iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55816

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Standardized, Enhanced and Robust Automated Fingerprint Recognition using CNN

Gautham Jayakrishnan[1], Ashwin Nair[2], Vishal Vinod Kumar[3], Dr. Suresh[4]
[1, 2, 3]*UG Student,* [4]*Assistant Professor, SRM Institute of Science and Technology, Chennai*

Abstract: ***In recent years, biometric authentication systems have seen rapid development in various industries, and they continue to provide high security functions for access control systems. Many types of unimodal biometric authentication systems have been developed. However, these systems can only provide a low to moderate range of security features. Therefore, a combination of two or more unimodal biometrics (multiple modalities) is required to achieve higher security capabilities. To achieve higher accuracy, this article uses generalized probabilistic learning model algorithm for processing finger vein images. Image preprocessing is done with the help of finger vein image database to prepare it for further processes of feature extraction and matching. It then uses generalized probabilistic learning model algorithm to find the feature points. algorithm is used to match the features to obtain the image information and determines the final identity according to the sparse distribution. Compared with other machine learning methods for finger vein detection, the proposed method has a higher accuracy rate.***
Index Terms: Biometric, Biometric Authentication, Convolutional Neural Network, Fully Convolutional Network

I. INTRODUCTION

Typically, a good biometric has a number of essential characteristics. It should first be inclusive. This indicates that most users or apps can utilize the biometric. Biometric technology as it is now cannot guarantee that it will work for every user. So, we must increase the biometrics' capacity to be applied to the majority of consumers. High differentiating capacity is the second essential component of a good biometric. Certain biometric technologies are used to monitor human health or for delicate security purposes. High biometric differentiating accuracy must be clearly essential and crucial; otherwise, the items will not only be pulled from the market but will also suffer catastrophic repercussions, including loss of life and property. Permanent is the third crucial component of biometrics. It implies that biometric tools can effectively and efficiently observe and gather users' vital bodily characteristics. Most of the time, these qualities cannot be altered or eliminated. Certain important physical traits, however, are not truly monotonous and permanent. We thus expect that the ideal biometric will acquire characteristics that are as steady and unchanging as feasible in practice. Collectability is the fourth essential quality of a perfect biometric. It implies that the biometric should be able to effectively gather the necessary traits and data from users.In addition, the high cost of manufacture makes regular biometrics difficult to hedge. Greater production costs are frequently associated with higher authentication accuracy. Nevertheless, the cost is great to bear after the bond has been broken. I thus intend to explore this.Biometric systems are developing and becoming better very quickly. The usage of contactless biometric devices, which were previously anticipated to be extensively used in, has been significantly accelerated by the current SarS-COV epidemic. The real-world uses for biometric systems are fairly varied and include everything from offline smartphone identification to airport security to facial detection for virtual , of demographics, races, and genders. Hence, it is crucial to make sure that the systems in use can handle all of their potential users fairly and equally. The terms bio (life) and metron (a measure) are combined to form the word biometrics, according to Morris' definition. In other words, it involves doing measurement and analysis using physical characteristics and behavioral clues. This definition has persisted over time, and its uses have changed as well. The three main functions of these systems are enrollment, authentication, and identification. Users can enrol to add their biometric information to a gallery and link it to their identities. Authentication gets a user's identity claim and biometric data, verifies the information given by the user and the information in the gallery associated with the claimed identity. At the end, identification only gets the biometric information and attempts to match it with every identity in the gallery , if no match is made, it returns no identity. Among these projects. The system can be secured by supplementary duties like presentation attack detection and morphing assault detection. As was already established, the widespread use of biometrics suggests that all of these technologies reliably identify and authenticate people.

II. EXISTING METHODOLOGY

This paper presents a basic overview, key parameters, and enhancement protocols of the Time Efficient Stream loss tolerant Authentication (TESLA) protocol.

The now in use system comparing TLI TESLA theoretically to the formerly suggested standards for security services and shown that the new protocol reduces DoS attacks on the network and prevents excessive use of the buffer in the sensor node. Additionally, as compared to earlier TESLA Protocols, it ensures continuous packet receipt and speeds up with minimal latency, the authentication procedure of the transmitted message. The current system addressed the TESLA protocol implementation challenges and offered the most recent solutions and parameter choices for boosting the TESLA protocol efficacy. A further focus of the current research was on using biometric authentication as a potentially effective replacement for public cryptography in the authentication procedure. Doing a security study of the TLI TESLA protocol and comparing its time complexity to alternative TESLA protocols. carrying out a theoretical study on the parameters chosen to assist the TLI TESLA protocol perform at its peak. Presenting a biometric authentication method as a replacement for PKI for the purpose of creating the first authentication settings for the TLI TESLA protocol. The following example illustrates another benefit of this protocol: If an attacker is successful in making a fake receiver key, all messages or keys provided for verification will be compromised by that single point of failure. A limit for the greatest number of authentication messages from the base station that fail due to errors will be set by the receiver in the protocol. The receiver sends a request to the server to update key whenever it reaches the threshold value. After that, the key server goes through the time intervals that the base is interacting with that receiver and then broadcasts the key appropriate for those intervals. The receiver next uses a key it has just received to verify the message sent by the base station. In these circumstances, the protocol replaces the existing key with a key that is new since the message's successful authentication shows that the previously stored key is malicious. A crucial step is to secure the communication path between the key server and the receiver. The key server receives a request from receiver and notifies the base that the key needs to be updated. The base will then broadcast a message that contains a new key that will be used to communicate with the receiver. At some point after that, the key server will eventually transmit a symmetric key that will be used to encrypt that message. After a certain amount of time, the server divulges the key, enabling the receiver to extract the new key for interacting with the key server and authenticating both parties.

Drawbacks of Existing System-The existing information system has several drawbacks that limit its functionality. Firstly, the system's learning phase may not cover the entire scope of its behavior, leaving gaps in its understanding. Additionally, the system's knowledge is often narrowly specialized, which can limit its practical application. The computation burden of the system may also hinder its use in real-life scenarios, as it can be too demanding. Furthermore, the system typically has high polynomial running times, which can slow down its performance. Lastly, there may be a lack of synchronization between the training and test data, leading to potential errors and inaccuracies. These limitations highlight the need for improvements to the system's design and functionality to overcome these drawbacks and enhance its effectiveness. have lengthy polynomial running durations in general. Cost of adding complexity to the analysis. does not use a fingerprint's local and global properties to create an identification. May blow up computationally. Time and memory use are too expensive.

III. PROPOSED METHODOLOGY

Individuals are automatically recognized by biometric identification systems based on their biological and behavioral traits. They typically consist of four subsystems that enable the collection, processing, and comparison of biometric samples from individuals to determine whether or not those individuals are recognized. Biometric data is defined as a biometric sample or an aggregate of biometric samples at any stage of processing.

1) *Data Capture:* Using capture devices, it obtains biometric samples of people.
2) *Signal Processing And Feature Extraction:* These techniques work to extract a collection of prominent or discriminating characteristics (i.e., a feature vector) from the collected biometric data.
3) *Comparison:* It compares the stored biometric data y with the collected biometric data x to get similarity scores s = S(x y) based on various S similarity functions. The system determines whether two biometric feature vectors are from the same subject (a match) or from distinct subjects (a nonmatch) based on similarity ratings.

A pore feature-based method to biometric identification is presented in this research. Our technique uses convolutional neural network [CNN] modelling to detect gaps in the input fingerprint image. A region around each discovered pore is then given a CNN-based description. In particular, we created a CNN that learns discrete feature representation from pore patches via residual learning. By comparing the pore descriptors collected from two fingerprint photos in a bi-directional way, a matching score is created as proof. The network effectively creates an image sample from an actual low-resolution fingerprint sample after jointly learning a distinguishing feature representation from it. We combined characteristics from authenticating fingerprints to providing originality and selective data on each topic. In order to maximise the utilisation of extracted features, we additionally incorporate loss of ridge rebuilding employing ridge patterns. The identification issue is resolved by our suggested solution by enhancing fingerprint picture quality.

The efficiency of our suggested model is demonstrated by the The developed specimens exhibit outstanding recognition accuracy, which is virtually as good as the high-resolution original photographs.

IV. LITERATURE REVIEW

This study by Song-Kyoo Kim , Chan Yeob Yeun and Paul D. Yo., focuses on the use of machine learning for digital health in the domain of data secured by biometric technology.. The hazards of the conventional authentication techniques include. Loss, omission, and theft. Biometric authentication technology has progressed and is now used extensively. The suggested system's effectiveness in utilising a confusion matrix has been assessed, and with the use of compact data analysis, it has demonstrated up to 95% accuracy. The upper-range control limit using mean square error (MSE) is implemented using the AmangECG toolkit in MATLAB. (UCL), which has a direct impact on the quantity of approved samples, accuracy, and OP for three authentication performance parameters. On accordance with this methodology, it was discovered that OP may be increased by using a 0.0028 of UCL, that denotes 61 approved samples out of 70 of samples and guarantees the suggested validation system would reach 95% accuracy. Systems for biometric authentication provide a number of benefits over conventional ones. Also, the effectiveness of the suggested security mechanism was assessed using both an overall performance measure and a confusion matrix. It is discovered that 0.0028 of UCL, or 61 samples which are approved out of 70 with 95% accuracy on authentication, might optimise the OP.

The study by Anthony Ngozichukwuka Uwaechia and Dzati Athiar Ramli focuses on ECG which refers to electrocardiogram, a highly selective biometric feature, has recently attracted a lot of attention as a potential biometric trait. Unfortunately, ECG readings can be affected by a variety of sounds, including fundamental swaying, Interference with power lines, and Noises featuring high and low frequencies, making it difficult to implement accurate and reliable biometric identification systems. ECG signal denoising is therefore a significant preprocessing step and is essential for ECG-based biometric person identification. It is a very difficult problem to integrate various processes of ECG signal analysis for biometric recognition, preprocessing, extraction of features, selection of features, feature alterations, and classification are some examples. On the basis of an effective difference image projection, the vein line features were extracted at different scales. A quick Hamming distance implementation is used to match the probe images and the extracted gallery features. This method was easy to use and understand, but it was unable to recognize relationships between variables, and it was more likely to stumble upon a local optimum than randomized algorithms.

The study by Hailong Yao , Caifen Wang , Xingbing Fu , Chao Liu , Bin Wu and Fagen Li requires the technique cannot offer forward security or user privacy since it is susceptible to smart card loss attacks, threats based on off-line prediction and impersonating. We suggest a novel remote biometric authentication technique [RRBAS] based on ring learning with errors [RLWE] for one and multi-server contexts to overcome these problems. For multi-server situations, RRBAS is the first remote biometrics identification system built around a lattice. According to security analysis, RRBAS can offer post-quantum security, thwart known security threats, and fulfilthe random oracle's verified key exchange (AKE) security paradigm. The results of the Comparative examination and evaluation of experimentation demonstrate that the computational effectiveness of RRBAS is superior to that of Lamo et al.,whereas communication effectiveness is reduced in a smaller amount than traditional schemes due to the massive-size ciphertext of the lattice-based cryptosystem. Nonetheless, it can accomplish session key agreement in single-server and multi-server environments.

V. MODULE DESCRIPTION

There are 3 different modules present in this research. They are:

1) *Image Preprocessing*-Digital picture contrast adjustment is a point process that applies an equal constant value to each pixel in the image (either by addition, subtraction, multiplication, or division). This lesson examines how contrast-deficient digital photos may be improved by dispersing brightness values using contrast stretching and histogram normalising methods.
2) *Image Data Generator*-The era of data is now. And occasionally we have a high memory need due to the enormous volume of data that is surface. A vast quantity of data would be required to train a deep learning model in order for it to produce anything useful. But, if the data were really large, it would not be feasible to load it all into our memory due to memory constraints. If we put all of the data into memory, we most likely will run out of space. So, we need to find a different approach rather than putting the entire data set into RAM. To do this, we will develop a class called DataGenerator that will inherit from the keras.utils.sequence class.
3) *Model Creation and Training*-We create a system that starts with a lot of convolution layers, moves on to layers that are now channel-sampled [pooled] before becoming fully connected.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Input Layer: The training process begins by transforming the user's input picture into an array of a predetermined size, such as 160x160x1, where 160 denotes the pixel value for the image's height and width denotes the black and white channels. To extract picture properties like edges, colour, brightness, etc., a convolutional layer is used.
This process involves using several filter or kernel types, as illustrated below in the supplied picture, which may automatically train themselves to discover particular locations in an image through numerous rounds. A feature map is then produced, going through several levels once again.

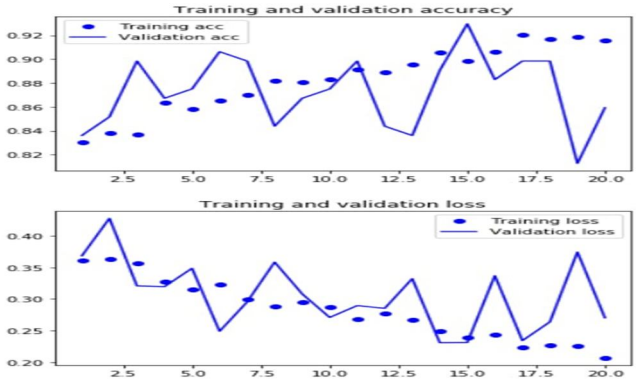


Fig 1 Training and validation accuracy graphs

Relu Activation Function: Rectified Linear Unit is known as Relu, and its activation function. This layer produces the value f(x) = max (0, x). By changing all the negative values to 0, this is used to produce the feature map linearity. Moreover, there are various other activation processes like sigmoid, tanh, etc. Every convolutional layer and every dense layer in our design have been subjected to the ReLU activation function. The three fundamental dimensions are height, breadth, and depth, or m * m * r in which each layer's insert x is structured in a computational neural network [CNN] model, height (m) equals width (m). The channel number and depth are both used interchangeably. The RGB photograph's depth (r), for instance, consists of three. Similar to its input picture, the accessible kernels (filters) for each convolutional layer are denoted using the character k and have three dimensions (n * n * q).Yet, in this scenario, n has to be smaller than m, and q has to be equal or less than r. The kernels act as a framework for local connections, which construct a k map of features h of size [mn1] for each and then convolve the input data applying the identical characteristics [bias b and weight W].

VI. CONCLUSION AND FUTURE ENHANCEMENTS

Even with the use of several methods, the identification of fingerprint fragments has proven to be a difficult task. This is especially true in the field of forensics, where fingerprint fragments are frequent and their recognition is crucial. Image binarization thinning and noise reduction are part of the first fingerprint processing. The minutia points are matched by applying the score matching approach with fingerprint recognition. Using the correlation between local embeddings produced from intermediate feature maps of two fingerprint pictures, we added a realignment stage that consistently enhanced the performance of all models, notably in difficult circumstances (e.g. partial overlap between the fingerprint images). No further training is necessary for this realignment technique, which may be used as a wrapper for any deep learning network. Future research will focus on enhancing the realignment approach to lessen the delay brought on by the existing implementation of brute force correspondence. To more intelligently aggregate two sets of local embeddings, we will research the usage of attention and/or graphical neural networks.

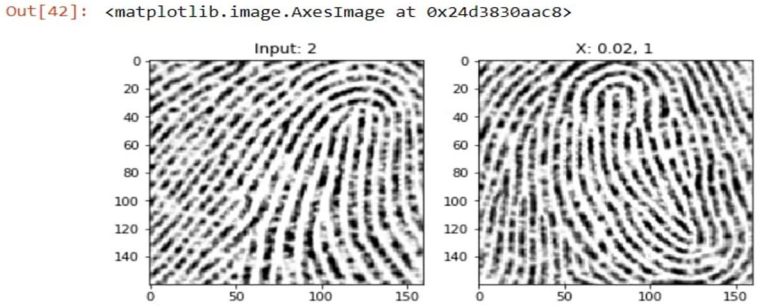
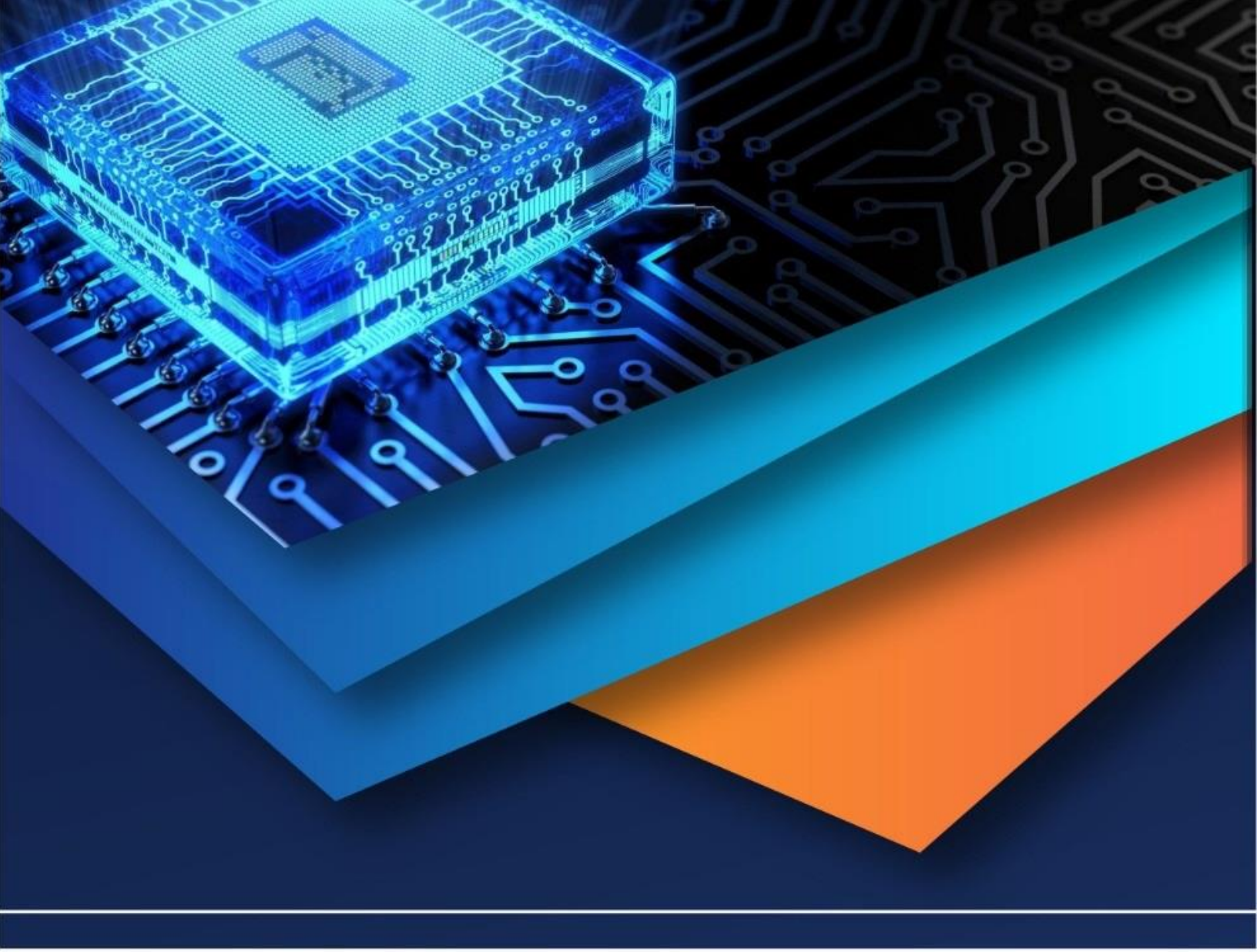


Fig 2 Final result

REFERENCES

[1] F. Agraoti, F. M. Bui, and D. Hatzinakos, Secure telemedicine: Biometrics for remote and continuous patient verication, J. Comput.
[2] E. J. da Silva Luz, G. J. P. Moreira, L. S. Oliveira, W. R. Schwartz, and D. Menotti, Learning deep off-the-person biometrics representa- May 2018
[3] C. Shaojie, Z. Meng, and Q. Zhao, Electrocardiogram recognization based on variational AutoEncoder, in Machine Learning and Biometrics. IntechOpen, Aug. 2018.
[4] A. N. Uwaechia, N. M. Mahyuddin, M. F. Ain, N. M. A. Latiff, and N. F. Zabah, Multi-user mmWave MIMO channel estimation with hybrid beamforming over frequency selective fading channels, in Proc.
[5] A. Alharbi and T. Alharbi, Design and evaluation of an authentication Apr. 2020.
[6] G. Lundahl, L. Gransberg, G. Bergqvist, G. Bergstrm, and L. Bergfeldt, Sep. 2020, Art. no. e0239074.
[7] J. P. Berman, M. P. Abrams, A. Kushnir, G. A. Rubin, F. Ehlert, A. Biviano, J. P. Morrow, J. Dizon, E. Y. Wan, H.
[8] Fully Convolutional Network Variations And Method On Small Dataset
[9] D. Jang, S. Wendelken, and J. M. Irvine, Robust human identication Art. no. 76670M.
[10] Tianyou Hu; Yancong Deng; Yuwei Deng; Anmin Ge Convolutional neural networks: an overview and application in radiology
[11] W. Zareba, and A. J. Moss, Correlation method for detec- tion of transient T-wave alternans in digital Holter ECG recordings, Ann.
[12] S. Tabakov, I. Iliev, and V. Krasteva, Online digital lter and QRS detector applicable in low resource ECG monitoring systems, Ann.
[13] R. Salakhutdinov and G. Hinton, Deep Boltzmann machines, in Proc
[14] L. Premk; Ž. Emeršič; T. Oblak- Automatic Latent Fingerprint Segmentation Using Convolutional Neural Networks



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY