can be accessed by unlocking the smartphone device, where entry-point authentication plays an important role for unlocking. A direct contact, fixed emotions or specific postures are mostly used by many existing biometrics for pattern classifications, but gait recognition doesn't require any specific notifications to identify the persons that works in a natural way [10-11]. In general, gait images or videos are recorded/captured from a far distance. In order to identify a person, vision techniques are used by gait recognition with a low resolution images/videos. The normal cameras in a mobile phone is used to collect the gait images and videos, therefore, recognition of gait is attractive, simple and effective method. Moreover, gait recognition algorithms are effective even with low-quality images [12,13]. In this research study, there are three major steps presented in the proposed architecture, where the steps include pre-processing the data, extracting the features and matching process. A personal information of smartphone is secured by developing the gait recognition of smartphone architecture. The research study designed the Residual Convolutional Neural Network for verifying the user behaviour in gait recognition. The steps for training and prediction of user behavioural patterns are explained through continuous authentication in the proposed algorithm. The validations are conducted on CASIA-A, B and OU-SIR datasets for validating the performance of RCNN in terms of accuracy, precision, F1-score and sensitivity.

The remaining research paper is consisting of: Section 2 presents the discussion of various existing techniques, where problem statement of the research study is provided in Section 3. The explanation of the system design with proposed algorithm is illustrated in Section 4 and the validation of proposed RCNN method with traditional techniques is depicted in Section 5. Finally, the conclusion of the research study is presented in Section 6.

II. Literature Review

In this section, the existing techniques includes different neural networks and fuzzy logic techniques are discussed that are used for predicting the gait behaviour of a person. Moreover, the key benefits of the existing techniques with its limitations are presented from the year 2017 to 2020. The parameters such as recognition accuracy, precision, recall and f-measure are used to validate the effectiveness of existing techniques.

N. Takemura et al. [14] designed an input and output architecture for CNN for recognizing the cross-view gait. Two major aspects were considered in this developed method, where the first aspect was identification versus verification and the final aspect was the trade-off between the displacements of spatial information that was caused by view difference and subject difference. The experiments were conducted on OU-ISIR large population dataset, where the results proved that Siamese network and triplet network were suitable for verification and identification. Here, the developed method identified the cross-view gait only by considering the spatial displacement that were caused by view angle difference. But, the displacement of spatial was caused by clothing difference, carrying status difference, walking speed difference, etc., which were not focused by the developed CNN method.

S. Tong et al. [15] addressed the multi-view gait recognition problem by implementing the Spatial-Temporal Deep Neural Network (STDNN) that consists of Spatial Feature Network (SFN) and Temporal Feature Network (TFN).The low-level edge features were extracted by adopting the sub-network of TFN and given as an input to the Spatial-Temporal Gradient (STG) network. A multilayer CNN was used to extract the spatial features, where a long short-term memory unit was used to extract the STG features. When comparing with intra-class variations, inter-class variations were larger by optimizing the SFN using verification loss and classification loss. The simulations were conducted on three datasets includes CASIA-B, CMU MoBo and OU-SIR datasets. The results stated that the STDNN method achieved better performance than other existing techniques, however the developed method was insufficient to handle the over-fitting problems.

I. Huitzil et al. [16] studied the recognition of gait system that depends on fuzzy ontologies and Microsoft Kinect. When comparing with existing techniques, the study proposed the novel recognition algorithm based on fuzzy logic achieved better performance for straight line walks. The issues of identification of unknown individuals were solved by the developed method, which were not presented in the system knowledge base. In order to improve the performance of the method, a new dataset with 91 individuals were developed and the results proved that the developed algorithm was robust against small changes in the biometrical values across different steps. But, the reflective clothing and footwear affected the recordings quality, when building the new datasets, which was the major drawback of the method.

X. Wang et al. [17] achieved better gait recognition by using Trituple gait silhouettes (TTGS) feature representation and Multichannel CNN (MCNN). The essential features of human gait were extracted by using MCNN approach, where gait data was pre-processed by TTGS that contained local information and didn't required the segmentation of strict gait cycle. The experiments were conducted on popular datasets included CASIA Dataset B and OU-ISIR Large Population Dataset in terms of cumulative match characteristics (CMCs). The results proved that the developed method achieved better performance than other existing techniques. However, the method failed to process the original gait videos and worked only on the silhouette images.

H. Arshad et al. [18] recognized the human gait by integrating framework of DNN with Fuzzy Entropy controlled Skewness (FEcS) approach. The pre-trained CNN model was used to extract the DCNN features and their information were mixed using parallel fusion approach. The best subsets of features were selected by using the FEcS approach with the calculation of skewness and entropy vectors from the fused vectors. The four datasets include CASIA-A, B, C and AVAMVG gait was used to test the efficiency of the developed method and the results proved that the FEcS approach achieved better performance. However, the developed method neglected some useful features and the system accuracy was affected due to low-resolution video sequences.

In order to address the issues of existing techniques, the research study designed a RCNN approach for recognizing the human gait in order to preserve the credential information of end users.

III. Problem Statement

In this section, the major problem of this research study that are presented in smartphone is explained. In general, a vast amount of personal information is presented in the user's smartphone. The entry-point authentication is generally used to secure the privacy of user's information, where knowledge-based passwords in authentication is used for unlocking the smartphones that are visible to user's surrounding people. Then, the unauthorized users (maybe friends/relatives) access the smartphone by stealing the knowledge-based passwords using internal attacks. Therefore, the confidential information of users are easily accessed that may cause mischiefs. Moreover, the major existing techniques such as neural networks may suffers from overfitting problems.

IV. Proposed Methodology

The explanation of the proposed method is presented in this section. In order to address the theft of user's information, the existing techniques designed the two-phase authentication of the smartphone. However, this technique needs extra time for verification and it suffers from an internal attack, when the password space of the second phase is visible. Therefore, behavioural biometric of smartphone is introduced in this research study by developing a Residual Convolutional Neural Network (RCNN), because behavioural patterns of the individual user are identical. The proposed architecture is consisting of two phases namely enrollment phase and verification phase, which is shown in Fig. 1.

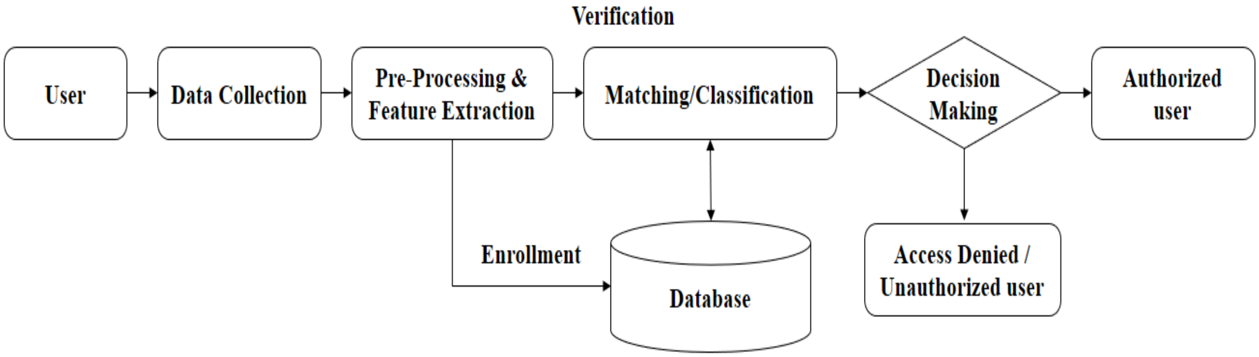


Fig. 1. Proposed Architecture.

There are three stages presented in the enrollment phase namely data collection, pre-processing with extracting the important data and database. In the verification phase, there are four stages are presented such as collecting the data, pre-processing with feature extraction, database and matching the data for final decision (i.e. decision making). In the below section, every stages in enrollment and verification phases are illustrated as follows:

A. Data Collection

The behaviour activity of user is collected by using tiny sensors in the smartphones, where the gyroscope sensors as G and accelerometer sensors as A of the smart phone are selected for collecting the biometric patterns of users. Consider $G=\left[G_x,G_y,G_z\right]$ and $A=\left[A_x,A_y,A_z\right]^T$, where x,y,z are defined as vectors and those vectors are stored in two dimensional arrays called $A and G$. The transpose of two dimensional arrays are horizontally concatenated and stored in a single two-dimensional array, where the Eq. (1 and 2) shows the transpose of $A and G$ and Eq. (3) shows the storage of concatenation of Eq. (1 and 2).

$$A=\left[A_x,A_y,A_z\right]^T \tag{1}$$

$$G=\left[G_x,G_y,G_z\right] \tag{2}$$

$$D=\left[A,G\right] \tag{3}$$

Where, a two-dimensional array is illustrated as D . After collecting the data, it will give as an input for pre-processing stage.

B. Pre-Processing and Feature Extraction

In order to improve the behavioural pattern quality, the missing values are removed in the pre-processing stage from the raw behavioural data. Then, the feature extraction stage occurred by obtaining the pre-processed behavioural data. In the process of extraction, the RCNN method is used to extract both spatial and temporal features from the pre-processed data.

C. Database

The behavioural templates are stored in the database that are labelled with user ID, where two phases are connected with database logically as depicted in Fig. 1. The user templates for verification is used in database for enrollment phase and matching templates are stored for final classification for verification phase.

D. Matching and Decision Making

In this section, the developed method concludes that whether the end user is either genuine/authorized users or non-genuine/unauthorized users. The user identity's matching score is calculated by comparing templates using matching algorithm. In order to produce a match score, the research study uses the RCNN classifier, which is explained in below section. Therefore, the user as whether authorized user or unauthorized user is decided by using the produced match score. The user can access the resources in smartphones only if the user is authorized, otherwise, the access is denied.

E. Design of Classifier

In visual imagery, the most commonly used technique is Residual Convolutional Neural Network or ResNet [19], which is a class in DNNs. The identity of user is classified by using RCNN with learning models for behavioural analysis, which is the major objective of the proposed classifier. The RCNN classifier obtained the training and testing for analysing the human gait behaviour in this work. The feature maps are produced by converting the images with filters in the RCNN approach. In order to receive high-level features from the input data, the next convolution layer received this kind of feature maps. Fig. 2 illustrates the basic architecture of RCNN [20].

The dimensionality of image is reduced and non-linearity is added by using the down sampling operation and non-linearity function between the convolution layers. When the dominant features are predicted in the feature maps, the down sampling operation used the max pooling layer for reducing the dimensionality. The feature maps are vectorized by using the flattering layers, once the NN is initialized. At every output neurons, a number is produced by forwarding flatten input vector into network in the NN that shows how much a certain activity is classified as input vector. In the proposed RCNN techniques, the parameters for mapping function, pooling process and loss function of softmax classifier are used. The following equations will explains the parameters for each function. Fig. 3 shows the working procedure of RCNN classifier.

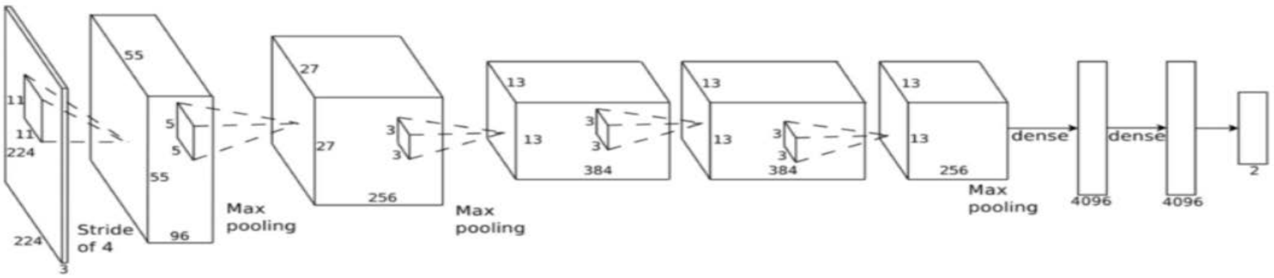


Fig. 2. Basic Architecture of CNN.

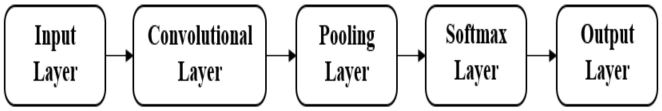


Fig. 3. Working Procedure of RCNN Classifier.

The local information of data is extracted by using convolution layer in RCNN classifier. In addition, the input features are improved by the convolutional operations that minimized the interference of noise. The mathematical equation (4) shows the mapping operation in the process of convolution.

$$x_j^l = f_c\left(\sum_{i\in M_j} x_i^{l-1}\times k_{i,j}^{l-1}\times k+\theta_j^l\right) \tag{4}$$

where, convolutional layer's mapping set is denoted as x_j^l, feature set in $(l-1)$ convolutional layer is illustrated as x_j^{l-1} and convolutional kernel between mapping set and feature set is represented as $k_{i,j}^l$ in the convolutional layer l. The bias is described as θ_j^l and activation function is depicted as f_c. During training process, over-fitting is highly reduced by using the pooling process. The mathematical expression (5) describes the pooling process as:

$$x_j^l = f_p\left(\beta_j^l down\left(x_i^{l-1}\right)+\theta_j^l\right) \tag{5}$$

where, downsampling method is denoted as $down(.)$ from the layer of $(l-1) to\, l^{th}$ layer, additive bias is described as θ_j^l, multiplicative bias is denoted as β_j^l and the activation function is illustrated as $f_p(.)$. There are two types presented in the pooling process, where types include maximum and average pooling. A rasterization layer is formed by arranging the final pooling layer (i.e. matrix features), where fully connected layer is further connected with the matrix features. Eq. (6) stated the node output as:

$$h_j = f_h\left(\sum_{i=0}^{n-1} w_{i,j}x_i-\theta_j\right) \tag{6}$$

where, the input vector connection weight is illustrated as $w_{i,j}$, node threshold is denoted as θ_j and activation function is described as $f_h(.)$. The mathematical equation 7 represents the loss function of softmax classifier.

$$J(\theta) = -\frac{1}{m}\left[\sum_{i=1}^{m}\sum_{j=1}^{k} l\left\{y^{(i)}=j\right\}\log\frac{e^{\theta_j^l}}{\sum_k e^{\theta_k^l}}\right] \tag{7}$$

where, j^{th} input neuron is denoted as $e^{\theta_j^l}$ in the l layer, all neuron input is described as $\sum_k e^{\theta_k^l}$, j^{th} neuron output is stated as $\frac{e^{\theta_j^l}}{\sum_k e^{\theta_k^l}}$ constant is illustrated as e and indictor function is depicted as $l(.)$. The indicator function's result is one, when the brace value is true and the result of indicator function is zero, when the brace value is false. The rule items are added in $J(\theta)$ for preventing the local optimum falling. After the rule items are added, the equation (8) shows the softmax classifier's loss function as $J(\theta)$.

$$J(\theta) = -\left[\sum_{i=1}^{m}\sum_{j=1}^{k} l\left\{y^{(i)}=j\right\}\log\frac{e^{\theta_j^l}}{\sum_k e^{\theta_k^l}}\right]+\frac{\rho}{2}\sum_{i=1}^{k}\sum_{j=0}^{n}\theta_{ij}^2 \tag{8}$$

where, weighted term is denoted as $\frac{\rho}{2}\sum_{i=1}^{k}\sum_{j=0}^{n}\theta_{ij}^2$ and the excessive parameters are stabilized by using this weighted term in the training set. The output sum is normalized at the output layer by employing the softmax activation function, where one is added to all numbers at output neuron. The weight at the NN is updated by utilizing the learning function in the training phase and filters at the convolution layers of the RCNN method. In order to update the weights and filters, the activities loss is considered as input by the learning algorithm and propagates the error into the network. Finally, the output of the RCNN classifier predicted the user as either authorized user or unauthorized user from the input data. The next section will explain the validation of the RCNN with other techniques in terms of various parameters.

V. Results and Discussion

The dataset description, performance analysis of RCNN and comparative analysis of developed method is explained in this section, where the RCNN method is implemented in 3.0 GHz Intel i5 processor, with 4 GB RAM and 1 TB hard disk. The algorithm is designed by using Python language, where the performance metrics namely sensitivity, precision rate, False Negative Rate (FNR), F1-score and accuracy are used to validate the RCNN with different existing techniques. Initially, the collection of data in this research study is presented as follows.

A. Database Description

In this research study, three datasets such as CASIA A, B and OU-ISIR dataset are used to validate the performance of RCNN method. The gait video of CASIA-A dataset is collected in an outdoor environment with two alternate days. Four gait sequences are performed by involving 20 subjects in three distinct views as frontal, obliquely and laterally. Therefore, the dataset consists of total 240 gait sequences $\left(i.e\, 20\times4\times3\times240\right)$ the image resolutions of 352×240 that are recorded in 25 frames per second (fps). The average length of every sequence is about 90 frames, where 168 video sequences are used for training process and others for testing in this research study.

A 31 females and 93 males (total of 124) are used in this dataset, where USB cameras are used to record the gait videos for 11 various views in an indoor environment. Hence, this dataset is broadly used for multi-view gait recognition. The frame size of the recorded video is 320×240 at 25fps rate, where the difference of angle view direction for each video is 180 that are arranged as 0, 18, ..., 72, 90, ..., 162 and 1800. For multi-view video, gait sequences are recorded with three variations, which includes six video sequences for walk and finally, four video sequences by carrying bags and wearing a coat. The total video sequences is $10\times11\times124=13,640$ for CASIA-B dataset. The ratio of 70:30 is used for validation process and only 900 views are considered in this research study that consists of 1240 video sequences.

In order to collect the gait videos, 2135 males and 1872 females of total 4007 subjects with 1 to 94 years old ages are used in the OU-ISIR dataset. A gallery and probe are considered as two gait sequences for every subject. Four observation angles includes 550, 650, 750, 850are used to capture the gait sequences for each and every subject. In this dataset, variations are not provided for walking conditions and when comparing with CASIA-B dataset, the cross-view angle between gallery and probe is small. The performance of various gait recognition techniques are evaluated by using this dataset, because it consists of vast amount of subjects with different ages.

B. Parameter Evaluation

In this section, the performance metrics are discussed, which is used to test the efficiency of the proposed architecture system and also used to justify the practical developments of proposed RCNN method. There are five metrics namely accuracy, precision, F1-score, sensitivity and FNR are used to validate the performance of RCNN classifiers. The mathematical expression for this metrics are depicted in the following equations (9), (10), (11) and (12).

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN}\times100 \tag{9}$$

$$\Pr ecision=\frac{TP}{TP+FP}\times100 \tag{10}$$

$$Sensitivity=\frac{TP}{TP+FN}\times100 \tag{11}$$

$$F1-Score=\frac{2TP}{2TP+FP+FN} \tag{12}$$

where, True Positive is denoted as TP, True Negative is illustrated as TN, False Positive is described as FP and False Negative is depicted as FN in the above three equations.

C. Performance Analysis of Proposed Method for CASIA-A Database

In this section, the performance analysis of RCNN is validated with different classifiers includes Linear Support Vector Machine (LSVM), Quadratic-SVM (QSVM), Weighted K-Nearest Neighbour (WKNN) and FEcS-DNN [18] in terms of various parameters for CASIA-A database. Table I provides the validated results of RCNN in terms of accuracy, sensitivity, FNR, precision, and F1-score. Fig. 4 shows the graphical representation for precision and sensitivity, where Fig. 5 presents the validation results of FNR.

TABLE I. Experimental Analysis of Proposed Method for CASIA-A database

Methodology	**Parameters**				
	Sensitivity(%)	**Precision(%)**	**FNR**	**F1-score(%)**	**Accuracy(%)**
LSVM	97.67	98.0	1.9	97.83	98.1
QSVM	99.00	99.33	0.7	99.16	99.3
WKNN	96.67	96.67	3.6	96.67	96.4
FEcS-DNN	99.33	99.00	0.7	99.16	99.3
RCNN	99.59	99.47	0.2	99.50	99.9

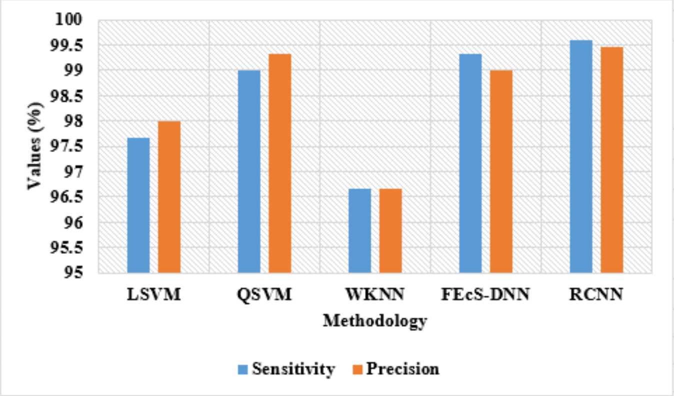


Fig. 4. Graphical Representation of Proposed RCNN in Terms of Sensitivity and Precision.

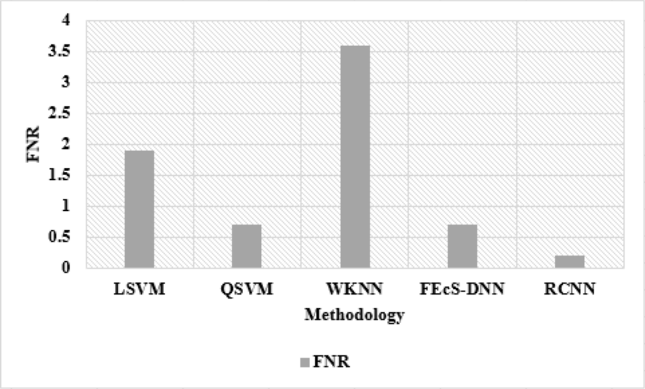


Fig. 5. Validation of Proposed RCNN by means of FNR.

The existing techniques WKNN and LSVM provides poor performance than other techniques, for instance, the WKNN achieved nearly 96% of sensitivity and precision, where LSVM achieved nearly 97.5% of sensitivity and precision. This is because, the WKNN works based on the weight calculation and LSVM's parameter are not effectively assigned. Therefore, FEcS-DNN method extracted spatial and temporal features and increased the performance such as it achieved nearly 99% of sensitivity and precision. However, the DNN method neglect the useful information for gait recognition, where the proposed RCNN method solved the issues of existing techniques. Hence, the proposed RCNN method achieved 99.59% of sensitivity and 99.47% of precision rate.

In the experiments of FNR on CASIA-A dataset, the WKNN method provided poor performance i.e. it obtained 3.6 FNR than other techniques. The existing LSVM obtained 1.9 FNR, where QSVM and FEcS-DNN obtained 0.7 FNR, because the existing techniques are affected by overfitting issues. But, the proposed RCNN method solved the overfitting problems by using the speed learning of residuals and obtained only 0.2 FNR. Fig. 6 illustrates the graphical results of proposed RCNN on the basis of F1-score and accuracy.

From the experimental analysis, it is proved that the proposed method achieved better performance than various classifiers for CASIA-A dataset. Among other techniques, the existing WKNN achieved poor performance, because the method classifies the extracted input based on weights calculations. When compared with FEcS-DNN technique (99.16% F1-score and 99.30% accuracy), the proposed method slightly increased the F1-score (i.e. 99.50%) and accuracy (i.e. 99.90%) values, this is because the Residual in the proposed method reduces the impact of vanishing gradients. The next section will discuss the performance analysis of proposed method for CASIA-B dataset.

D. Performance Analysis of Proposed Method for CASIA-B Database

Table II presents the performance analysis of RCNN method with LSVM, QSVM, WKNN and FEcS-DNN [18] for CASIA-B database. Fig. 7 presents the graphical results of RCNN in terms of precision and sensitivity, where Fig. 8 shows the FNR results of proposed method.

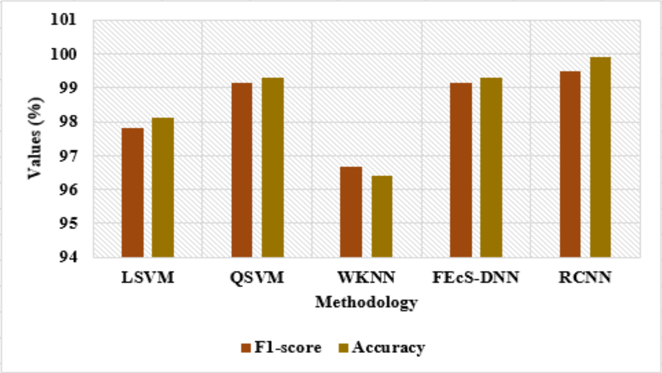


Fig. 6. Analysis of RCNN by means of F1-Score and Accuracy.

TABLE II. EXPERIMENTAL ANALYSIS OF PROPOSED METHOD FOR CASIA-B DATABASE

Methodology	**Parameters**				
	Sensitivity(%)	**Precision(%)**	**FNR**	**F1-score(%)**	**Accuracy(%)**
LSVM	71.75	73.00	28.2	72.37	71.8
QSVM	86.25	86.75	13.6	86.50	86.4
WKNN	66.25	66.75	33.7	66.50	66.13
FEcS-DNN	92.00	92.40	7.8	92.20	92.2
RCNN	94.16	95.47	4.1	94.68	97.9

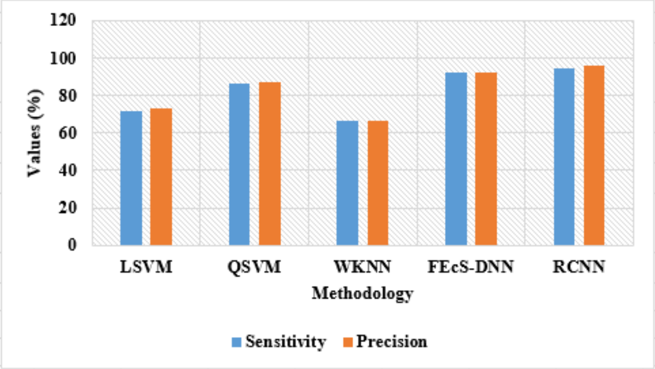


Fig. 7. Graphical Representation of RCNN in terms of Sensitivity and Precision

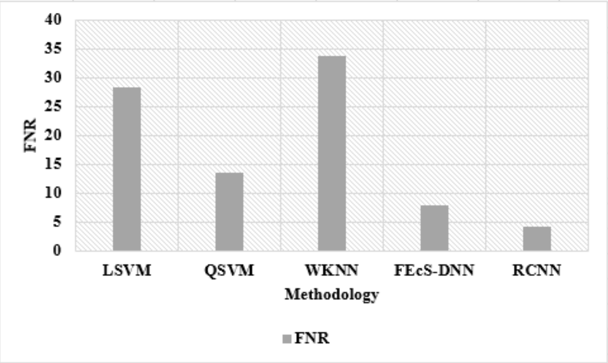


Fig. 8. Analysis of Proposed RCNN by means of FNR.

From the Table II, the experimental analysis shown that the proposed RCNN achieved better performance in terms of sensitivity and precision rate. The existing WKNN technique only provided poor performance than all other techniques, i.e. it achieved only 66% of sensitivity and precision rate. The QSVM and FEcS-DNN method achieved nearly 86-92% of sensitivity and precision rate, where the proposed RCNN achieved 94% of sensitivity and 95% of precision rate on CASIA-B dataset.

The WKNN method obtained high FNR rate (i.e. 33.7%), where LSVM and QSVM obtained 28.2 FNR and 13.6 FNR on CASIA-B dataset. When compared with existing FEcS-DNN technique, the proposed method obtained less FNR on CASIA-B dataset. However, the results showed that the RCNN method obtained 4.1 FNR due to practical usability issues are occurred during authentication. This leads to unauthorized users as genuine users and access the sensitive information of users in the smartphones. Fig. 9 represents the validated results of RCNN method by means of F1-score and accuracy.

The proposed RCNN method achieved less accuracy (i.e. 97.9%) due to high FNR values on this dataset. However, the proposed method achieved better performance than other existing techniques. For instance, the WKNN and LSVM achieved only nearly 66-72% of accuracy, where FEcS-DNN achieved only 92.2% accuracy. The reason behind the less accuracy is that the existing techniques are failed to represent the accurate temporal features and negation of some useful information. In order to achieve better gait recognition, the research study developed the RCNN method and extract the temporal and spatial features. The next section will describe the comparative analysis of RCNN on OU-ISIR dataset.

E. *Comparative Analysis of Residual Convolutional Neural Network*

In this section, the proposed method is compared with CNN with Chrono-gait image (CNN-CGI), SFN, TFN andSTDNN [15] in terms of accuracy for CASIA-B and OU-ISIR dataset. Table III shows the comparative analysis of proposed RCNN by means of accuracy. The graphical representation of accuracy is illustrated in Fig. 10.

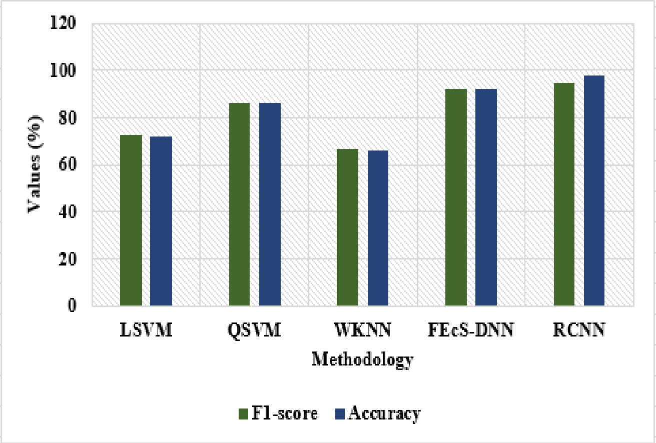


Fig. 9. Performance Analysis of Proposed RCNN in Terms of F1-score and Accuracy.

TABLE III. Comparative Analysis of Proposed RCNN in terms of Accuracy (%)

Methodology	Database	
	CASIA-B	OU-ISIR
CNN-CGI	89.83	91.42
SFN	92.17	92.64
TFN	93.26	93.87
STDNN	94.24	95.67
Proposed RCNN	97.90	98.15

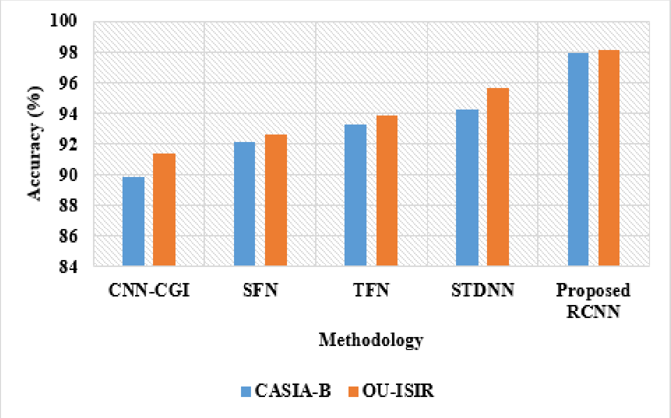


Fig. 10. Comparative Analysis of Proposed RCNN by means of Accuracy.

From the Table III, it is clearly stated that the proposed RCNN method achieved better performance for two datasets such as CASIA-B and OU-ISIR. Initially, the CNN-CGI achieved 91.42% accuracy for OU-ISIR than CASIA-B dataset, because a certain amount of temporal information is carried by CNN. However, the CNN-CGI method failed to represent the temporal features accurately, so the performance is degraded. The existing techniques includes SFN, STDNN and TFN achieved nearly 92%-95% accuracy in both datasets, because low-level edge features and spatial features were extracted. But, those existing techniques are suffered from over-fitting problems that leads to poor accuracy. Therefore, the research study developed the RCNN method, which achieved 97.90% accuracy on CASIA-B dataset and achieved 98.15% accuracy on OU-ISIR dataset. The developed method extract both spatial and temporal features and the overfitting problems are solved by RCNN method.

VI. Conclusion

A smartphone can be accessed by either authorized user or unauthorized user, therefore a human gait recognition is developed in this research study. A continuous authentication is important for accessing the smartphone, hence the developed architecture is suitable for applying on any operating system. The RCNN classifier is implemented in this study for improving the security of credential information from the unauthorized user access in smartphones. The experiments are conducted on three datasets such as CASIS-A, B and OU-ISIR dataset in terms of accuracy, sensitivity, precision, FNR and F1-score. The results proved that the RCNN method achieved 99.9% accuracy for CASIA-A, 97.9% accuracy for CASIA-B and 98.15% for OU-ISIR dataset, where the existing FEcS-DNN approach achieved only 99.3% accuracy for CASIA-A and 92.2% for CASIA-B dataset. The experimental results showed that the RCNN technique achieved 4.1% FNR for CASIA-B dataset, because the environmental conditions provide the practical usability issues at the time of authentication. Therefore, the genuine user can't able to access the smartphone at certain instance, because those users are misclassified due to usability issues. In future work, some efficient methodologies must be developed to address the practical usability issues during authentication.

References

[1] M. Gomez-Barrero, C. Rathgeb, G.Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters", Information Fusion, vol.42, pp.37-50, 2018.

[2] M. M. Al Rahhal, M. L. Mekhalfi, M. Guermoui, E. Othman, B. Lei, and A. Mahmood, "A Dense Phase Descriptor for Human Ear Recognition", IEEE Access, vol.6, pp.11883-1187, 2018.

[3] S. A. Bargal, A. Welles, C. R. Chan, S. Howes, S. Sclaroff, E. Ragan, and C. Gill, "Image-based Ear Biometric Smartphone App for Patient Identification in Field Settings", In: Proc. of 10th International Conf. On VISAPP, vol.3, pp.171-179, 2015.

[4] C. Cintas, M. Quinto-Sánchez, V. Acuña, C. Paschetta, S. De Azevedo, C. C. S. de Cerqueira, and S. Canizales-Quinteros, "Automatic ear detection and feature extraction using geometric morphometrics and convolutional neural networks", IET Biometrics, vol.6, pp.211-223, 2016.

[5] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Expert Systems with Applications, vol.42, pp.8198-8211, 2015.

[6] R. Venkatesh, N. U. Maheswari, and S. Jeyanthi, "Multiple Criteria Decision Analysis Based Overlapped Latent Fingerprint Recognition System Using fuzzy Sets", International Journal of Fuzzy Systems, vol.20, pp.2016-2042, 2018.

[7] E. J. Ragan, C. Johnson, J. N. Milton, and C. J. Gill, "Ear biometrics for patient identification in global health: a cross-sectional study to test the feasibility of a simplified algorithm", BMC research notes, vol.9, pp.484, 2016.

[8] N.Geethanjali, and K. Thamaraiselvi,"Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System", International Journal of Computer Applications, vol. 70, pp. 14 2013.

[9] X. Li, Y. Yin, Y. Ning, G. Yang, and L. Pan, "A hybrid biometric identification framework for high security applications", Frontiers of Computer Science, vol.9, pp.392-401, 2015.

[10] X. Wang, and W. Q. Yan, "Cross-view gait recognition through ensemble learning", Neural Computing and Applications, pp. 1-13, 2019.

[11] U. Martinez-Hernandez, and A. A. Dehghani-Sanij, "Adaptive Bayesian inference system for recognition of walking activities and prediction of gait events using wearable sensors". Neural Networks, vol. 102, pp. 107-119, 2018.

[12] J. P. Singh, S. Jain, S. Arora, and U. P. Singh, "Vision-based gait recognition: a survey". IEEE Access, vol. 6, pp. 70497-70527, 2018.

[13] X. Li, Y. Makihara, C. Xu, Y. Yagi, and M. Ren, "Joint Intensity Transformer Network for Gait Recognition Robust Against Clothing and Carrying Status", IEEE Transactions on Information Forensics and Security, vol. 14, pp. 3102-3115, 2019.

[14] N. Takemura, Y. Makihara, D. Muramatsu, T. Echigo, and Y. Yagi, "On input/output architectures for convolutional neural network-based cross-view gait recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, pp. 2708 – 2719,2017.

[15] S. Tong, Y. Fu, X. Yue, and H. Ling, "Multi-view gait recognition based on a spatial-temporal deep neural network". IEEE Access, vol. 6, pp. 57583-57596, 2018.

[16] I. Huitzil, L. Dranca, J. Bernad, and F. Bobillo, "Gait recognition using fuzzy ontologies and Kinect sensor data", International Journal of Approximate Reasoning, vol. 113, pp. 354-371, 2019.

[17] X. Wang, J. Zhang, and W. Q. Yan, "Gait recognition using multichannel convolution neural networks", Neural Computing and Applications, pp. 1-11, 2019.

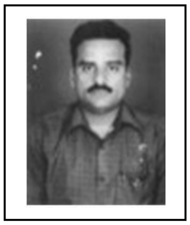
[18] [18] H. Arshad, M. A. Khan, M. I. Sharif, M. Yasmin, J. M. R. Tavares, Y. D. Zhang, and S. C. Satapathy, "A multilevel paradigm for deep convolutional neural network features selection with an application to human gait recognition", Expert Systems, pp. e12541, 2020.

[19] H. Gao, B. Cheng, J. Wang, K. Li, J. Zhao, and D. Li, "Object classification using CNN-based fusion of vision and LIDAR in autonomous vehicle environment". IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4224-4231, 2018.

[20] A. Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton,"Imagenet classification with deep convolutional neural networks",Advances in neural information processing systems, pp. 1-9, 2012.

Authors' Profile

Gogineni Krishna Chaitanya research scholar received his Bachelors Degree in Computer Science from Acharya Nagarjuna University and Masters Degree from JNTUK. He is currently pursuing Ph.D degree with Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502 Andhra Pradesh, India. His research interests include digital forensics, Biometrics, Authentication and Machine Learning.



Dr. K Raja Sekhar received his Ph.D Degree in Computer Science and Engineering from Acharya Nagarjuna University. He is currently a Professor with the of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502 Andhra Pradesh, India. He has published more than 50 articles in journals and Conference proceedings. His research interests include Digital forensics, Biometrics, Network Security and Usable security. He received several Excellence awards and several best paper awards. He has been on the editorial boards of several journals.