International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7426
***Article Received**: 07 May 2023 **Revised:** 25 June 2023 **Accepted:** 26 July 2023*

Age-Adaptive Multimodal Biometric Authentication System with Blockchain-based Re-Enrollment

Geetanjali Sawant[1], Vinayak Bharadi[2], Kaushal Prasad[3], Pravin Jangid[4]
[1]Research Scholar, Department of Information Technology
Finolex Academy of Management and Technology
Ratnagiri, India
geetanjalinileshsawant@gmail.com
[2]Professor, Department of Information Technology
Finolex Academy of Management and Technology
Ratnagiri, India
Vinayak.bharadi@famt.ac.in
[3]Professor, Department of Mechanical Engg.
Finolex Academy of Management and Technology
Ratnagiri, India
principal@famt.ac.in
[4]Research Scholar, Department of Information Technology
Finolex Academy of Management and Technology
Ratnagiri, India
pravinjangid@gmail.com

Abstract— In the long run, a significant time gap between enrollment and probe image challenges the model's prediction ability when it has been trained on variant biometric traits. Since variant biometric traits change over time, it is sensible to construct a multimodal biometric authentication system that must include at least one invariant trait, such as the iris. The emergence of Deep learning has enabled developers to build classifiers on synthesized age-progressive images, particularly face images, to search for individuals who have been missing for many years, to avail a comprehensive portrayal of their appearance. However, in sensitive areas such as the military and banks, where security and confidentiality are of utmost importance, models should be built using real samples, and any variations in biometric traits should trigger an alert for the system and notify the subject about re-enrollment. This paper proposes an algorithm for age adaptation of biometric classifiers using multimodal channels which securely update the biometric traits while logging the transactions on the blockchain. It emphasizes confidence-score-based re-enrolment of individual subjects when the authenticator module becomes less effective with a particular subject's probe image. This reduces the time, cost, and memory involved in periodic re-enrolment of all subjects. The classifier deployed on the blockchain invokes appropriate smart contracts and completes this process securely.

Keywords: Variant/Invariant Biometric trait, Confidence-score, smart contract, blockchain**.**

I. INTRODUCTION

Any human physiological and/or behavioral characteristic is used to construct an authentication system. However, multimodal is always preferred over unimodal classifier as unimodal has the limitations such as universality, uniqueness, permanence, intraclass variation and inter-class similarity [1][2]. Classifier is trained on dataset samples, captured from the user during the enrolment process. This enrolment process is done over a very short period, typically a couple of days up to a couple of months. Hence, in along run of biometric authentication system, the recognition accuracy in terms of false rejection rate starts affecting, if the classifier is built based on a variant biometric trait such as the face, signature, gait, etc. which varies as age progresses [3][4]. Some real-time sample face images compiled over two decades are shown in Figure 1.

Age invariant identification and verification research has been extensively carried out on face biometric traits. As it is used in many applications mainly photo identification demanding services such as access control, claim settlements, criminal investigation, searching a person who has been missing for a long duration, automatic photo tagging, and e-commerce to display wearable products in different colors and combinations [5][6]. Before the emergence of deep learning, age progression and regression methods were primarily applied with a physical model and prototype approaches. The physical modeling approach aims to model the physical characteristics of an age-progressive face, such as the progressive changes in hair, mouth, and skin texture [7][8].

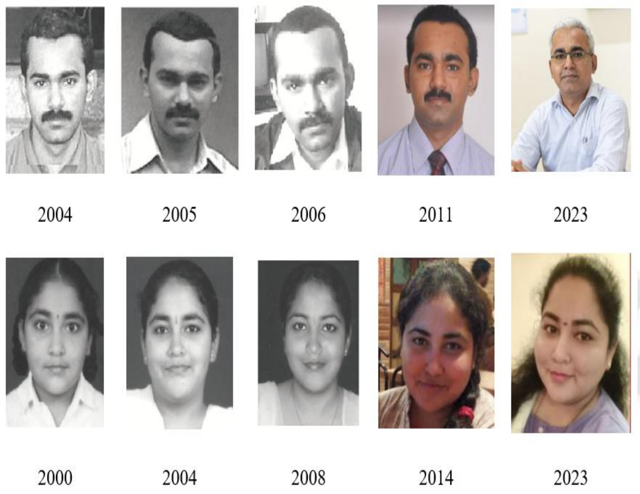


Fig. 1. Age progressive Face samples

The methods belonging to this approach, require a substantial amount of matched data and are pretty time-consuming. The prototype approach performs face aging using a non-parametric model. Initially, it partitions all faces into distinct age groups, and an average face within each age group is computed as a specimen. The difference between the average faces is treated as the aging effect and this effect is transferred to individual face to produce an aged face. However, the prototype approaches discard the personalized information and all the people share the same aging pattern [9][10]. Moreover, regardless of the model type, all these methods perform a one-step transformation from one age group to another by learning a single mapping function. Thus, the one-step mapping function typically fails to capture the dynamics of the in-between face sequence between adjacent age groups [11].

With age progression, intra-class variations become larger than inter-class variations, and the mixed features of age and identity reduce the robustness of the Age variant Face Recognition system to recognize cross-aged faces. Hence, the emphasis was on separating age-dependent features from identity-revealing features and obliterating age-dependent features from performing recognition [12]-[19]. Deep learning techniques enabled developers to use Generative Adversarial Networks (GANs) in image synthesis and translation tasks, but GANs require a huge and balanced dataset to carry out training. There are a number of ways to handle imbalanced classes but it involves additional computational cost. The Conditional generative adversarial networks (cGANs) have achieved impressive results in aging faces. Existing cGANs-based methods basically require a pixel-wise loss to keep the identity and background consistent. However, reducing the pixel-wise loss between the input and its synthesized image results in a ghosted or blurry face image [20]-[24].

Existing face recognition systems face challenges of variation in pose, illumination, expression, and light effect within compiled images as well as in probe images. Many factors such as gender, appearance, aspects, beard, hair, baldness, and attire are needed to be taken into account while synthesizing age-progressive images. In addition to this, consideration of the effects of aging on the facial appearance which differs from person to person in age-invariant face recognition increases the model's complexity. At the same time, we can not ignore the fact that occasionally variations in biometric traits are permanent, mostly these changes are situational or temporary. Subject's mood such as happiness/sadness/laziness/overexcitement, illness, temporary accidental injury, mental stress, or physical stress while capturing a sample or probe image may affect the classifier's classification ability. Hence, it is not only about the face-physiological biometric trait, but the variations that occur in behavioral traits over time are significantly large and to track these variations is time-consuming and heavily results in high computational cost and in increased model complexity. Many existing methods have tried to construct models using Age Invariant Face Recognition database but did not consider the subject-wise confidence level with which the subject is identified. Some methods emphasized the key descriptors of the face which could help in avoiding the possibility of false rejection when the system is used for a longer duration.

A biometric authentication system is basically used for identification and verification. The effects of aging on a trait differ from person to person in its appearance, to learn these patterns and to produce accurate simulations of how a trait ages or rejuvenates, is a complex methodology and moreover, we do not have assurance till that aged time elapses. A model trained on synthesized images is good for identification but the limitations of these techniques express its unsuitability and risk involved in using it for verification. In sensitive applications such as banking, military, etc., it is always advisable to recollect biometric trait samples from subjects when variations start affecting recognition so that it will ensure nonrepudiation, security, and liveliness of the subject.

Our proposed system consists of multimodal biometric authentication performing a classifier built using one invariant biometric trait and it asks for re-enrolment when model reaches to level of false rejection due to variations in features exhibited by biometric trait sample compared to its enrolled samples. To solve the problem of misclassification associated with age progression, we have proposed confidence score-based authentication. As individual ages, their physical features change gradually and cumulatively. For example, face-aging results in fine lines around the eyes and mouth and change in

DOI: https://doi.org/10.17762/ijritcc.v11i9s.7426
***Article Received**: 07 May 2023 **Revised:** 25 June 2023 **Accepted:** 26 July 2023*

skin texture, shape of face. Model does not falsely reject sample at sudden but the matching score decays over time in response of input varied-probe image. Hence, our system sets and utilizes proposed-research-specific thresholds to determine the exact time to notify subject about reregistration. Classifier is deployed on permission blockchain to carry out said process securely by avoiding any kind of intermediate data tampering [25][26] and enabling system to trigger appropriate smart contract depending upon confidence level of subject authentication.

II. METHOD

The proposed system is basically a multimodal biometric classifier built from variant traits such as faces and invariant traits such as iris.

Dataset: UPOL dataset of Iris containing 768 x 576 sized six images of each of 64 subjects. We used our own dataset 101FACES containing 8 samples sized 256 x 256 of below 30 years aged subjects from 101 classes. Practically, The system does not use a classifier trained on age-progressive synthesized images. However, to evaluate the proposed plan, we need three datasets belonging to different age groups of the same classes. For the same, images from the original face dataset are synthesized using all networks at different age groups and stored with respective datasets [27][28]. Fig. 2 shows the sample images from the datasets. We have samples from four age groups of classes (AG I: age (<30), AG II:(>30 age ≤ 45), AG III: (>45 age ≤ 60), AG IV:(age>60)) from an original dataset which is piled into respective age group representing datasets.

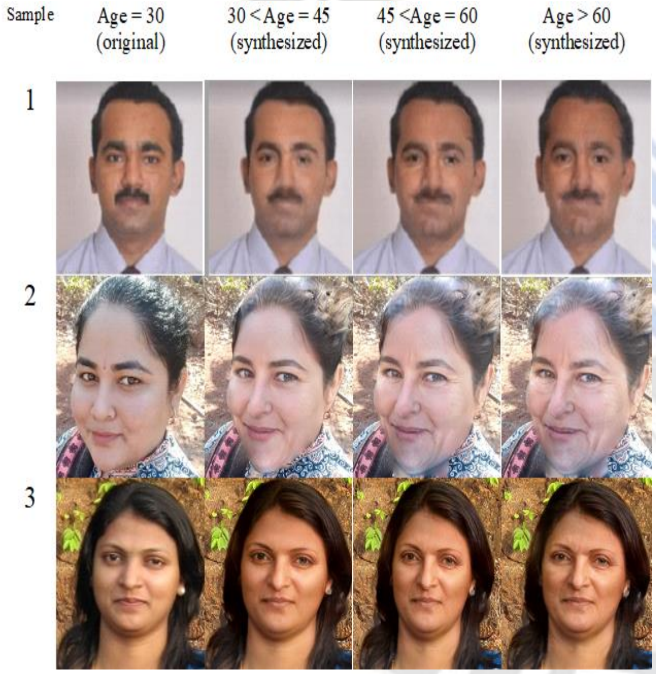


Fig. 2. Age-progressive synthesized images stored with different datasets

Fig. 3 represents the trigger of re-enrolment-notification depending on variant traits' prediction-confidence-score.

The following terms and thresholds describe the working of the proposed system.

a. **Invariant biometric trait**: A multimodal classifier must include a feature vector of at least one biometric trait which will remain constant over time. This feature vector will be used to encourage the variant feature vectors' updation. Invariant biometric traits are Fingerprint, Palmprint, Iris, and Retinal Scan. We used iris for our experimentation.

b. **Variant biometric trait:** A biometric trait whose feature vector does not remain constant over time, is called a variant biometric trait. Invariant feature vectors will be used to encourage the updating of variant feature vectors. Face samples are chosen for analysis of the proposed system.

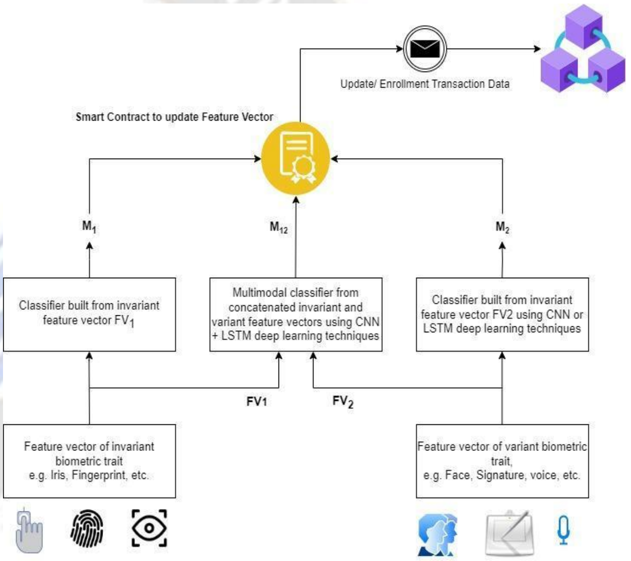

Update/ Enrollment Transaction Data
Smart Contract to update Feature Vector
M1
M12
M2
Classifier built from invariant feature vector FV1
Multimodal classifier from concatenated invariant and variant feature vectors using CNN + LSTM deep learning techniques
Classifier built from invariant feature vector FV2 using CNN or LSTM deep learning techniques
FV1
FV2
Feature vector of invariant biometric trait e.g. Iris, Fingerprint, etc.
Feature vector of variant biometric trait, e.g. Face, Signature, voice, etc.

Fig. 3. Architecture of executing smart contract based on classifier's decisions

c. **Allowed degree of variance in confidence level, *conf***: It is an allowed degree of dissimilarity in the biometric features for which re-enrolment is not required or a measure that represent controlled dissimilarity. In case of biometric traits such as signature, voice; this dissimilarity is calculated in terms of Euclidean distance.
Mid value of accuracy along with confidence interval is used as a threshold for first five tests which have been resulted in a successful authentication.

d. **Multimodal biometric model**: Fusion is carried out at the decision level to construct a biometric authentication-performing classifier. This proposed system consists of three channels, two channels corresponding to selected one invariant and one variant trait and a third corresponding to the combined feature vector of these two.

e. **Event to trigger an update of feature vector:** At any point in time, the event to update the feature vector triggers when either of the following conditions is met**.**

i. **Time_to_update_feature_vector threshold, *triggtm***: When already set datetime elapses, it triggers an event of updating the feature vector. Currently, it is set to 6 months. It may be changed to any logical time by analyzing the system over a longer duration than 6 months. It may alert the system to update feature vectors even though the threshold representing the maximum low confidence score is not reached.

ii. **Number_Low_confidence_score threshold, *triggconf***: How frequently the subject is authenticated with a low confidence score is recorded. When the count exceeds the set threshold of an allowable number of times authentication with a low confidence score occurs, smart contract triggers to update the feature vector even though time is not elapsed.

To set thresholds from the original dataset, certain steps are followed. Fig. 4 shows the procedure followed to notify the subject about alteration in his variant trait.

a. A pair of biometric traits, i.e. iris having high permanence and face having low permanence, are chosen to build unimodal deep learning models M_1 and M_2 from iris and face feature vectors fv_1 and fv_2 respectively. Face images are fed to the convolutional neural networks to fetch features and from Iris images, Kekre's median codebook [29] is generated to feed it to Long-short term memory for the respective classifier's construction.

b. These feature vectors are combined to construct a multimodal classifier M_{12}.

c. Set a threshold time_to_update_feature_vector to the 6 months later datetime from the date, images are enrolled on.

d. Set maximum low_confidence_level score threshold to the average confidence_score resulted from the validation of input to the variant trait-based classifier.

To define the confidence threshold for each subject:

i. Initial confidence is defined in the following specified way: Say we have n number of samples from class C_i. The feature vector of n samples is represented as fv_0, fv_1, fv_2, …. fv_{n-1}}.

ii. Calculate the euclidean distance between fv0, with fv1 to fvn-1, as {dvi1, dvi2,…. dvin-1}

iii. Calculate mean: $\underline{dv_i} = \frac{dv_{i1}+ dv_{i2}+\cdots.+dv_{in-1}}{n}$

Table I. Smart contract invocation depending upon variant biometric classifier's output

M_1O	M_2O	$M_{12}O$	Smart Contract
Reject or authenticate with a low confidence score	Authenticate	Authenticate	Record_SCon: Record datetime and increment count of authentication with low confidence matching score.
Authentic cate	Authenticate	Authenticate	Vote_SCon: To perform specific tasks, authenticated parties want to be involved. e.g Voting

iv. Calculate sample variance for new sample from class: $s_i = \sqrt{\frac{\Sigma\,(dv_{new}-\underline{dv_i})^2}{n-1}}$

Where, dv_{new} is the average feature vector distance of a new sample's feature vector from the other samples' feature vector from ith class.

v. If x1, x2……xn are normally distributed $a = \chi^2_{1-\frac{\alpha}{2,n-1}}$ and $b = \chi^2{}_{\frac{\alpha}{2,n-1}}$, then (1-α)% confidence interval for variance σ^2 is, $\left(\frac{(n-1).s_i^2}{b}\right) \leq \sigma^2 \leq \left(\frac{(n-1).s_i^2}{a}\right)$

vi. Accuracy with a mid value of interval is used as initial allowable maximum low_confidence_threshold to perform classification first five test images which resulted in correct authentication. We used Mean Effective Confidence (MEC) method [30] to derive confidence score associated with classification and these scores are averaged to revise maximum_low_confidence_threshold.

$$\text{MEC}=\frac{1}{n}\sum_{i=1}^{n} C_i * Normalize(CS_i)$$

C_i = 1, i^th^ prediction is correct.

n=5, number of testing samples,

C_i denotes the correctness and

CS_i represents the confidence score of i^{th} prediction which is normalized between 0 and 1

We have used, so $C_i = 1$ *in case of all samples.*

e. For the fed input test sample to the biometric authentication system consisting of three models and record their output as {M1O, M2O, M12O}.

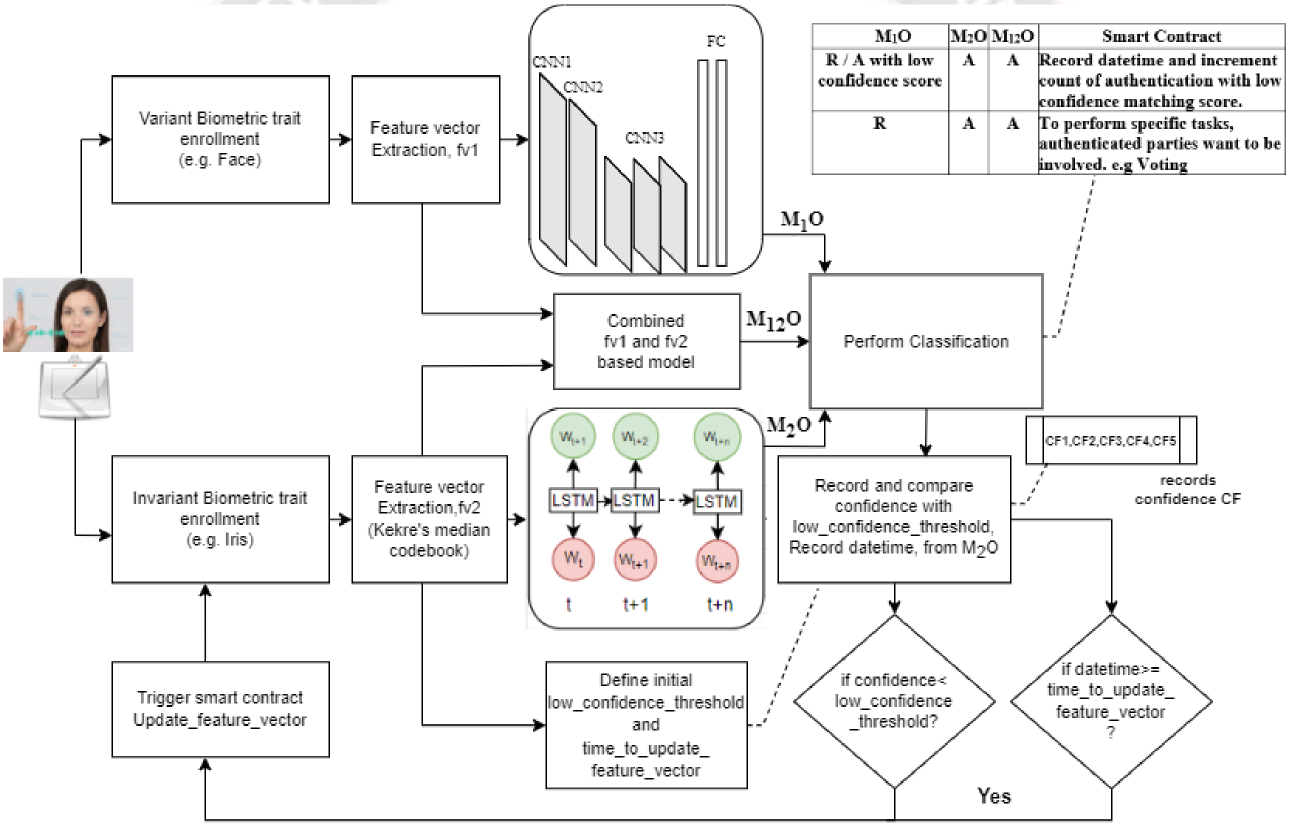
f. This model is integrated with permission blockchain to enable the invocation of smart contracts. Once a subject is authenticated, depending upon the confidence score pushed to the blockchain, either of the following smart contracts is invoked. Channels' output corresponding to smart contract invocation is shown in Table I.

i. **Vote_SCon-** As the subject gets authenticated, it triggers a smart contract running on blockchain, a subject is intended to participate. e.g., to vote for a candidate in an election.

ii. **Record_SCon-** Record false rejection for each subject by incrementing counter *fr* when confidence score is below threshold *conf*. If the subject is successfully authenticated with below confidence threshold *conf*, then it's internally reported as an alteration in trait and increments *triggconf* by one and invokes Vote_Scon too.

iii. **Enroll_SCon-** Compares *fr* with *triggconf*. If fr >= *triggconf*, then it notifies the subject to re-register biometric trait samples.

Fig. 4 shows the execution of the proposed system. To trigger updates of feature vectors, a biometric authentication system is deployed on the Permission blockchain. The web interface is generated to input the probe image and run the classifier on an input image. To decide which smart contract to invoke, outputs M1O, M2O, and M12O were analyzed. The system addresses only the limitation of variant biometric traits, confidence score was calculated for the probe image and found that on successful authentication, Vote_SCon executes, and on authentication with a low confidence score, both Vote_Scon and Record_Scon execute. Once authentication with a low confidence score exceeded the set threshold *conf*, the number of times such authentication is allowed; Enroll_Scon ran and notified subject to re-enroll. Blockchain ensures security, non-repudiation, and availability of updated feature vectors by storing the logs.


Variant Biometric trait enrollment (e.g. Face)
Feature vector Extraction, fv1
CNN1
CNN2
CNN3
FC
M_1O
Combined fv1 and fv2 based model
$M_{12}O$
Perform Classification
M_2O
W_{t+1}
W_{t+2}
W_{t+n}
LSTM
LSTM
LSTM
W_t
W_{t+1}
W_{t+n}
t
t+1
t+n
CF1,CF2,CF3,CF4,CF5
records confidence CF
Invariant Biometric trait enrollment (e.g. Iris)
Feature vector Extraction,fv2 (Kekre's median codebook)
Record and compare confidence with low_confidence_threshold, Record datetime, from M_2O
Trigger smart contract Update_feature_vector
Define initial low_confidence_threshold and time_to_update_ feature_vector
if confidence< low_confidence _threshold?
if datetime>= time_to_update_ feature_vector ?
Yes

M_1O	M_2O	$M_{12}O$	Smart Contract
R / A with low confidence score	A	A	Record datetime and increment count of authentication with low confidence matching score.
R	A	A	To perform specific tasks, authenticated parties want to be involved. e.g Voting

Fig. 4. Proposed Multimodal Biometric Authentication System *A: Authenticate, R: Reject, CF: confidence score

III. RESULTS AND DISCUSSION

Once the thresholds are set by following the steps from the above section, a classifier constructed on the original dataset is applied to validate samples from other datasets. Fig. 5 shows the accuracy of classifier along with confidence interval. Table II represents the accuracy and the confidence interval. One sample from each dataset of variant traits is used to check a confidence score which is ultimately used to classify the sample. A score less than the set threshold triggers a smart contract to record the count of authentication with low_confidence_score. It also triggers a smart contract to notify the system and subject regarding re-enrolment, when such authentication exceeds *triggconf* threshold value.

DOI: https://doi.org/10.17762/ijritcc.v11i9s.7426
***Article Received**: 07 May 2023 **Revised:** 25 June 2023 **Accepted:** 26 July 2023*

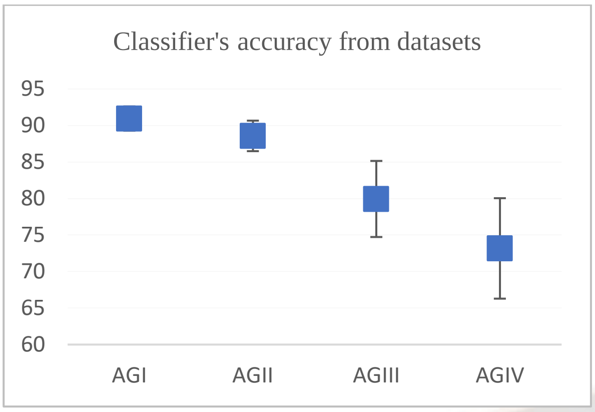


Fig. 5. Confidence interval of the classifier built from the original dataset and validated on remaining datasets.

We can observe that the synthesized image from age above 60 for sample 1 is far different from the real image from 2023 shown in Fig 6. This difference underlines the importance of re-enrollment. For evaluating models after re-enrolment, we added synthesized images from age groups II, III, and IV successively to the original dataset and recorded improved accuracy and confidence score. Table III represents the accuracy and corresponding confidence interval.

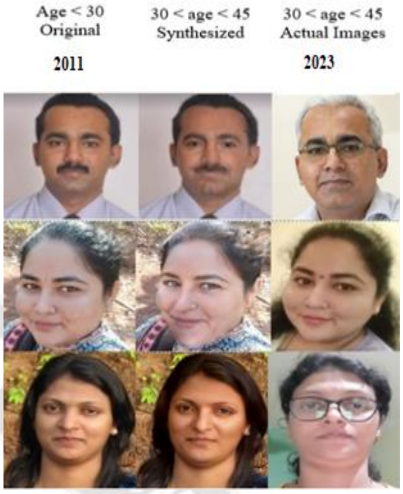


Fig. 6. The sample images from year 2011, synthesized images from AG II, and real images from 2023

Table II. Experimental Results from age progressive datasets

Datasets		Overall False Rejection Rate of variant classifier	Accuracy of integrated classifier	Accuracy of variant classifier	The confidence score of sample1	The confidence score of sample2	The confidence score of sample3
AGI	Age ≤ 30	10.76	93.39	91.95 ± 1.66	0.94	0.94	0.93
AGII	30 < Age ≤ 45	12.40	91.53	88.58 ± 2.09	0.92	0.89	0.93
AGIII	45 < Age ≤ 60	12.89	85.67	79.94 ± 5.21	0.87	0.81	0.88
AGIV	Age > 60	15.07	81.45	72.17 ± 6.88	0.73	0.73	0.74
				As the low_confidence threshold is 92, the confidence score below this causes it to invoke smart contract 2, and on exceeding *triggconf* or *triggtm*, smart contract Enroll_Scon gets executed.			

Table III. Experimental results after adding synthesized images to original datasets in response to re-enrolment notification (in practical use real samples from the subject will be collected and added to the dataset for further training)

Datasets		Overall False Rejection rate of the variant classifier	Accuracy of integrated classifier	Accuracy of variant classifier	The confidence score of sample1	The confidence score of sample2	The Confidence score of sample3
AGI	Age ≤ 30	10.76	93.39	93.05 ± 1.66	0.94	0.94	0.93
AGI +AGII	30 < Age ≤ 45	12.40	92.17	92.03 ± 1.28	0.92	0.92	0.93
AGI+AGII+AGIII	45 < Age ≤ 60	12.89	93.39	93.11 ± 0.99	0.93	0.92	0.94
AGI+AGII+AGIII+AGIV	Age > 60	15.07	94.6	94.16 ± 0.83	0.92	0.92	0.94

IV. CONCLUSION

On three grounds the results are concluded. First, the accuracy of the integrated classifier from Table 2 and Table 3, confirm that the multimodal biometric authentication system built on the face-variant trait and iris-invariant trait proved to be more robust than unimodal system and/or multimodal invariant traits-based system.

Secondly, the confidence score-based re-enrolment controls the memory, time, and computational cost incurred in conventional periodic reregistration of subjects.

The third point is related to the use of classification. Classification is used for identification or verification. To verify individuals using passports, driving licenses, and Aadhar card with face-based authentication, in the clearance of signed cheques with signature-based authentication; it is essential to recollect samples of variant traits as age progresses. The change in lifestyle, surgeries, medical treatment (affecting body structure), and accidental injury may affect the trait's characteristics and hence, the variant trait-based classifier's prediction ability gets affected adversely. Re-enrolment assures the subject's liveliness, guarantees non-repudiation, and avoids impersonation when the subject is notified through the smart contracts deployed on the permission blockchain. We can clearly observe the difference between a synthesized image of sample 1 and the real image from 2023 from age group 45-60, which emphasizes that in certain applications identification depending upon synthesized images-based training may give good results but in sensitive areas, authentication/verification must be done from classifiers which are constructed from real images only.

REFERENCES

[1] Krishna Dharavath, F. A. Talukdar, R. H. Laskar, “Study on Biometric Authentication Systems, Challenges and Future Trends: A Review”, DOI: 10.1109/ICCIC.2013.6724278

[2] R. Parkavi; K.R. Chandeesh Babu; J.Ajeeth Kumar, “Multimodal Biometrics for user authentication”, IEEE 2017. DOI: 10.1109/ISCO.2017.7856044, 2017 11th International Conference on Intelligent Systems and Control (ISCO)

[3] Andreas Lanitis & Nicolas Tsapatsoulis ,“On the Quantification of Aging Effects on Biometric Features”, IFIP International Conference on Artificial Intelligence Applications and Innovations AIAI 2010: Artificial Intelligence Applications and Innovations pp 360–367

[4] Andreas Lanitis, “A survey of the effects of aging on biometric identity verification,” International Journal of Biometrics Volume 2 Issue 101 December 2010 pp 34–52 DOI:10.1504/IJBM.2010.030415

[5] Hachim El Khiyari, Harry Wechsler, “Age Invariant Face Recognition Using Convolutional Neural Networks and Set Distances”, Journal of Information Security, 2017, 8, 174-185, http://www.scirp.org/journal/jis, ISSN Online: 2153-1242

[6] Zhizhong Huang; Junping Zhang; Hongming Shan, " When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark", IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume: 45, Issue: 6, 01 June 2023), Page(s): 7917 – 7932, DOI: 10.1109/TPAMI.2022.3217882

[7] D. Gong, Z. Li, D. Lin, J. Liu, and X. Tang, “Hidden factor analysis for age invariant face recognition,” in Int. Conf. Comput. Vis., 2013, pp. 2872–2879.

[8] Y. Wen, Z. Li, and Y. Qiao, “Latent factor guided convolutional neural networks for age-invariant face recognition,” in IEEE Conf. Comput. Vis. Pattern Recog., 2016, pp. 4893–4901.

[9] T. Zheng, W. Deng, and J. Hu, “Age estimation guided convolutional neural network for age-invariant face recognition,” in IEEE Conf. Comput. Vis. Pattern Recog. Worksh., 2017, pp. 1–9.

[10] Singh Choudhary, S. ., Ghosh, S. K. ., Rajesh, A. ., Alfurhood, B. S. ., Limkar, S. ., & Gill, J. . (2023). BotNet Prediction in Social Media based on Feature Extraction with Classification using Machine Learning Algorithms. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 150 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2553

[11] H. Wang, D. Gong, Z. Li, and W. Liu, “Decorrelated adversarial learning for age-invariant face recognition,” in IEEE Conf. Comput. Vis. Pattern Recog., 2019, pp. 3527–3536.

[12] Wei Wang, Zhen Cui, Yan Yan, Jiashi Feng, Shuicheng Yan, Xiangbo Shu, and Nicu Sebe, “Recurrent Face Aging”, 2016 IEEE DOI: 10.1109/CVPR.2016.261 pp.2378-2386

[13] Megan A. Witherow, Manar D. Samad, Norou Diawara, Haim Y. Bar, and Khan M. Iftekharuddin “Deep Adaptation of Adult-Child Facial Expressions by Fusing Landmark Features”, IEEE 2022 https://doi.org/10.48550/arXiv.2209.08614

[14] Xuege Hou; Yali Li; Shengjin Wang, “Disentangled Representation for Age-Invariant Face Recognition: A Mutual Information Minimization Perspective” , IEEE 2021, DOI: 10.1109/ICCV48922.2021.00367

[15] Chi Nhan Duong, Kha Gia Quach; Khoa Luu; T. Hoang Ngan Le; Marios Savvides, “Temporal Non-volume Preserving Approach to Facial Age-Progression and Age-Invariant Face Recognition”, IEEE 2017 DOI: 10.1109/ICCV.2017.403

[16] Thanh-Dat Truong, Chi Nhan Duong, Kha Gia Quach, Ngan Le, Tien D. Bui, Khoa Luu, “LIAAD: Lightweight Attentive Angular Distillation for Large-scale Age-Invariant Face Recognition”, https://doi.org/10.1016/j.neucom.2023.03.059

[17] Yandong Wen; Zhifeng Li; Yu Qiao , “Latent Factor Guided Convolutional Neural Networks for Age-Invariant Face Recognition”, IEEE 2016, DOI: 10.1109/CVPR.2016.529

[18] Yitong Wang, Dihong Gong, Zheng Zhou, Xing Ji, Hao Wang, Zhifeng Li, Wei Liu & Tong Zhang, “Orthogonal Deep Features Decomposition for Age-Invariant Face Recognition”, ECCV 2018: Computer Vision – ECCV 2018 pp 764–779

[19] Jian Zhao, Yu Cheng, Yi Cheng, Yang Yang, Haochong Lan, Fang Zhao, Lin Xiong, Yan Xu, Jianshu Li et. al. “Look Across Elapse: Disentangled Representation Learning and Photorealistic

Cross-Age Face Synthesis for Age-Invariant Face Recognition", January 2019Article No.: 1135Pages 9251–9258https://doi.org/10.1609/aaai.v33i01.33019251

[20] Dihong Gong, Zhifeng Li, Dacheng Tao, Jianzhuang Liu, Xuelong Li, "A maximum entropy feature descriptor for age invariant face recognition", DOI: 10.1109/CVPR.2015.7299166

[21] Simone Bianco, "Large Age-Gap face verification by feature injection in deep networks", Pattern Recognition LettersVolume 90Issue C15 April 2017pp 36–42https://doi.org/10.1016/j.patrec.2017.03.006

[22] Sveinn Palsson, Eirikur Agustsson, Radu Timofte, Luc Van Gool, "Generative Adversarial Style Transfer Networks for Face Aging", IEEE 2018 DOI: 10.1109/CVPRW.2018.00282

[23] Chia-Ching Wang; Hsin-Hua Liu; Soo-Chang Pei; Kuan-Hsien Liu; Tsung-Jung Liu, "Face Aging on Realistic Photos by Generative Adversarial Networks", IEEE 2019, DOI: 10.1109/ISCAS.2019.8702303

[24] Ms. Mayuri Ingole. (2015). Modified Low Power Binary to Excess Code Converter. International Journal of New Practices in Management and Engineering, 4(03), 06 - 10. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/38

[25] Hao Wang, Dihong Gong, Zhifeng Li, Wei Liu, "Decorrelated Adversarial Learning for Age-Invariant Face Recognition", IEEE 2019, Pages: 3522-3531. DOI Bookmark: 10.1109/CVPR.2019.00364

[26] Haiping Zhu, Zhizhong Huang, Hongming Shan, Junping Zhang, "Look Globally, Age Locally: Face Aging With An Attention Mechanism, IEEE 2020, DOI: 10.1109/ICASSP40776.2020.9054553

[27] Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin, Fei-Yue Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends ", 2018 IEEE Intelligent Vehicles Symposium (IV) A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[28] Geetanjali Sawant, Vinayak Bharadi, "Permission Blockchain based Smart Contract Utilizing Biometric Authentication as a Service: A Future Trend", IEEE 2021, 10.1109/ICCDW45521.2020.9318715

[29] Seogkyu Jeon; Pilhyeon Lee; Kibeom Hong; Hyeran Byun, "Continuous Face Aging Generative Adversarial Networks", DOI: 10.1109/ICASSP39728.2021.9414429

[30] Or-El, Roy, et al. "Lifespan Age Transformation Synthesis." European Conference on Computer Vision. Springer, Cham, 2020.

[31] Dr. H B Kekre, T K Sarode, V A Bharadi, Tejas Bajaj, February 26–27, 2010. "A Comparative Study of DCT and Kekre's Median Code Book Generation Algorithm for Face Recognition", ACM. https://doi.org/10.1145/1741906.1741961

[32] Sheng Wan; Tung-Yu Wu; Wing H. Wong; Chen-Yi Lee , "Confnet: Predict with Confidence", IEEE April 2018, DOI: 10.1109/ICASSP.2018.8461745

AUTHORS PROFILE

Geetanjali Nilesh Sawant received a B.Eng. degree in Information Technology and M.Tech. degree in Computer Engg. from Mumbai University, India. She worked as an Assistant Professor at Mumbai University. Currently, she is pursuing Ph.D. in the Information Technology department from Finolex Academy of Management and Technology, a remote center of Mumbai University. Her research interests include data mining, deep learning, and blockchain. She can be contacted at email: geetanjalinileshsawant@mail.com

Vinayak A. Bharadi received the B.E. and M.E. from Mumbai University in 2002 and 2007, respectively, and the Ph.D. degree in Electronics and Telecom. Engg. from NMIMS University, India in 2011. Currently, He is working as professor at FAMT, Mumbai University. He has authored or co-authored more than 200 refereed journal and conference papers, 7 book chapters, with Elsevier and Springer, IEEE, ACM etc. He has total 4 Granted and 9 Filed Patents as well as 06 Copyrights in his name. His research interests include the applications of Machine Learning, Deep Learning and artificial intelligence, Signal Processing, Image Processing and Computer Vision applied to Biometric Authentication Systems, operation, and control. He can be contacted at email: vinayak.bharadi@outlook.com

Kaushal K. Prasad received the Bachelors of Technology Mechanical Engg. from Dr. Babasaheb Ambedkar Technological University, Lonere, India in 1996 and Master of Technology in Thermal and environmental Engg. and the Ph.D. degree in Mechanical Engg. from IIT Kharagpur, in 2005 and 2013 respectively. He is Principal and professor in Mechanical Engg. Department at FAMT, Mumbai University. He has authored or co-authored more than 30 refereed journal and conference papers, 1 book. He has total 1 Granted and 1 Filed Patents as well as 02 Copyrights in his name. His research interests include the Fluid flow and heat transfer across different structures, cooling and air conditioning, Thermal Properties of Biometric and Environmental Sensors. He can be contacted at email: principal@famt.ac.in

Pravin S. Jangid received the B.Eng. and M. Eng. degree in Computer engineering from Thakur college of Engineering and Technology, Mumbai University, Maharashtra, India, in 2008 and 2015, respectively. Currently, he is an Assistant Professor at the Department of Computer Engg., Shree L R Tiwari College of Engineering, Mumbai University and pursuing Ph.D. in the Information Technology department from Finolex Academy of Management and Technology, a remote center of Mumbai University. His research interests include image processing, cloud computing, blockchain and artificial intelligence. He can be contacted at email: pravinjangid@gmail.com