IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Deep Learning Based Biometric Authentication Using Finger Veins

G.S.D.Saran[1], L . Sai Kiran[2], B. Mukesh[3], B. Sai[4]

Mrs. P. Bhavana (Assistant Professor), Department of ECE , Sasi Institute of Technology And Engineering , Tadepalligudem , 534101

Abstract: The biometric authentication is improved over the recent last years to enhance the security. Face Recognition and AI based authentication are regular models to validate the human presence.

The attackers can hack the above mentioned biometrics so that there is a need to protect the users data with other biometrics like Finger Veins . In this work, we are proposing that Finger Veins as they are presented under the skin so there is less chance to hack and also economically viable. The feature extraction and registration process is carried out by the deep learning techniques like Convolution neural networks (CNN).

INTRODUCTION

Biometrics, derived from the Greek words "Bio" (meaning life) and "Metric" (to measure), represents a pioneering field offering a compelling solution for person recognition. Biometric systems stand as robust, highly secure, and inherently natural alternatives for verifying one's identity. The central objective of these systems revolves around the automation of human identification processes. Unlike traditional methods reliant on easily manipulated or compromised means such as badges, personal identification numbers (PINs), passwords (which can be words or phrases), and ID cards, biometric systems rely on an individual's distinctive physiological traits (e.g., fingerprint, iris, vein patterns, hand geometry, and ear shape) or behavioral characteristics (e.g., gait, signature, and keystroke dynamics)[1]. Identity verification systems have become indispensable in various domains, encompassing account logins, online payments, and automated teller machines (ATMs). These technologies are designed to safeguard user privacy and information security. The classical password, though widely used, suffers from drawbacks such as protracted

BIOMETRIC SYSTEM PERFORMANCE EVALUATION

The evaluation of biometric systems' performance represents a pivotal and indispensable facet in the design and architecture of biometric recognition systems. This section delves into the techniques for analyzing biometric systems and elucidates various metrics and graphical representations that shed light on the intricacies of biometric system operations. As previously alluded to, biometric systems can be categorized into two primary modes: verification and identification. It is imperative to differentiate between these two modes, as they exert substantial influence on the evaluation of performance.

The field of biometrics offers an array of solutions for addressing image classification problems [15]. These methods are adaptable to classification problems involving two or more classes, and the performance of classifiers is contingent upon the number of samples per class and their composition. Consequently, the choice of the most suitable method hinges on the specific requirements of the targeted application. A pragmatic approach involves initial method selection, followed by rigorous testing and subsequent evaluations.

In data analysis, the initial step typically involves the construction of an array representation known as a "confusion matrix." This table (Table 2.3) quantifies the number of predictions, denoted as *Xi, j* (or X class, prediction), representing samples of class *i* assigned to class *j* among a set of *C* classes. The number of samples constituting class *i* is denoted as *Ki*, and the total number of predictions attributed to this class is referred to as

		Prediction			Total /Classes
		Classi	*Classi*	*Classc*	
	Classi	Xl,1	*X,*	*X1,c*	K1
Real Class	*Class2*	$X_{i,1}$	$X_{i,i}$	$X_{i,c}$	*Ki*
	Classc	$X_{c,1}$	$X_{c,i}$	$X_{c,c}$	*Kc*
Total Predictions		*Mi*	*Mi*	*Mc*	I

Table 2.3: Prediction Confusion Matrix of a C-Class Classifier

		Prediction		Total /Classes
		Positive Class	Negative Class	
Real Class	Positive Class	Tp	Fn	P
	Negative Class	Fp	Tn	N
Total Predictions		P_{pos}	P_{neg}	I

Table 2.4: Prediction Confusion Matrix of a C-Class Classifier

Mi. The sums of *Ki* and *Mi* collectively amount to the total number of samples (I).

With this context, for each class i, treated as a binary problem (Class *i* as positive, all other classes *i* E *j* as negative), or directly for a two-class problem, the predictions can be classified into four principal categories:

1. **True Positive (Tp)**: Samples of the positive class (i) correctly classified (X,i).

2. **False Negative (Fn)**: Samples of the positive class (i) incorrectly classified ((X,y ,V $_i$E *j*).

3. **True Negative (Tn)**:Samples of the negative class *(j)* correctly classified (X,t,V *t*6 [1,*C*]E*i*).

4. **False Positive (Fp)**: Samples of the negative class (j) incorrectly classified (X, ,V j E i).

In the case of a problem with *N* classes, treated individually as binary problems, confusion matrices are constructed for each class i. The confusion matrix for a two-class problem establishes a connection between the total number of samples (P) from the positive class, the total number of samples (N) from the negative class, and the four aforementioned categories, which in turn determine the total number of samples classified as positive (Ppos) and negative (Pneg).

Various measures can be derived from a confusion matrix, from the problem with Two-classes we can describe the following metrics:

- False Acceptance Rate (FAR): Defined as the probability that the biometric security

- system mistakenly accepts an access attempt by an unauthorized user.

FAR = ^ (2.1)

Tn + *Fp* *N*

- False Rejection Rate (FRR): Defined as the probability that the biometric security system mistakenly reject an access attempt by an authorized user name.

$$FRR = \frac{Fn}{Tp + Fn} = \frac{Fn}{P} \quad (2.2)$$

- Sensitivity: is calculated as the number of correct positive predictions divided by the total number of positives. It is also called recall or True Positive Rate or Genuine Acceptance Rate (GAR) witch is given by $GAR = 1 - FRR$.

$$Sensitivity = \frac{Tp}{Tp + Fn} = \frac{Tp}{P} \quad (2.3)$$

- Specificity: is calculated as the number of correct negative predictions divided by the total number of negatives. It is also called true negative rate. It can also be calculated by (1 - *speci ficity* = *FAR)*.

$$Specificity = \frac{Tn}{Tn + Fp} = \frac{Tn}{N} \quad (2.4)$$

- Precision: is calculated as the number of correct positive predictions divided by the total number of positive predictions. It is also called positive predictive value.

$$Precision = \frac{Tp}{Tp + Fp} = \frac{Tp}{Ppos} \quad (2.5)$$

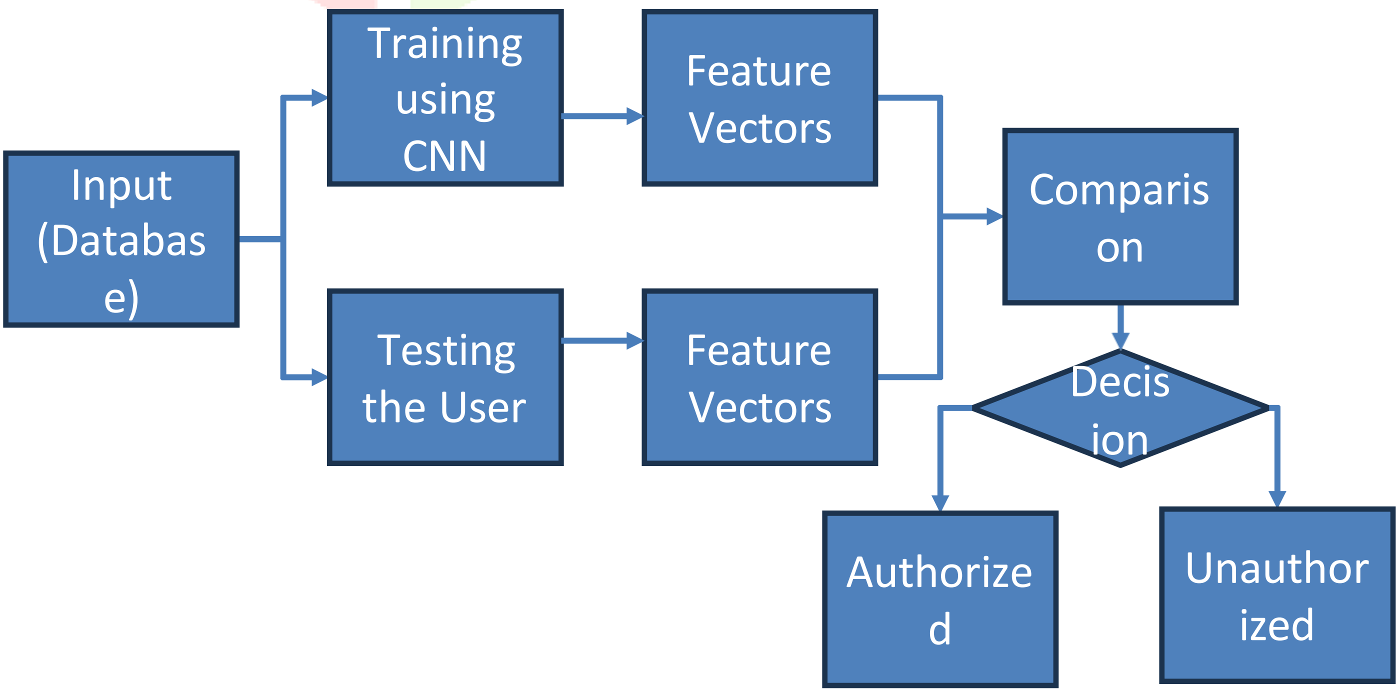
- Equal Error Rate *(EER):* is calculated as the number of all incorrect predictions divided by the total number of the classes. *EER* defined also as the best compromise between *FAR* and *FRR* .
The best error rate is 0.0, whereas the worst is 1.0.

$$EER = \frac{Fp+Fn}{Tp + Tn + Fp + Fn} = \frac{Fp + Fn}{P + N} \quad (2.6)$$

- **Accuracy (ACC)**: is calculated as the number of all correct predictions divided by the total number of the dataset. The best accuracy is 100%, whereas the worst is 0.0.

$$ACC = \frac{Tp + Tn}{Tp + Tn + Fp + Fn} \quad (2.7)$$

Each of this metrics has a percentage describing a certain capability of the model.



Proposed Block Diagram

Results

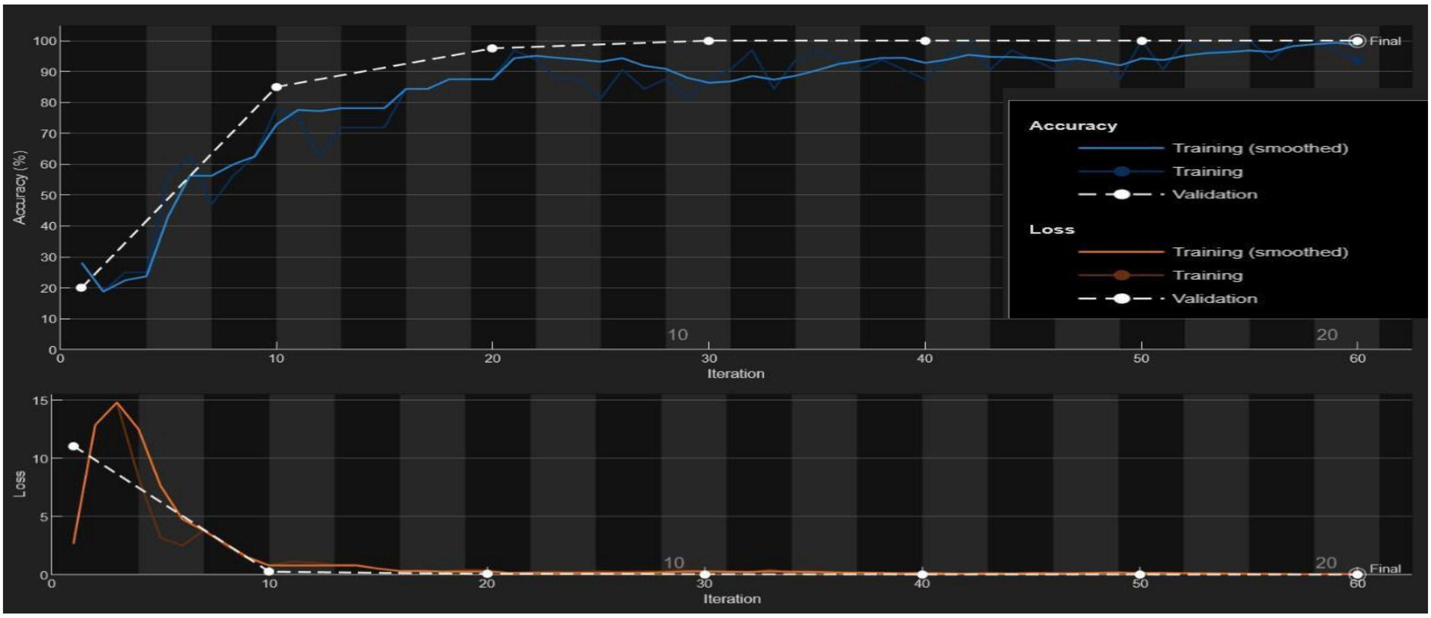


Fig:output graphs

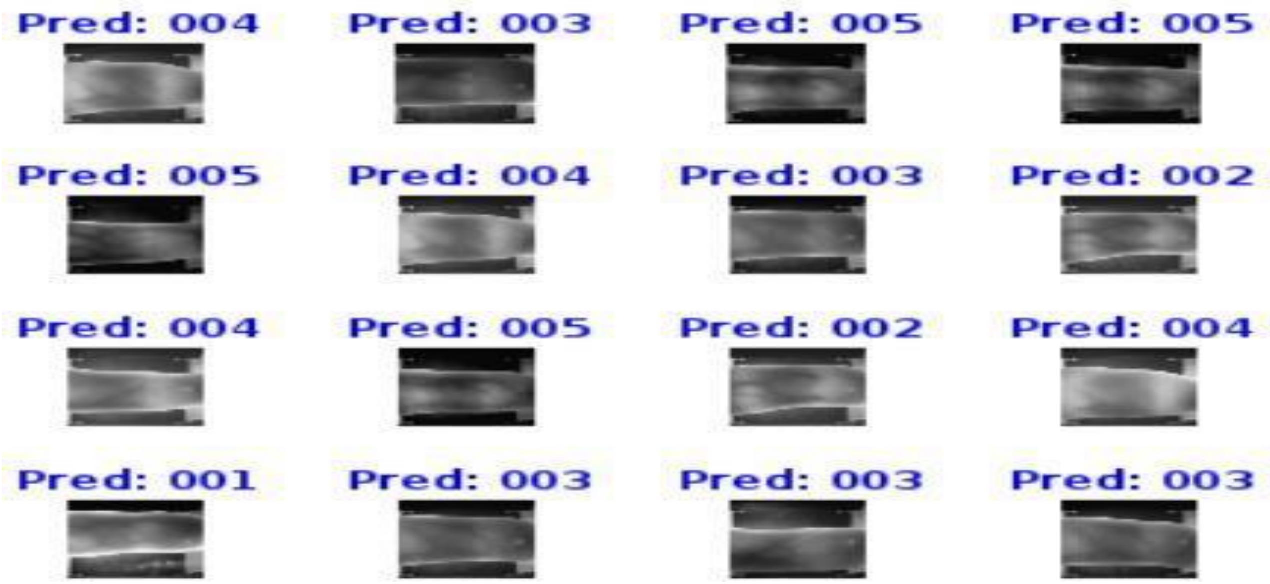


Fig: fingervine image predctions

Command Window

Training on single CPU.
Initializing input data normalization.

Epoch	Iteration	Time Elapsed (hh:mm:ss)	Mini-batch Accuracy	Validation Accuracy	Mini-batch Loss	Validation Loss	Base Learning Rate
1	1	00:00:24	25.00%	35.00%	2.5590	6.5444	0.0010
4	10	00:00:29	78.12%	97.50%	0.8947	0.1291	0.0010
7	20	00:00:33	93.75%	97.50%	0.2759	0.0479	0.0010
10	30	00:00:37	100.00%	100.00%	0.0517	0.0199	0.0010
14	40	00:00:40	90.62%	100.00%	0.1558	0.0040	0.0010
17	50	00:00:44	93.75%	100.00%	0.1648	0.0014	0.0010
20	60	00:00:48	100.00%	100.00%	0.0434	0.0005	0.0010

Training finished: Max epochs completed.
Test Accuracy: 100%
>>

Fig: accuracy table

Methodology	Accuracy (%)	(FAR)	(FRR)	Execution Time (ms)
Traditional Feature-Based (SIFT)	85.3	2.1	4.5	120
Deep Learning-Based (ResNet-50)	92.5	1.4	3.2	95
Proposed CNN Model	97.8	0.8	2.0	60

Performance Comparison

CONCLUSION

The field of biometric security systems has witnessed remarkable advancements and a shift toward more secure, efficient, and convenient methods of personal identification. Security has grown increasingly crucial in recent years. The Finger Vein Authentication System has attracted our interest due to its robustness, consistency, and high level of performance.

Biometrics, such as fingerprint and iris biometrics, have a lower level of reliability. Finger vein authentication removes the possibility of tampering since it relies on the fact that each person's veins are distinct, even if they are identical twins, and reside beneath the skin their whole lives. In recent years, a number of deep learning algorithms have greatly increased the ability to recognize finger vein patterns. Finger vein authentication and the deep learning approaches used to build the Finger Vein Recognition system are the major objectives of this manuscript..

REFERENCES

[1] **Anil K. Jain, Aran A. Ross, and Karthik Nandakumar.** *Introduction to Biometrics.* **Springer US, 2011.**

[2] **Anil K Jain, Aran Ross, and Salil Prabhakar. An introduction to biometric recognition.** *IEEE Transactions on circuits and systems for video technology,* **14(1):4- 20, 2004.**

[3] **Uday Bhanu Ghosh, Rohan Sharma, and Abhishek Kesharwani. Symptomsbased biometric pattern detection and recognition. In** *Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis,* **pages 371-399. Springer, 2022.**

[4] **Kejun Wang, Hui Ma, Oluwatoyin P Popoola, and Jingyu Li. Finger vein recognition.** *Biometrics,* **pages 31-53, 2011.**

[5] **Xinwei Qiu, Wenxiong Kang, Senping Tian, Wei Jia, and Zhixing Huang. Finger vein presentation attack detection using total variation decomposition.** *IEEE Transactions on Information Forensics and Security,* **13(2):465-477, 2017.**

[6] **Changxing Ding and Dacheng Tao. Pose-invariant face recognition with homography-based normalization.** *Pattern Recognition,* **66:144-152, 2017.**

[7] **Maneet Singh, Richa Singh, and Arun Ross. A comprehensive overview of biometric fusion.** *Information Fusion,* **52:187-205, 2019.**

[8] **Chuck Wilson.** *Vein pattern recognition: a privacy-enhancing biometric.* **CRC press, 2010.**

[9] **Shaveta Dargan and Munish Kumar. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities.** *Expert Systems with Applications,* **143:113114, 2020.**

[10] **Bir Bhanu and Venu Govindaraju.** *Multibiometrics for human identification.* **Cambridge University Press, 2011.**

[11] **Zahid Akhtar, Abdenour Hadid, Mark S Nixon, Massimo Tistarelli, Jean-Luc Dugelay, and Sebastien Marcel. Biometrics: In search of identity and security (q & a).** *IEEEMultiMedia,* **25(3):22-35, 2018.**

[12] **Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, and Fabio Roli. Fingerprint liveness detection using local texture features.** *IETBiometrics,* **6(3):224-231, 2017.**

[13] **Muhammad Sharif, Mudassar Raza, Jamal Hussain Shah, Mussarat Yasmin, and Steven Lawrence Fernandes. An overview of biometrics methods. In** *Handbook of Multimedia Information Security: Techniques and Applications,* **pages 15-35. Springer International Publishing, 2019.**

[14] **Abdenour Hadid, Nicholas Evans, Sebastien Marcel, and Julian Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned.** *IEEE Signal Processing Magazine***, 32(5):20-30, 2015.**

[15] **Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing.** *Advances in biometrics for secure human authentication and recognition.* **CRC Press, 2013.**

[16] **Yang Liu and Elizabeth Shriberg. Comparing evaluation metrics for sentence boundary detection. In** *2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07,* **volume 4, pages IV-185. IEEE, 2007.**

[17] **Zhi Liu, Yilong Yin, Hongjun Wang, Shangling Song, and Qingli Li. Finger vein recognition with manifold learning.** *Journal of Network and Computer Applications,* **33(3):275-282, 2010.**

[18] **Jian-Da Wu and Chiung-Tsiung Liu. Finger-vein pattern identification using principal component analysis and the neural network technique.** *Expert Systems with Applications,* **38(5):5423-5427, 2011.**