Prediction and Validation of Biometric Authentication Security System Using Various Algorithm Tools

G.B.Veeresh[1], Dr.B. Satyanarayana[2]
{veereshksrm@gmail.com[1], bachalasatya@yahoo.com[2]}

Asst.Professor, CSE. Dept ,KSRM College of Engg , Kadapa, AndhraPradesh, India. 516003.[1],
Professor ,CST Dept, SK university, Anantapur, Andhra Pradesh State , India, 515003 [2]

Abstract. Ensuring touchy data is vital in this computerized world because of the simple accessibility of vindictive clients. These days, advanced wholesale fraud is on the ascent in the computerized local area. What's more, recognizing and alleviating this sort of work is a test. Biometric verification qualifications assume a significant part in securing most of online business. Confirmation of conventional strategies, for example, IDs and passwords isn't adequate to battle wholesale fraud or security sharing. The responsibility for introductions of the understanding might be effortlessly neglected, speculated, lost, shared or taken. To defeat security penetrates, we should guarantee free exchanges that give security and ease of use in any electronic business. In this paper, a legitimate biometrics ID is introduced. This incorporates highlights, for example, palm printing, finger impression and iris to give a more exact distinguishing proof of the individual. The proposed framework is most appropriate for individual distinguishing proof and requires high security during internet shopping, banking network and so on Each biometric component is tried and the equivalent is under 80%, the client will confirm each secret key in turn. Something else, exchanges can be dropped consequently and security infringement will be diverted to the worker. The proposed biometric framework is exceptionally dependable and secure with the goal that unapproved client access is confined. Particulars map is presented for finger extraction, iris and palm print and different encryption calculation. The framework is executed and tried with various boundaries like precision, productivity, protection, security, unwavering quality and gives the most encouraging outcomes in experiments.

Keywords: Biometric, Accuracy, Performance, Usability, Algorithm.

1 Introduction

Information security is worried about the confirmation of privacy, respectability and admittance to data definitely. There are numerous apparatuses and techniques that can uphold data security the executives. In any case, the biometric-based framework has developed to help different parts of data security. Biometric validation upholds the part of ID, verification and credibility in data security. Biometric approval has filled in notoriety as an approach to give human ID. Individual distinguishing proof is vital in numerous applications and the expansion in Visa extortion and information burglary as of late shows that this involves extraordinary worry to the more extensive local area. Singular passwords, pin ID or token settings all have deficiencies that upset their activity in a more extensive organization [1-5]. Biometric is utilized to distinguish the personality of an information test when contrasted with

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308868

a format, which is utilized in cases to recognize explicit people by explicit attributes. Proprietor based: utilizing a solitary "token, for example, a security tag or card and data support: utilization of a code or secret phrase. Traditional confirmation frameworks frequently utilize various example contributions for adequate approval, for example, explicit example highlights. This expects to fortify security as various examples are required, for example, wellbeing labels and codes and test sizes. Thusly, the benefit tried to demonstrate biometric validness is that they can build up a consistent coordinated association between an individual and a piece of information [14 - 16].

2 Related work

The E-installment framework is a mechanized interaction of trading monetary incentive for business bunches in deals and broadens this level past ICT (Information Communication Technology) networks [7]. Power installments are coordinated into four stages. They are Electronic Check, Online Electronic Cash, Smart Card installment and Online Card Payment [13]. Suitable power installments are utilized for a particular gathering of power exchanges. A dependable e-installment framework can give respectability, guarantee security, effectiveness, consistence, versatility, convenience, acknowledgment and negligible monetary danger. These are viewed as components of a biometric framework [8]. The Biometric framework is safer in check and ID and is a significant worry for wellbeing improvements in our current circumstance [5]. The Biometrics framework is protected and dependable and utilizes fingerprints, iris and palm print for the actual varieties of human existence. The social attributes of the monster, the voice are additionally affirmed [11]. In 2009, Stanley depicted biometrics as the least difficult and most secure verification instrument. It won't be fake, taken, fake or acquired. The element number in the biometric goes about as a dependable check instrument. These incorporate variety, general acknowledgment, acknowledgment, consistence, shirking and execution. Verification is fundamental to secure the whole framework. Incorporates confirming framework client ID. Validation can be confirmed in three different ways utilizing a pin and secret key, one client has a shrewd card and security token or another client has social or actual highlights like the iris, palm and finger [12 - 14]. In [14], a safe biometric framework was presented. The biometric application has two unmistakable classes [9]. Confirmation and enlistment. In the enrollment area the client ID subtleties are gone into the program data set. In the confirmation segment the biometric client data is contrasted and the records of the data set.

3 Research Methodology

Biometric framework gives a superior method of client confirmation. Biometric confirmation is a programmed strategy wherein the character of an individual is checked by various conduct or actual elements. Parameters considered for study are Accuracy Efficiency Privacy Security Reliability

i)Accuracy (1) *False Acceptance Rate. (2) False Rejection Rate (3) Equal Error Rate (4) Authentication Accuracy*

ii)Efficiency

iii)Privacy

iv)Security
v)Reliability

Potential Risks in Biometric Authentication

Fake sensor
Resubmitting biometric signal
Common network signal

Algorithm used

SVM Algorithm
Minutiae Algorithm
DWT Algorithm
RC4 Algorithm

The Weka 3.8.9 has implemented to get the optimal solution of the above dataset. The below approaches have implemented and got optimal solution

4 Results And Discussion

Study conducted in Mat Lab tool along with weka software tool. Various algorithmshows its significance in security authentication. RC4 algorithm based tools shows improved performance for all criteria. The values showed herewith table no 1 &2 and also in figure 1 and 2.

Table 1.Evaluation of Total score of criteria level for different algorithm

Criteria	SVM Algorithm	Minutiae Algorithm	DWT Algorithm	RC4 Algorithm
Accuracy	85	67	70	86
Efficiency	80	70	77	85
Usability	87	80	65	87
Privacy	90	85	70	91
Security	92	80	79	90
Reliability	78	70	80	85

Figure 1.Total score of criteria level for different algorithm

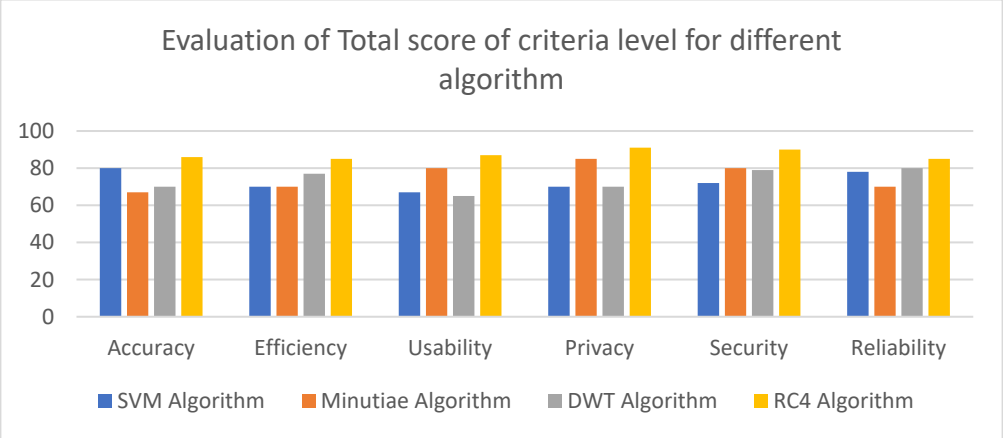
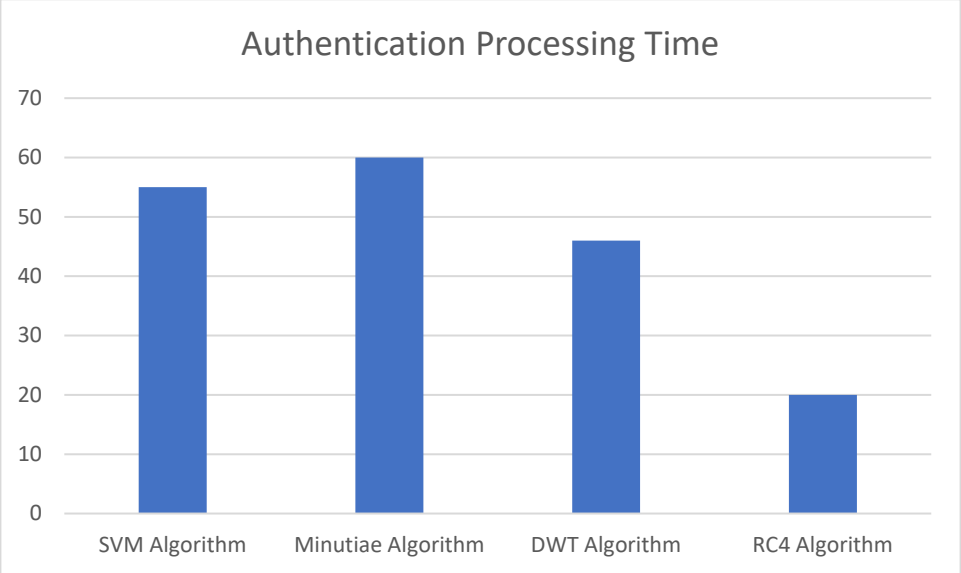


Table 2. Authentication processing time

S.No	Algorithm	Time (ms)
1	SVM Algorithm	55
2	Minutiae Algorithm	60
3	DWT Algorithm	46
4	RC4 Algorithm	20

Figure 2. Authentication processing time



Advances in the field of Information Technology additionally make Information Security an indistinguishable piece of it. To manage security, Authentication assumes a significant part. This paper presents a survey on the biometric confirmation methods and some future prospects in this field [10-13]. In biometrics, a person should be distinguished dependent on some trademark physiological boundaries. A wide assortment of frameworks require solid individual acknowledgment plans to either affirm or decide the character of an individual mentioning their administrations. The motivation behind such plans is to guarantee that the delivered administrations are gotten to simply by a real client, and not any other individual. By utilizing biometrics it is feasible to affirm or build up a person's character [6-9].

Conclusion

Late advances in the field of biometric confirmation. We brought up possible assaults and security hazards in biometric validation and further proposed a progression of assessment

models for assessing the presentation of existing works. We gave a relative assessment on the new writing by partitioning existing biometric verification frameworks into two classifications by utilizing either static biometric highlights or dynamic ones. We tracked down that the greater part of the current frameworks experience the ill effects of safety and protection issues, albeit the confirmation precision of certain frameworks dependent on unique biometric highlights ought to be additionally improved. In light of our overview, we tracked down a few open issues and conjecture future examination headings. We accept that improving the security and protection of biometric confirmation ought to be accentuated in future exploration

References

[1] R. Spolaor, Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, "Biometric authentication methods on smartphones: A survey," PsychNology Journal, vol. 14, no. 2-3, pp. 87–98, 2016.

[2] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," Proceedings of the IEEE, vol. 85, no. 9, pp. 1365–1388, 1997.

[3] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 54–65, 2015.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007.

[5] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable Fingerprint Templates with Delaunay Triangle-Based Local Structures," in Cyberspace Safety and Security, vol. 8300 of Lecture Notes in Computer Science, pp. 81–91, Springer International Publishing, Cham, 2013.

[6] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, "Matching with Secure Fingerprint Templates Using Non-invertible Transform," in Proceedings of the 2008 Congress on Image and Signal Processing, pp. 29–33, Sanya, China, May 2008.

[7] Ayo C.K and. Ukpere, W. I. (2010), "Design of a secure unified e-payment system in Nigeria: A Case Study". African Journal of Business Management,Available online at http://www.academicjournals.org/AJBM, 4(9), pp. 1753-1760

[8] Biometrika, (2011), "Introduction to Biometric Systems", s.l.: Biometrika (Italy) Available at:http://www.biometrika.it/ eng/wp_biointro.html.

[9] Deravi, F. (1999) "Audio-Visual Person Recognition for Security and Access Control" Joint Information Systems Committee, University of Kent at Canterbury.

[10] Drygajio, A, (2011), "Information and Communication Security", LIDIAP Speech processing and Biometrics Group, Institute of Electrical Engineering, EcolePolytechniqueFederalede Lausanne (EPFL).http//scgwww.epfl.ch/courses.

[11] French, T, (2012), "CIS050-6 Week 6: Biometrics". , Luton Campus, UK: University of Bedfordshire. Available at: http://breo.beds.ac.uk.

[12] Kay,R.(2005),"Biometric authentication", s.l.: Computerworld, Available at:http://www. computerworld.com/s/article/100772/Biometric_Authentication.

[13] Mukherjee, A. &Nath P, (2003), "A model of trust in online relationship banking". International Journal of Bank Marketing, 21(1), pp. 5-15.

[14] Ratha, N. K., Connell, J.H, and Bolle, R.M, (2010), "Enhancing Security and Privacy in Biometric Based Authentication System". IBM Systems Journal, 40(3), pp. 615-634.

[15] Stanley, P., Jeberson, W., and Klinsega V.V., (2009), "Biometric Authentication: A Trustworthy Technology for Improved Authentication", International Conference on Future Networks, , pp. 171-175.

[16] Ronald G. Wolak, (1998),"Network Security: Biometrics –The Password Alternative," School of Computer and Information Sciences.

[17] T. Vijayan , M. Sangeetha , A. Kumaravel & B. Karthik (2020): FeatureSelection for Simple Color Histogram Filter based on Retinal Fundus Images for DiabeticRetinopathy Recognition, IETE Journal of Research, DOI: 10.1080/03772063.2020.1844082.
[18] D. S. Vijayan, A. Leema Rose, S. Arvindan, J. Revathy, C. Amuthadevi, "Automation systems in smart buildings: a review", Journal of Ambient Intelligence and Humanized Computing https://doi.org/10.1007/s12652-020-02666-9
[19] Vijayan T, Sangeetha M, A. Kumaravel, Karthik B, "Gabor filter and machine learning based diabetic retinopathy analysis and detection", Microprocessors and Microsystems,2020. https://doi.org/10.1016/j.micpro.2020.103353.
[20] Vijayan T, SangeethaM, Karthik B, "Trainable WEKA Segmentation of Retinal Fundus Images for Global Eye Disease Diagnosis Application," International Journal of Emerging Trends in Engineering Research,Vol 8, No.9, pp. 5750-5754, Sep 2020. https://doi.org/10.30534/ijeter/2020/136892020
[21] C. Amuthadevi, D. S. Vijayan, Varatharajan Ramachandran, "Development of air quality monitoring (AQM) models using different machine learning approaches", Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-02724-2
[22] Vijayan T, Sangeetha M, A. Kumaravel, Karthik B, "Fine Tuned VGG19 Convolutional Neural Network Architecture for Diabetic Retinopathy Diagnosis," Indian Journal of Computer Science and Engineering (IJCSE), Vol. 11, No. 5, pp. 615-622 Sep-Oct 2020. DOI: 10.21817/indjcse/2020/v11i5/201105266.
[23] Vijayan T, Sangeetha M, Karthik B, "Efficient Analysis of Diabetic Retinopathy on Retinal Fundus Images using Deep Learning Techniques with Inception V3 Architecture," Journal of Green Engineering, Vol 10, Issue 10, pp. 9615-9625. Oct 2020