Image Fusion Based Multimodal Biometric Recognition

Sunitha Nandhini A., Suhashini M. S., Yasvanthini B., Sharmila Devi M.

Abstract: Biometric Authentication is a security process that replays on the unique biological characteristics of an individual. Biometric Authentication system compare a biometric data capture to stored, confirmed authentic data in a database. It is simply the process of verifying the identity using the measurements or other unique characteristics of the body, then logging us in a service, device and so on. It is an effective way to prove identity because it can't be replicated. Multi focus Image fusion is a process of fusing two or more images to obtain a new one. Used to reduce the problems like blocking, ringing artifacts occurs because of DCT. The low frequency sub-band coefficients are fused by selecting coefficient having maximum spatial frequency. The goal is classifying the images to classes of authorized and unauthorized using multi class SVM. The fingerprint image and iris image are fused together using SWT, the features are extracted from the fused image and labelled using GLCM algorithm. The testing image is then compared with trained samples and classified as authorized or unauthorized by using FFNN.

Keywords: About Biometric Authentication, Feed forward Neural Network, Fusion, SWT.

I. INTRODUCTION

With the rapid improvement of the Internet and cell devices, authentication structures have been extensively used to shield consumer devices, content and accounts. When customers have more than one accounts, password management will become more hard to carry out because it is often hard to remember exclusive passwords for a extraordinary program, mainly those with high safety tiers. To resolve this problem, biometrics are used in person validation because of their particular traits. A fashionable person login scheme primarily based on something associated with a password or something related to a password or PIN. Therefore, the number of bodily and functional functions may additionally range in biometric structures together with fingerprint, iris, face, hand geometry, palm print, fingerprint, gait, voice and signaling. Biometric systems can work in two methods i.E. Validation or identity. Biometric validation is the characteristic of validating a biometric pattern of an experiment with its equal structure or model in keeping with the permission given via the consumer. While, biometric documentation is a function of integrating the studies system with a couple of arrangements or models located in a fixed of unknown or subscribed individuals. Multimodal biometric schemes, consisting of structures that are not mounted inside the same way, may be used to cross special biometric parameters. This paper discusses the procedure of integrating human beings that's a rigorous yet crucial assessment of newly developed biometrics to broaden biometric biometric strategies. It may be visible in pre-made biometric statistics the use of exceptional combos of biometric statistics in exclusive classes, together with fit tag, function view or selection view. The system of biometric differentiation and the majority of biometric recognition arrangements may be acquired via examining those fusion points.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.

Ms. Sunitha Nandhini A*., Assistant Professor, Department of CSE, Sri Krishna College of Technology, Coimbatore, Tamilnadu, India.
E-mail: asuni.cc@gmail.com

Suhashini M. S., Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, Tamilnadu, India.
E-mail: 16tucs233@skct.edu.in

Yasvanthini B., Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, Tamilnadu, India.
E-mail: 16tucs257@skct.edu.in

Sharmila Devi M., Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, Tamilnadu, India.
E-mail: 16tucs217@skct.edu.in

II. BIOMETRIC AUTHENTICATION SYSTEMS

This Biometric authentication is a security method that is compatible with the person's biometric functions to enable the man or woman seeking to get entry to the device is permitted to do so. Biometric trends are physiological and genetic markers which are particular to a exceptional man or woman and can be in comparison to the authorised trainee characteristics. If the biometric capabilities of the individual seeking to get right of entry to the device fit the characteristics of the legal user, get right of entry to to the device is allowed. Biometric authentication can be mounted on any bodily location, which controls access points.

FIG 1.Sample Fingerprint

Biometric authentication methods may also contribute as a form of two-factor authentication or multi-factor authentication, either by combining multiple biometric patterns with a traditional password or secondary device that supplements the biometric verification. Biometrics do still face some hurdles to widespread buyer adoption. Certain biometric technologies are very complex to program, install, and use, and may require educating consumers to assure they are used correctly.

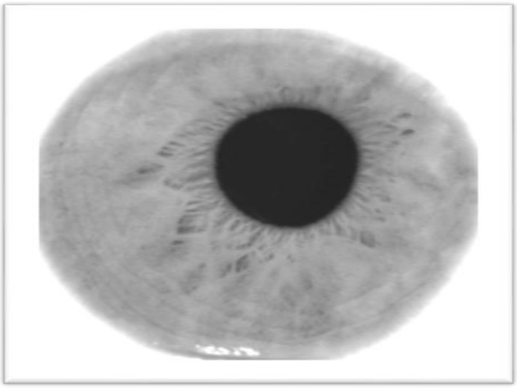

FIG 2. Sample Iris

III. RELATED WORKS

Sheetal Chaudhary, Rajender Nathetal. [10] developed a multimodal biometric device for the participation of the iris, dictionary and fingers based totally at the college-level process using more than one vector guide features. Here, SVM makes experience in a relational way to cope with the complexity of missing biometric actors. It reproduces all feasible mixtures of all biometric functions separately. They have worked with assist gadget as their approach and have checked the adoption rate through 99 percent. Divyakant T. Meva, C. K. Kumbha Rana et al. [11] offer a broadly used biometric device from centuries ago. Depending at the want for IT, this statistics guarantees the satisfaction and requirements of the authorization. But Unimodal Biometric arrangements have their boundaries. To spoil the boundaries of Unimodal Biometric Systems, they labored on a Multimodal Biometric Structures plan. As far as they are involved, the authors have analyzed the facts within the Multimodal Biometric scheme designed and evolved to enhance the validity of the validation. Improved fingerprints and face popularity techniques with a mixture of points. They are concerned about figuring out the size of an action using more than one units of weights disbursed on fingerprints and face scores. They have established a achievement rate of 93 percentage and a 6 percent failure charge. Norsalina Hassan, [12] proposed facial makeup and fingerprints with a strong recognition pattern. Installation is completed at the corresponding faculty level. Fixed capabilities for shared modes have been accepted the usage of vector help machines. Hearing on the expression of the face and fingers indicates a top notch deal that the overall performance of a biometric biometric system provides excellent acknowledgment associated with the abnormal biometric situation. They worked out the precis rule and checked for a possible blunders of 0.83. Yogesh. H. Dandawate, Sajeeda. R. Inamdar et al. [13] suggests the seize of diverse natural human precursors, sample and vein using Hardware and the three capabilities previously evolved and attached by means of cryptography collaboration. Palm is distinct as a biometric exceptional as there are no two veins of the equal palm vegetation besides that they are the equal creature and Palm has bodybuilding curtains as a outstanding problem to look in character in comparison to other biometric texts. They have worked at the Gabor part check and the Gabor filter out which have an typical accuracy of 97%. Nassima Kihal [14] proposed a biometric arrangement for validation, using fusion of the iris and palm. Implement every implant strategy and apply packet erosion into four stages. Kamel Aizi Mohamed Muslim Ahmed Sabri et al. [15] determined the patron server structure for a multimodal biometric method. As a human, they used two techniques, the iris and the sounds to enhance safety. No biometrics can not be used for authentication. They labored at the procedure of accounting and calculated false popularity and rejection of values.

IV. PROPOSED WORK

In the proposed method used the extent degree fusion of the iris and fingerprints the use of the extraction feature, as well as the fingerprint scanning. The graphical interface was created for the proposed device. First it labored at the cases of the iris used within the Hough circle transformation after which extracted the vector of the independent components of the function vector. Subsequently experiments were achieved the use of fingerprints in which binarization and photograph discount were accomplished the usage of unique morphological capabilities.

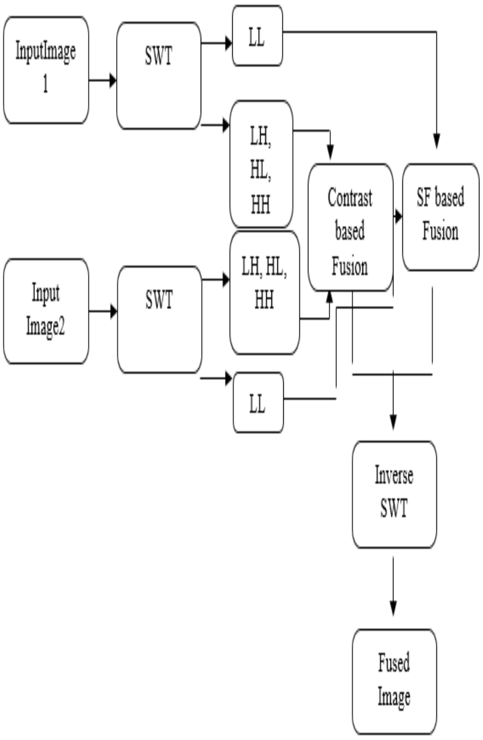

Fig 3 Fusing Image

Step1- The fingerprint image is given as input to SWT algorithm.

Step2- SWT splits the input image into four parts as high and loss pass filters.

Step3- Step1 and Step2 is repeated for iris image.

Step4- The low pass filters of fingerprint image and iris image are fused together. The high pass filters of fingerprint image and iris image are fused together.

Step4- Inverse SWT is applied to obtain a complete fused image by combining low pass and high pass filters.

Step5- GLCM algorithm extracts the features like Energy, Entropy, Contrast, Correlation from the fused image and labels the image.

Step6- The inputs are given to FFNN algorithm and it fetches the feature values for that image.

Step7- If the values matches with trained images, then the document will open.

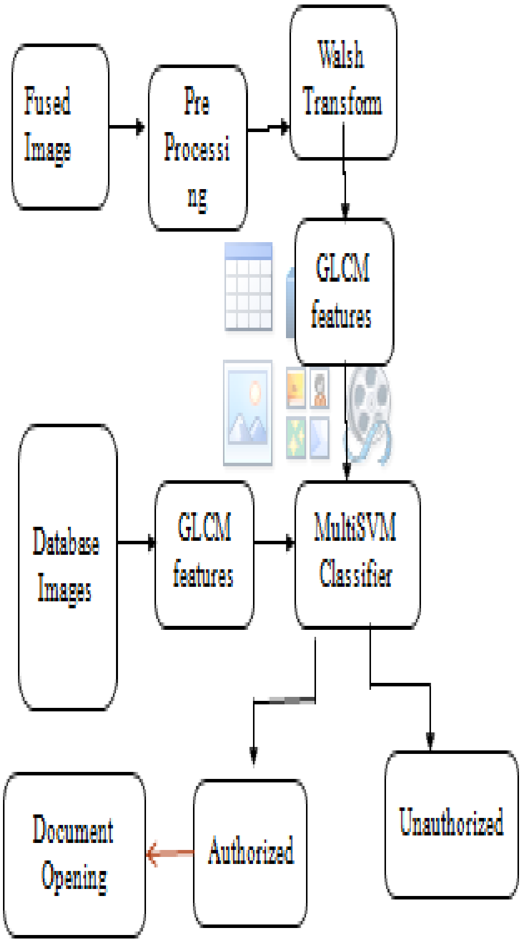

Fig 4 Verification Authority

V. STATIONARY WAVELET TRANSFORM

Stationary wavelet change is a supplement to the usual discrete wavelet trade. SWT uses excessive and low skip filters. SWT uses the high and low skip filters for each data and inside the next section produces orders. Each new sequence has the identical duration as the unique sequence. In SWT, rather than scrolling it convert the filters to each level by way of combining them with xeros. SWT is more complicated.

VI. FEED FORWARD NEURAL NETWORK

A feed forward neural network is an artificial neural network where links do not form a cycle. As such, it is quite different from recurrent neural network. The feed forward neural network extracts the feature[16] from the input image. The information moves in one direction, from the input nodes to the output nodes. There are no cycles or loops in the system as researched.

VII. RESULT AND DISCUSSION

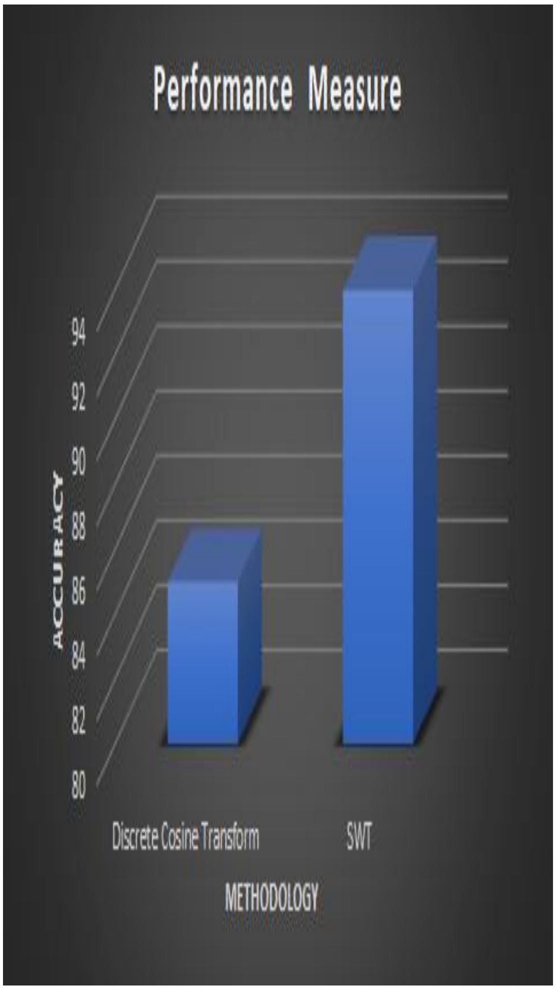

Fig 5 Performance Measure

Performance:

Methodology	Accuracy
Cascade Classifier	85
Convolution Neural Networks	94

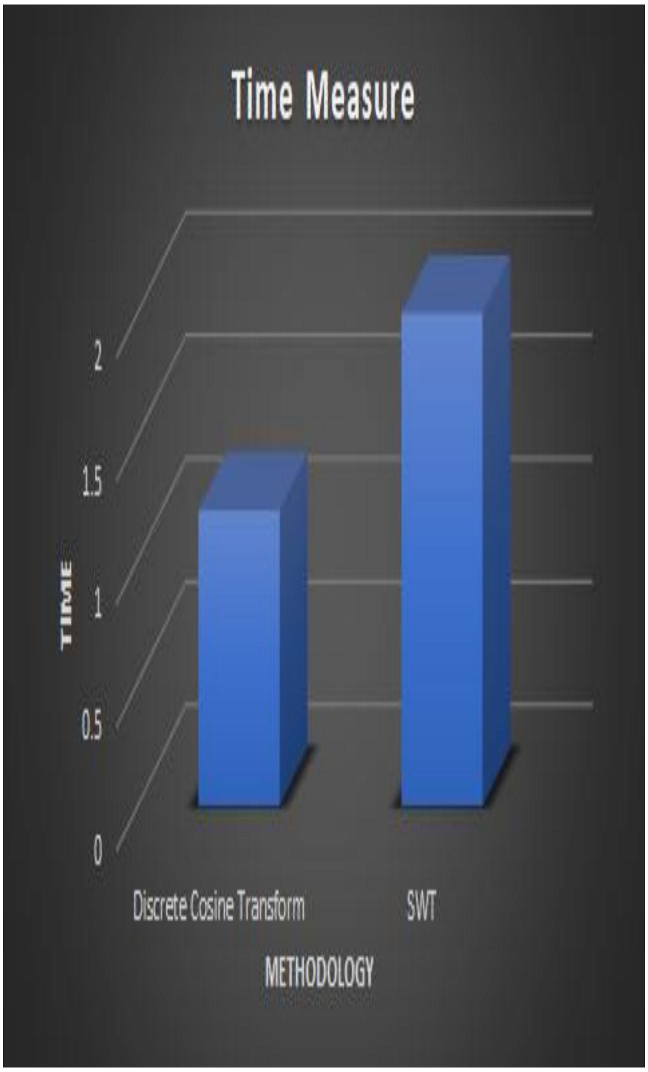

Fig 6 Time Measure

Time measure:

Methodology	Time in seconds
Cascade Classifier	1.2
Convolution Neural Network	2

VIII. CONCLUSION

Image fusion based multimodel biometric recognition- has demonstrated high accuracy and high security under a large number of different conditions. SWT overcome the data loss, outliers in a better manner. The approach of fusing image reduced the blocking, ringing artifacts. From the proposed implementation, it shows that the performance of multi biometric scheme, fusion process and classification is taken place with low error, better quality and reduction of false negative rates. The purpose is classifying the tissues to two training of legal and unauthorized using FFNN.

REFERENCES

1. A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction To Biometric Recognition", in IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, 2004, pp. 4–20.
2. Haryati Jaafar, Dzati Athiar Ramli, "A Review of Multibiometric System with Fusion Strategies and Weighting Factor", International Journal of Computer Science Engineering (IJCSE), Vol. 2 No.04 July 2013, pp.158-165.
3. J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez, "Authentication Gets Personal With Biometrics", in IEEE Signal Processing Magazine, Vol. 21, 2004, pp. 50–62.
4. M.X. He, S.J. Horng, P.Z. Fan, R.S. Run, R.J. Chen, J.L. Lai, M.K. Khan and K.O. Sentosa, "Performance Evaluation of Score Level Fusion in Multimodal Biometric Systems", Journal of Pattern Recognition, Vol. 43, No. 5, 2010, pp. 1789-1800.
5. J.P. Campbell, D.A. Reynolds, and R.B. Dunn, "Fusing High And Low-Level Features for Speaker Recognition", in Proceeding of EUROSPEECH, 2003, pp. 2665-2668.
6. A. Jaina, K. Nandakumar, A. Ross, and A. Jain, "Score Normalization in Multimodal Biometric Systems", Journal of Pattern Recognition, Vol. 38, 2005, pp. 2270.
7. Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview", Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.
8. K. I. Chang, K. W. Bowyer, and P. J. Flynn, "Face recognition using 2D and 3D facial data," in Proc. Of Workshop on Multimodal User Authentication, (Santa Barbara, CA), pp. 25–32, Dec 2003.
9. Roy, K., and Bhattacharya, P. (2006), Iris recognition with support vector machines, Springer Lecture Notes in Computer Science ICB 2006, Zhang, D., and Jain, A. K. (Eds.), vol. 3832, pp. 486-492.
10. Chaudhary, Sheetal, and Rajender Nath. "A Robust Multimodal Biometric System Integrating Iris, Face and Fingerprint using Multiple SVMs." *International Journal of Advanced Research in Computer Science* 7, no. 2 (2016).
11. Meva, Divyakant T., and C. K. Kumbha Rana. "Design and evaluation of multimodal biometric system with fingerprint and face recognition." International Journal of Scientific and Research Publications 5, no. 4 (2015): 1-4.
12. Hassan, Norsalina, Dzati Athiar Ramli, and Shahrel Azmin Suandi. "Fusion of Face and Fingerprint for Robust Personal Verification System." International Journal of Machine Learning and Computing 4, no. 4 (2014): 371
13. Dandawate, Yogesh H., and Sajeeda R. Inamdar. "Fusion-based multimodal biometric cryptosystem." In Industrial Instrumentation and Control (ICIC), 2015 International Conference on, pp. 1484-1489. IEEE, 2015.
14. Kihal, Nassima, Salim Chitroub, and Jean Meunier. "Fusion of iris and palmprint for multimodal biometric authentication." In Image Processing Theory, Tools and Applications (IPTA), 2014 4th International Conference on, pp. 1-6. IEEE, 2014.
15. Aizi, Kamel, Mohamed Muslim, and Ahmed Sabri. "Remote multimodal biometric identification based on the fusion of the iris and the fingerprint." In Electrical Engineering (ICEE), 2015 4th International Conference on, pp. 1-6. IEEE, 2015.
16. Sreeja N.K., Sankar A,"Pattern matching based classification using ant colony optimization based feature selection", 2015, applied soft computing journal.

AUTHORS PROFILE

A. Sunitha Nandhini, Assistant Professor in the Department of Computer Science and Engineering, Sri Krishna College of Technology. She is currently pursuing her PhD under Anna University,Chennai.She received her B.E in Computer Science and Engineering and M.E in Computer and Communication from Anna University, India in 2006 and 2008 respectively. She is a member of ISTE and her research focuses on Adhoc network,Network Security.She has published papers in International Journal.

Suhashini M. S., currently pursuing bachelors degree program in computer science and engineering at Sri Krishna College of Technology, Coimbatore, Tamilnadu, India E-mail: 16tucs233@skct.edu.in

Yasvanthini B., currently pursuing bachelors degree program in computer science and engineering at Sri Krishna College of Technology, Coimbatore, Tamilnadu, India E-mail: 16tucs257@skct.edu.in

Sharmila Devi M., currently pursuing bachelors degree program in computer science and engineering at Sri Krishna College of Technology, Coimbatore, Tamilnadu, India E-mail: 16tucs217@skct.edu.in