Emerging Trends in Digital Transformation

ISSN: 3107-4308 | Conference Issue 2025

International Conference on Emerging Trends in Engineering, Technology & Management (ICETM – 2025)

ETDT

ETDT
Emerging Trends in Digital Transformation
Special Issue - 2025 ISSN: 3107-4308 *Paper ID:* ***ETDT-SI-13***

International Conference on Emerging Trends in Engineering, Technology & Management (ICETM-2025)
Conducted by *Viswam Engineering College (UGC—Autonomous Institution)* held on 11th & 12th, April- 2025

EFFECTIVE TECHNIQUE FOR FINGERPRINT LIVENESS DETECTION USING PROBABILISTIC NEURAL NETWORKS

G.Praburam, Viswam Engineering College

ABSTRACT- Fingerprint Detection and recognition is the most Challenging and widely used Biometric technologies. Today's modern world, apparently it is used in many real applications. The real images of human identification characteristics are spoofed by Putty, Play-doh, Fingerprint mold, etc. Here we obtain a Probabilistic Neural Networks (PNN) used to oversee training set to develop probability density functions intense a pattern layer to fingerprint liveliness detection. This is a model based the core concept and based on multivariate probability estimation. Yield state-of-the-art results for architecture or hyper parameter selection is not needed for pre-trained PNNs., Not only for extreme architectures but also for requiring ones used by Dataset Augmentation is to improve the performance. More advantaged accuracy on very small training sets using these large pre-exercise networks. Our best model achieves an overall rate of 95.1% of correctly exercised classified samples.

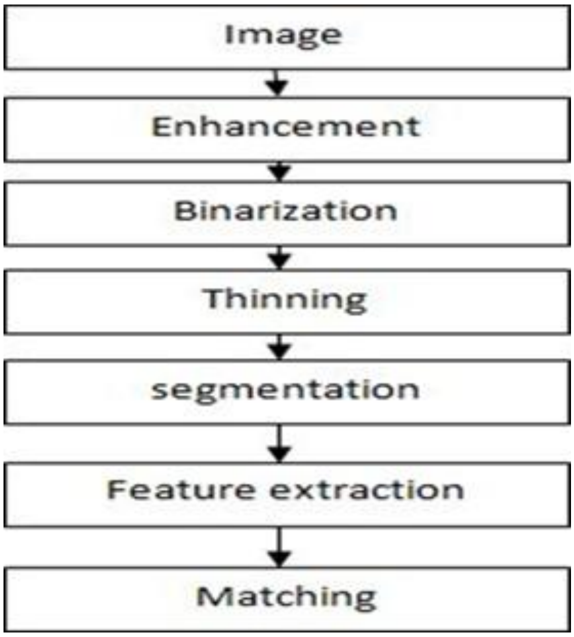
I. INTRODUCTION

Image Processing is the science of manipulating an Image. With the advent of digital cameras and their easy interoperability with computers, the process of Digital Image Processing has acquired an entire new dimension and meaning. Image Processing works with the digital images to enhance, distort, accentuate or highlight inherent details in the image.

DIGITAL IMAGE PROCESSING

With the help of scanning devices, our computer systems acquire the image, store the image in memory in digital form, process the image in various ways. This mechanism is called Digital Image Processing.

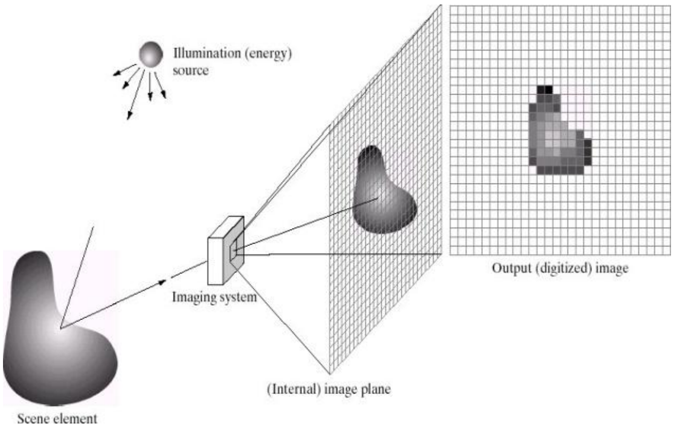
BLOCK DIAGRAM



DOI : https://doi.org/10.5281/zenodo.17277742

DIGITAL IMAGE PROCESSING

A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels.



Pixel values typically represent gray levels, colours, heights; opacities etc. Remember *digitization* implies that a digital image is an *approximation* of areal scene.

1.2 IMAGE ENHANCEMENT

The moisture and scars of a finger as well as the pressure due to a fingerprint sensing could distort the quality of the acquired fingerprint image.

- We adopt an ad hoc strategy to enhance the quality of a fingerprint image.
- Support that A(i ,j)is image gray level at pixel (i, j), μ and s2 are the mean and variance of graylevels of input image, and α=150, γ=95, γ must satisfy γ>s.

The enhanced image B(i ,j)is given as follows.

- $$B(i, j) \leftarrow \alpha + \gamma \ * \ ([A(i, j) - \mu] \ / s)$$

IMAGE BINARIZATION

We have to distinguish valley and ridge of a fingerprint image before smoothing and thinning. So, the gray value of pixels in the enhanced fingerprint image will be binarized to 0 or 255.

- First, we compute the gray value of P25andP50from the enhanced image, where Pk is the kth percentile of enhanced fingerprint image histogram.
- Then we partition an enhanced fingerprint image into w by w blocks and compute the mean of each blocks. We define that M_j is the mean of the j-th block.
- If the gray value of pixel S_i is less than P_{25}, we assign 0 to S_i. If the gray value of pixel S_i greater thanP50, we assign 255 to Si. Other wise,the pixel value is defined by the following rule:

$$S_i = \begin{cases} 255 \text{ if } \dfrac{1}{8}\sum_{\substack{x=0 \\ x \neq i}}^{8} S_x \geq M_j \\ 0 \quad \text{otherwise} \end{cases}$$

SMOOTHING

- After binarization, we find that there is still much noise on ridge region. In order to make the result of thinning better, we have to smooth the fingerprint image first. A smooth stage uses neighboring pixels to remove noise.
- First a 5 by 5 filter is used. The pixel p_i is assigned by:

$$p_i = \{255 \text{ if } \Sigma_{5x5} N_w \geqq 18$$
$$0 \quad \text{if} \quad \Sigma_{5x5} N_b \geqq 18$$

p_i other wise

DOI : *https://doi.org/10.5281/zenodo.17277742*

Then a 3 by 3 filter is further proceed by:

$$p_i = \{255 \text{ if } \Sigma_{3x3} N_w \geqq 5$$
$$0 \quad \text{if } \Sigma_{3x3} N_b \geqq 5$$

pi other wise

THINNING

- The purpose of thinning stage is to gain the skeleton structure of fingerprint image.
- It reduces a binary image consisting of ridges and valleys into a ridge map of unit width.

SEGMENTATION

Thresholding is the simplest segmentation method.

The pixels are partitioned depending on their intensity value. Global thresholding, using an appropriate threshold

$$g(x, y) = \begin{cases} 1, & \text{if } f(x, y) > T \\ 0, & \text{if } f(x, y) \leq T \end{cases}$$

1.3 BIOMETRIC FINGER PRINT SYSTEM

Fake biometrics means by using the real images of human identification characteristics create the fake identities like fingerprint, on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication but biometric system has more method to detect the fake users and that's why the biometric system is more secure, because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different types that are face recognition system, fingerprint recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioral biometric).

HAMMING DISTANCE CALCULATION APPROACH

Many machine learning algorithms presuppose the existence of a pair wise similarity measure on the input space. Examples include semi-supervised clustering, nearest neighbor classification, and kernel-based methods, when similarity measures are not given a priori, one could adopt a generic function such as Euclidean distance, but this often produces unsatisfactory results. The goal of metric learning techniques is to improve matters by incorporating side information, and optimizing parametric distance functions such as the Mahalanobis distance. Motivated by large-scale multimedia applications, this paper advocates the use of discrete mappings, from input features to binary codes.

The Hamming distance, a natural similarity measure on binary codes, can be computed with just a few machine instructions per comparison. Further, it has been shown that one can perform exact nearest neighbour search in Hamming space significantly faster than linear search, with sub linear run-times. By contrast, retrieval based on Mahalanobis distance requires approximate nearest neighbour (ANN) search, for which state-of-the-art methods do not always perform well, especially with massive, high-dimensional datasets when storage overheads and

DOI : https://doi.org/10.5281/zenodo.17277742

distance computations become prohibitive.

2.FEATURE EXTRACTION:

Circular string extraction

Circular string matching is a problem which naturally arises in many biological contexts. It consists in finding all occurrences of the rotations of a pattern of length m in a text of length n.

A circular string of length n can be viewed as a traditional linear string which has the left- and right- most symbols wrapped around and stuck together in some way. Under this notion, the same circular string can be seen as n different linear strings, which would all be considered equivalent. Given a string x of length n, we denote by x i =x[i..n−1]x[0..i−1], 0<i<n, thei-th rotation of x and x0=x.

A probabilistic neural network is predominantly a classifier. PNN uses a supervised training set to develop probability density functions within a pattern layer. This is a model based on competitive learning with a winner takes all attitude‟ and the core concept based on multivariate probability estimation.

Probabilistic (PNN) and General Regression Neural Networks (GRNN) have similar architectures, except there is a fundamental difference. General regression neural networks perform regression where the target variable is continuous, whereas Probabilistic networks perform classification where the target variable is categorical.

DATABASE UPDATION

In this module the given image is to be compared with the database images, this operation is to be going to processed for an finding a matching pattern in an given query image.

MATCHING

Matching process is used to classify whether the given input image is matched with one of the database images or not.

3. CONCLUSION

The description of an effective approach for finger print recognition, which concentrates on fingerprint lash and finger print noise detection. The proposed algorithm uses a bank of Log-Gabor filters to extract the edge information based on phase congruency. Acquired edge information is then infused with region information to localize the noise regions. This proposed method will achieve encouraging performance for improving the recognition accuracy of a finger print recognition system. In this study we applied different classification studies in fingerprint liveness detection in order to broad the traditional approaches that use the knowledge about the fake/spoof samples for training the models. Therefore, in a first approach we mixed the fake materials in train and test sets instead of training and testing with only one specific material. However, this approach is still not very realistic since we assumed to have knowledge about all the possible spoof attacks. So, the next approach was to test with one material and train with the rest of the materials. As expected, this approach lead to worse results since we are using a complete unknown material in the test step. Finally, the last approach, which we consider the most worth following, consisted on using only the information of the real samples when training our model and then tests it with real and fake samples. In fact, what we are performing is a semi-supervised classification characterizing the real samples and expecting our model to classify correctly as fake the spoof samples in the test set. Two different methods were used, a CNN, being the best results produced by this latter one. Although the results of the semi- supervised approach are worse than the supervised classification, we still consider the firs t to be more realistic. In our opinion, is more adequate to evaluate the robustness of a liveness method to unknown spoof attacks not assuming complete or even partial knowledge about the fake/spoof samples to be used by an intruder. We consider the results obtained in our experiments encouraging to pursue this approach in future works broadening the study to other databases and also other biometric traits. This approach has raised interest recently in the liveness detection field as some referred works show, but, to the best of our knowledge has not been yet fully studied and in our opinion can be further explored. In this work, we also illustrate the variability in the background of fingerprint images among the different datasets used and we argue about the necessity of a segmentation step.

DOI : https://doi.org/10.5281/zenodo.17277742

FUTURE ENHANCEMENT

The goal of this paper is blood vessel detection, diseases like red spot, bleeding, micro aneurysm, hemorrhages, hard exudates, soft educates and intra retina micro aneurysm will still need to be diagnosed as part of future work.

REFERENCES

1. V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "Livdet 2015 fingerprint liveness detection competition 2015."
2. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generation Computer Systems, vol. 28, no. 1, pp. 311–321, 2012.
3. Y. Chen, A. Jain, and S. Dass, "Fingerprint deformation for spoof detection," in Biometric Symposium, 2005, p. 21.
4. B. Tan and S. Schuckers, "Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners," in Defense and Security Symposium. International Society for Optics and Photonics, 2006, pp. 62 020A–62 020A.
5. P. Coli, G. L. Marcialis, and F. Roli, "Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device," International Journal of Image and Graphics, vol. 8, no. 04, pp. 495–512, 2008.
6. P. D. Lapsley, J. A. Lee, D. F. Pare Jr, and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," Apr. 7 1998, uS Patent 5,737,439.
7. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," Information Forensics and Security, IEEE Transactions on, vol. 1, no. 3, pp. 360–373, 2006.
8. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in Advances in Biometrics. Springer, 2005, pp. 265–272.
9. A. K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: High resolution fingerprint matching using level 3 features," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, no. 1, pp. 15–27, 2007.
10. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on weber local image descriptor," in Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on. IEEE, 2013, pp. 46–50.
11. "Local contrast phase descriptor for fingerprint liveness detection," Pattern Recognition, vol. 48, no. 4, pp. 1050–1058, 2015.
12. R. FrassettoNogueira, R. de Alencar Lotufo, and R. Campos Machado, "Evaluating software- based fingerprint liveness detection using convolutional networks and local binary patterns," in Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings, 2014 IEEE Workshop on. IEEE, 2014, pp. 22–29.
13. D. Menotti, G. Chiachia, A. Pinto, W. Robson Schwartz, H. Pedrini, A. Xavier Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," Information Forensics and Security, IEEE Transactions on, vol. 10, no. 4, pp. 864–879, 2015.
14. X. Jia, X. Yang, K. Cao, Y. Zang, N. Zhang, R. Dai, X. Zhu, and J. Tian, "Multi-scale local binary pattern with filters for spoof fingerprint detection," Information Sciences, vol. 268, pp. 91– 102, 2014.
15. L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in Pattern Recognition (ICPR), 2012 21st International Conference on. IEEE, 2012, pp. 537–540.
16. S. B. Nikam and S. Agarwal, "Local binary pattern and wavelet-based spoof fingerprint detection," International Journal of Biometrics, vol. 1, no. 2, pp. 141–159, 2008.
17. L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection using binarized statistical image features," in Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on. IEEE, 2013, pp. 1–6.
18. P. Y. Simard, D. Steinkraus, and J. C. Platt, "Best practices for convolutional neural networks applied to

DOI : *https://doi.org/10.5281/zenodo.17277742*

visual document analysis," in null. IEEE, 2003, p. 958.

19. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Image net classification with deep convolutional neural networks," in Advances in neural information processing systems, 2012, pp. 1097– 1105.
20. O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein et al., "Image net large scale visual recognition challenge," International Journal of Computer Vision, pp. 1–42, 2014.
21. K. Simonyan and A. Zisserman, "Very deep convolutional networks forLarge-scale image recognition," CoRR, vol. abs/1409.1556, 2014.
22. S. Karayev, M. Trentacoste, H. Han, A. Agarwala, T. Darrell, A. Hertzmann, and H. Winnemoeller, "Recognizing image style," arXiv preprint arXiv: 1311.3715, 2013.
23. Y. LeCun et al., "Generalization and network design strategies," Connections in Perspective. North-Holland, Amsterdam, pp. 143–55, 1989.

DOI : *https://doi.org/10.5281/zenodo.17277742*