International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

New Aadhaar with Multimodal Biometric Model-Based E-Voting System with Dynamic Hybrid IANFIS-PSO

K.Kanimozhi, K.Thangadurai

Abstract: ***This work deals with the E-voting system with a biometric concept that will make the voting system smart, secure and easy to vote which can be linked with Aadhaar card. While the process of doing the Aadhaar enrolment process Authorities gathered information of fingerprints and iris of every character and this whole fact of every person persists in the Indian government database. However these two biometric is not enough for the voter authentication process, besides improving the recognition rate, combining multimodal biometric modalities might be more appropriate for E-voting applications. If the Indian Government link this database to the voter ID present in these days vote casting gadget, then all of us can easily forge their votes the use of multimodal biometric authentication. With this motivation, the new Aadhaar with multimodal biometric-based E-voting systems (AMBEVS) system is designed in this work and it allows users to be confirmed using either modality. Here the validation of the voters is verified with the use of Dynamic Hybrid ANFIS-PSO. A critical function and objective of the proposed gadget are to decorate the photograph high-quality and low diploma of complexity for the security of multimodal biometric reputation frameworks. The experimental results show that the proposed AMBEVS are more robust, reliable and accurate as compared to the unimodal based biometric systems.***

Keywords: Aadhaar, Adaptive system of neuro-fuzzy inference, Multimodal Biometric Electronic Voting Machine, Optimization of particle swarm.

I. INTRODUCTION

The cause of Aadhaar primarily based election vote casting device in public elections that would permit human beings to vote electronically, from their current city. A petition was moved in the Delhi High Court on Monday seeking a direction to the Election Commission of India (ECI) to link the election identity cards with the Aadhaar number to curtail bogus voting [1].

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
K.Kanimozhi*, Department of Computer Science, Bharathidasan University/ Government Arts College/ , Karur, India.
Dr.K.Thangadurai, Department of Computer Science, Bharathidasan University/ Government Arts College/ , Karur, India.

Authentication of voters, the security of the voting process and protecting the voted facts and those are the principle challenges of cutting-edge election balloting. That is why it's miles important to generate a comfortable election vote casting device. All regarded Aadhaar is the government identification database that is full of identification and biometric data like fingerprints and iris scans on extra than 1.1 billion registered Indian residents [2].

The application issuer Indane has got the right of entry to the Aadhaar database through an API, which the enterprise relies on to, check a purchaser's repute and verify their identity. However, due to the fact the company hadn't secured the API, it was feasible to retrieve private records on every Aadhaar holder, no matter whether or not they may be a patron of the utility company or not. An attacker is bound to locate some valid Aadhaar numbers there which could then be used to find their corresponding information. By through, Illegal vote casting can be faced in an election procedure where the candidate casts the votes of all of the contributors or a few amounts of participants in the listing illegally. This results inside the lack of votes for the other applicants taking part and additionally increases the wide variety of votes to the candidate who plays this movement. This may be performed externally at the time of balloting.

The prevailing device Arduino and fingerprint scanner is the e-balloting gadget with authentication the usage of Aadhaar card. It determines the precise voter using his/her Aadhaar no whether or not he/she is a valid voter or no longer. It permits a specific voter to solid the vote on-line and updates the database on the server. The biometric on-line voting gadget makes use of the Aadhaar card to retrieve the information about the voter [3].However a unimodal biometric is not enough and would never fully serve the purpose of voter authentication. So it is best to look at other forms of biometrics such as Multi-biometrics and a combination of biometrics and technologies. With this motivation presenting the multimodal authentication machine is to have superior protection while undertaking the polling or vote casting and to obtain 0 tolerance towards fraud and other crimes and to ensure protection-safety of the citizens. The principal contribution of the work is as follows:

1. First, the behavioral features such as signature, speech, and keystrokes dynamics, hand movements, and gait are taken as behavioral multimodal biometrics.
2. Second also include the physical biometrics such as the face, Iris, Finger, Palm print, Finger Vein, Ear, Dorsal vein and lip motion.

3. For all the multimodal biometrics the reprocessing is done using a Guided filter method which reduces the noise.
4. Then perform the image contrast enhancement using Improved CLAHE-HSI (Contrast Limited Adaptive Heist Eqn-Intensity Hue Saturation) method to improve the image quality.
5. Feature Extraction using An Improved Average Gabor Wavelet Filter
6. From the feature extraction results, decision level fusion is done using Dynamic Hybrid ANFIS-PSO.

The rest of the paintings are dependent as follows: segment 2 deals with the related work of voting system with different methods and mechanisms; Section 3 has a detail description of multiple modal biometrics and working of AMBEVS. Section four suggests the experimental effects of proposed AMBEVS for gaining high-level safety with the assist of multimodal biometrics and as compared with the prevailing machine. At last, segment 5 states the realization with future work.

II. RELATED WORK

In this section, the different works that can be suggested on the basis of the voting machine that use biometric identity as a main idea are provided. Some other works use distinct algorithms and some distinct works have particular approaches that are fully based on multimodal biometric identification. Some global places in the beyond used the e-balloting structures, e.g. Ireland, Estonia and Norway. In [4] supplied an instance from the canton of Valais Switzerland in March 2017, when the postal ballots were no longer obtained by the electorate and when the ballots were returned, it was acknowledged that the people concerned had already voted.

In [5] provided an insight into the use and vulnerabilities of digital voting machines (EVMs) in software, hardware and associated sentences challenges. In [6] used the blockchain technology in digital e-voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any corporation or country. In [7] supplied industrial responses dealing with a block chain generation token-based gadget and therefore ensure the anonymity and security of the voting system. In [8] showed some issues about the use of the digital voting block chain.

In [9] proposed an electronic balloting scheme that plays communication amongst citizens and electoral entities with a minimal variety of phases and cryptographic operations. In [10] provided an in-progress e-vote casting structure that has no longer been tested against allegations made to increase the safety and reduce the importance of elections. In [11] the e-ballot initiatives have been argued about, but the sophisticated gadget is just a few. In [12] have added a smart phone-primarily based digital platform this is extra of an instance of i-vote casting rather than e-balloting. In [13] suggest a ranked-preference on-line balloting device, which addresses these challenges. It removes all hardwired restrictions at the feasible assignments of factors to exceptional applicants in line with the electorate's private possibilities.

In [14] formulated an accustomed e-vote casting gadget with fingerprint deployed in the public cloud which offers dependable and quicker results. In [15] proposed and discussed the design of a comfy e-balloting device based totally on cryptographic protocols and biometrics which can update the traditional vote casting system of India. In [16] proposed a comfy and green frontend balloting protocol the use of a relied on platform module for far off internet balloting with the relied on 1/3-celebration authentication protocol.

In [17] developed an e-balloting device using Microsoft visual basic (VB6) and SQL As the database is incorporated with an RFID device for the voter's authentication reason. Many unimodal biometrics structures for balloting endure from an inability to tolerate deformed facts due to noise, deformed facts from the sensor device, a distorted sign from environmental noise and variability of a character's physical look and pattern over time. However, multimodal biometric can clear up numerous of these barriers by combining facts from more than one drawback of the uni biometric structures through grouping the biometric resources for the powerful vote casting scheme. The garage requirements, processing time and computational demands of a multimodal biometric gadget are true to evaluate with the existing unimodal primarily based vote casting gadget.

III. PROPOSED SYSTEM

Digital voting is a crucial thing of the e-governance of a rustic for organizing human beings' desire in selecting political management. In the proposed AMBEVS system, multimodal biometric-based authentication is used to enhance security to EVM. During the enrollment phase, the multimodal biometrics and details of the candidate (photo, name, Aadhaar number, and voter id)are taken and stored in the remote server. The Aadhaar database can be working as the backend. During the voting process, the voter places the multimodal biometrics of his/her biological and physical traits as shown in Fig.1.

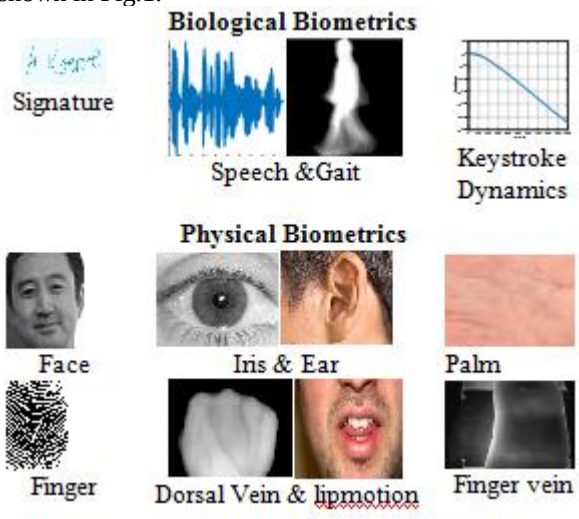

Fig.1. Multimodal Biometric Inputs

Then the feature of both biological and physical are matched with that of the Aadhaar database and checks its authenticity. A second check is carried out to verify whether the voter has already voted. If the multimodal biometrics is not validated or if the voter has already voted, then he/she is not allowed to vote.

The validation is done using the effective classifier algorithm of Dynamic Hybrid ANFIS-PSO. Hence, through these authentication checks, unauthorized voters and second time voting are eliminated and thus the security is ensured. The final polling result can be viewed at the central server by an authorized person using an IP address and password. The overall process of AMBEVS is shown in Fig.2.

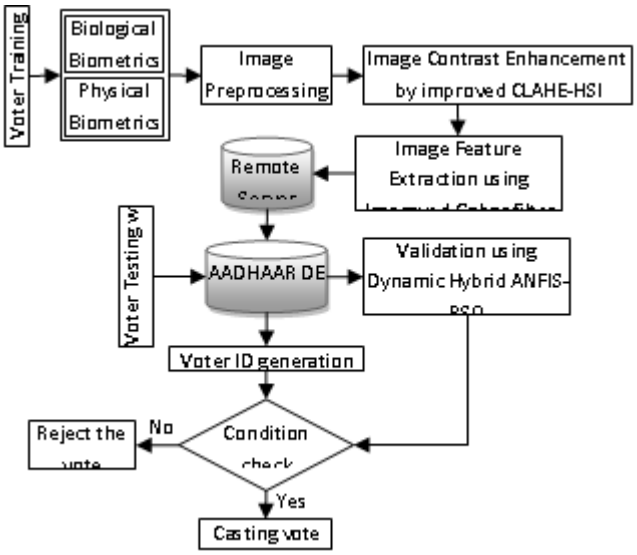

Fig.2.The overall process of AMBEVS

A. Image Preprocessing

The main aim of this section is to provide multilevel authentication in biometric systems. In this part, the biological and physical biometrics of a person is taken for the automatic identification of an individual by combining these two-level features of a person at the decision level fusion with the proposed classifier. In the preprocessing step, raw biometric template of all the biometrics such as Signature [18], Speech [19], Keystroke Dynamics [20], Gait Sequence [21], Face [19], Iris [19], Ear [19], Palm [19], Finger [19], Dorsal Vein [22], lip motion [23] and Finger vein [24] are preprocessed and the guided filter out is used to dispose of the noise and to enhance the pleasure of the picture. The step by step algorithm is given as follows:

- Read the input multimodal biometrics each image says (grayscale image), it acts as a guidance image.
- Make p =, where pacts as the guided filtering image (grayscale image).
- Enter the user fixed values assumed for and e_i, where r is the local window radius and e_i is the regularization parameter.
- Compute the mean by calculating I ₃ by which determine the covariance of $(I,$ using the formula:
  $cov_{I,p} = mean_{I,p} - mean_I .* mea$;
- Then compute the mean of $(I *$ and use it to compute the variance using the formula:
  $var_I = mean_{I,I} - mean_I .* mean$
- Finally, obtain the filtered output image by using the mean of and in the formula
  $q = mean_a * I + mea$;
- Display the output of noise-reduced images along with the input images.
- Image Contrast Enhancement using Improved CLAHE-HSI

In this phase, the main steps of the proposed CLAHE-HSI and electricity-regulation transformation [25] are defined. The CLAHE is a classic technique for reinforcing the nearby contrast of a photo; however, it has the challenge that the amplification of contrast is confined through clipping the histogram at a predefined clip coefficient. To overcome this trouble, a novel picture enhancement method is applied which mixes CLAHE-HSI electricity-law transformation.

The approaches of the proposed image enhancement algorithm are given as follows:

Step 1: Input multimodal RGB images are firstly transformed into IHS (intensity, hue, and saturation) area.

Step 2: CLAHE is carried out only to the luminance element i whilst keeping the h and s additives unchanged.

Step3: Observed by way of, based on CLAHE, strength-regulation transformation is carried out to the processed luminance component l to map a huge range of dark input values right into a narrower range of output values.

Step 4: At last, the modified luminance component , H, and S additives are transformed lower back to the RGB model, the result is converted again to the RGB photo format after which calculate PSNR.

It can further enhance the comparison, spotlight nearby info and stops over the enhancement of the flat area, which is of remarkable importance to also improve the translation accuracy of imaging logging statistics in the multimodal biometric database.

B. Image Feature Extraction

Feature Extraction using Improved Gabor Filter. Now that the reference point is situated, the fingerprint picture is filtered using the Improved Gabor filter to produce the multimodal biometrics function map that is used as a template and stored on a remote server. This model is combined with AADHAAR database templates in the subsequent matching step. The cause of region identification is to capture at some particular spatial scale the most significant axis of symmetry of a trait.

A sign's neighboring segment records can be acquired by converting the sign with a couple of band-skip quadrature filters (an exceptionally clear out and an outstanding filter). The use of quadrature filters enables the calculation of the amplitude and phase of the signal at a specified spatial region (spatial frequency). The selection of quadrature filters is the sophisticated Gabor filter that can be constructed with arbitrary bandwidth. In order to achieve simultaneous localization of spatial and frequency data, the signal analysis must be carried out at specific locations within the signal over a narrow variety (scale) of frequencies.

This can be achieved by constructing a filter financial institution to clear out the use of fixed quadrature filters by rescaling the enhanced Gabor. Each scaling is intended to determine the specific frequencies of the analyzed signal. Symmetry information is examined by examining variables where the reaction of the even clear out dominates the reaction of the uncommon clear out taking the distinction in their absolute values.

The transfer function (G) of an improved Gabor filter is built as the one produced from additives within the frequency domain: A single-dimensional Log Gabor function that regulates the frequencies at which the clear reaction and the rotational symmetric angular Gaussian feature control the selectivity of the filter's orientation.

$$G(\omega,\varphi,\theta,\sigma) = \exp\left(\frac{(\log(\omega/\omega_0))^2}{2(\log\varphi/\omega_0)}\right) \times \exp\left(-\frac{\alpha(\varphi,\theta)^2}{2\sigma_\alpha^2}\right)$$

The Gabor function is the wavelength, is the phase offset, is the orientation and is the aspect ratio will be calculated, also the x is the position of a light impulse in the visual field. The data produced will be used for the further classification procedure where the validation is checked for each voter. The ranges of texture part detection are described below.

Step 1: The Gabor filter and wavelet filter out are implemented in one path (in addition to all the vertical traces of the biometric image) on the side of the set of all parallel lines of the biometric image. The output is provided as a Gabor filter $H_k(x_c,y) = I(x_c,y) *$ where suggested convolution operator, clearly reflects Gabor with the fixed parameter $k = (u,l), I(x_c,$ represents the the column of the biometric picture , and denotes the reaction of the kth filter. The respective filtered images obtained for a set of four Gabor filters $H_1, H_2, H3, I.$ Further, the image i have filtered the usage of the 2 maximum normally used DWT together with the same instructions. Let H5, H6, H7, and H8 denote answers from the filter. Where H5 and H6 indicate a sub-band of stage-1 and degree-2 filter decomposition respectively, and where H7 and H8 denote comprehensive Gabor decomposition sub-band of degree-1 and stage-2 respectively.

Step 2: Asymmetric Gaussian filter smoothed the filtered snapshots obtained in step 1. $V_i(x,y) = H_i(x,y) * L(x,$ where, $L(x,$ refers to a Gussian filter $\sigma_x = 8x$ If pix are filtered along parallel vertical traces and $\sigma_y = 8x$, If images are filtered with parallel horizontal strains Vi(x, y) refers to the converted output of the biometric image in which $i = 1,\ldots.$

Step 3: Steps 1 and 2 are repeated in the orthogonal course to reap filtered biometric pix. Let Fi(x, y) denote all the snapshots filtered, where i = 1,..., 16. A sixteen-dimensional vector F(x, y) is acquired as $F(x,y) = [F_1(x,y),\ldots,F_{16}(x,y$

Step 4: A one-dimensional map Γ of the vectors $\{F(x,y$ is produced by detecting the feeling edge. For every pixel $(x,$, the scalar index $M(x,$ of the reference vector closest to $\{F(x,y$ is assigned

$$M(x,y) = \arg\min_i \|F(x,y) - u \text{ for } w_i \in$$

The vector photograph is thus transformed into a scalar photograph. Characteristic map M is smoothed with asymmetric Gaussian $E(x,y) = M(x,y) * L(x,$ Where $L(x,$ Gaussian filter indicates and E denotes a smooth picture. The function map (scalar image) from the photo's filtered images is shown.

C. Decision Module Using Dynamic Hybrid Anfis-Pso

The score level of the fusion process decision is based on the use of Dynamic Hybrid ANFIS-PSO. The final score of mapping is compared to a threshold value for distinguishing the authentic man or woman or impostor. In particular, neural community features and regression are used to dynamically generalize in put interactions based entirely on the adaptive neuro-fuzzy inference gadget (ANFIS). This approach was also combined with particle swarm optimization to optimize the voting prediction version. In dynamic evaluation, software sports consisting of network site visitors and device calls are analyzed whilst the utility is jogging.

In PSO, swarm begins with a collection of random responses, each of which is called a particle, represented here as functions, and Si represents the role of the particle. Similarly, a particle swarm moves in the region of trouble where, Vi expresses the velocity of the particle. When step-thru inputs Si a health characteristic f is assessed. Each particle statistics has its adequate position in the good fitness that has been achieved so far, in the vector. tracks the appropriate position identified with the help of any neighborhood member.

Inside the frequent model of PSO, the equation, it is the most suitable point for the entire population. A fresh velocity is obtained for each particle i in each iteration according to the individual's best positions represents the highest suitable factor within the entire population. A fresh pace is completed in each iteration for any particle in accordance with the adequate character positions $\vec{p}_i($, and $\vec{p}_i^{\,g}($ community. The new speed can be delivered by:

$$v_i(t+1) = wv_i(t) + c_1\emptyset_1.(\vec{p}_i(t) - \vec{x}_i(t)) + c_2\emptyset_2.(\vec{p}_i(t) - \vec{x}_i(t))$$

In which w represents the inertia weight, the high-quality acceleration coefficients are shown by way of and c2. and represents random vectors uniformly distributed in [0,1], wherein a random cost is attempted for every measurement vi limits inside the $[-v_{max}, v_{mi}$ collection depends on the issue. If the velocity exceeds the aforementioned limit, it is rearranged within its suitable boundaries in some instances. The location of every particle alters depending upon the velocities as follows:

$$s_i(t+1) = s_i(t) + v_i(t+1)$$

In accordance with the above equation, the particles tend to accumulate close to the large. The use of PSO to design an FS or optimize parameters is described as:

$$R + i: if\ x_1(k)\ is\ A_{i1}\ And, \ldots, And\ x_n(k)\ is\ A_{in}, the\ u(k)\ is\ \alpha_i$$

Here, is a crisp value, k is the time step, the variables entered are $x_i(k), i = 1, \ldots$, is a fuzzy set and $u($specifies the device output variable. Includes r rules for the FS and n enter variables, their free parameters are described by a position vector. Following the implementation and initialization of rule techniques, the preliminary parameters of the preceding portion are discussed and the ith response vector is generated as:

$$s_i = [s_{i1}, s_{i2}, \ldots, s_{iD}]$$
$$= [m_{11} + \Delta m^i_{11}, b_{fix} + \Delta b^i_{11}, \ldots, m_{1n} + \Delta m^i_{1n}, b_{fix} + \Delta b^i_{1n}, a_1, \ldots, m_{r1} + \Delta m^i_{r1}, b_{fix} + \Delta b^i_{r1}, \ldots, m_{rn} + \Delta m^i_{rn}, b_{fix} + \Delta b^i_{rn}, a_r]$$

In the equation, Δn and Δirepresents small random numbers, αi designates a random wide variety arbitrarily and homogeneously allocated in the fuzzy output range of the machine. The evaluation function f for Si based mainly on the results of the bushy device. The number one speed values of all particles, $v_i(0), i = 1, \ldots$, are generated randomly. The general performance of each particle is assessed in accordance with the FS indicated and f is defined because the above listed E(t) error-index. The excellent Pi position of each particle and the pleasant particle ƥn the whole populace is received in keeping with . The whole study method is performed once a predefined paradigm has been acquired [26].

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this phase, the information of the voter can get from the Aadhaar card database. It's far the newly developed information which has all of the facts regarding the people. Through the use of this database took the voter's records will be stored within the far off server. The proposed dynamic ANFIS-PSO classifier is utilized for the voter verification and this method is compared with the existing methods such as SVM and IANFIS. The parameters such as SSIM, F-measure, and accuracy are calculated to measure the performance efficiency of the three methods.

D. F-Measure Result Comparison

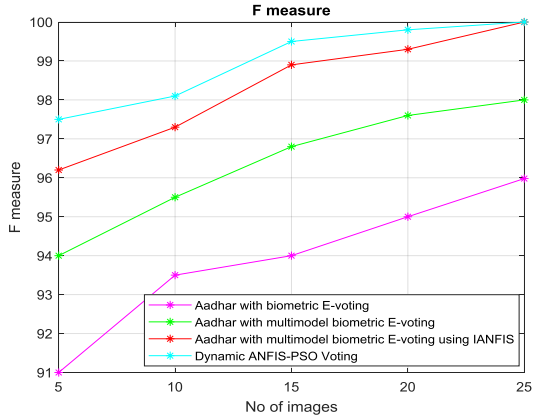

Fig.3. F-degree overall performance assessment in diverse compression techniques

Fig.3 indicates that the F-measure evaluation effects between proposed dynamic ANFIS-PSO, and existing IANFIS and SVM. The proposed method has a high F-measure value of 100. From the results, it is well known that proposed Dynamic ANFIS-PSO obtain high F-measure indicating the good lung nodule detection. Because the proposed scheme is based on excellent feature extraction called improved Gabor filter based concept is enhancing the learning efficiency of the proposed Dynamic ANFIS-PSO. When comparing the F-measure rate among the existing methods such as IANFIS and SVM are providing fewer rates of 98 and 98.98 respectively, which indicates the proposed work can give better fake voter detection results than the existing methods.

E. Recall Result Comparison

Fig.4 shows that the recall comparison results between proposed Dynamic ANFIS-PSO, and existing IANFIS and SVM. The proposed method has a high value of recall rate of 0.98. From the results, it is well known that proposed Dynamic ANFIS-PSO obtains high recall rate value indicating the good fake voter detection rate.

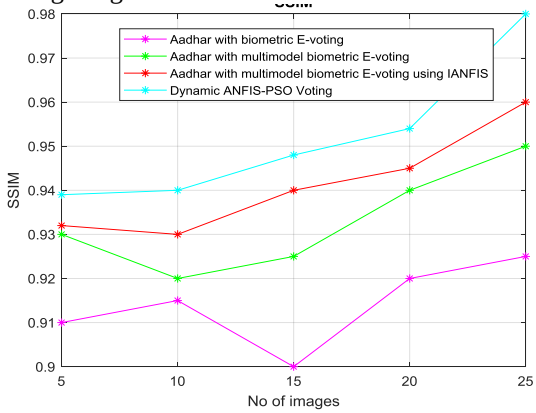

Fig.4. SSIM performance comparison in various compression techniques

Because the proposed scheme is having the effective image enhancement stage which reduces the noises. When comparing the recall rate among the existing methods such as IANFIS and SVM, providing a recall rate of 0.95and 0.925respectively, which shows the proposed work can give better detection results than the existing methods. The reason is that the proposed E-voting system has a good image preprocessing technique which removes the irrelevant information while verification process.

F. Accuracy Result Comparison

Fig.5 shows that the accuracy comparison results between proposed Dynamic ANFIS-PSO, and existing IANFIS and SVM. From the figure, the proposed method can obtain high accuracy when compared to existing methods. It is an effective way of getting the authenticated voter accurately with the high accuracy rate of 99.1%. When comparing the accuracy among the existing methods such as IANFIS, SVM and Aadhaar with biometric providing less rate of 98.3%and 97%respectively. Through the results, it can be seen that the proposed work is much better than the existing methods.

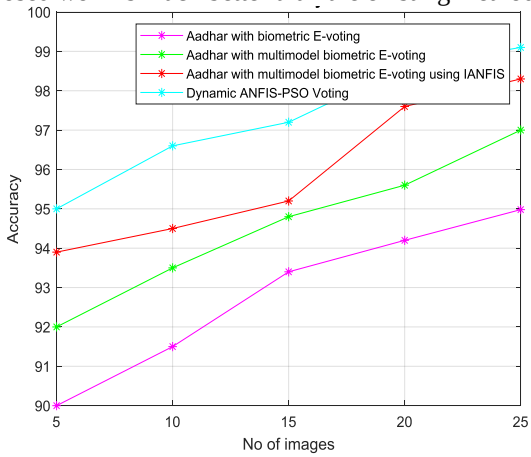

Fig.5. Accuracy performance comparison in various compression techniques

V. CONCLUSION AND FUTURE WORK

In this job, AMBEVS with a unique hybrid ANFIS and PSO became a proposal to predict the best parameters of an assessment of voting malware.

Brand new gadget prevents get admission to unlawful voters, affords ease of use, transparency and keeps the integrity of the balloting procedure. The device additionally prevents more than one vote by way of the identical person and tests eligibility of the voter. The experimental results display that the proposed AMBEVS machine is notably powerful for casting the vote from anywhere.

Future pictures include expanding studies to address acknowledged difficulties in the choice of factors, such as identifying and discarding noise-related point variables, illumination, and so forth. Yet achieving better performance and accuracy. Another is to focus on building a system that is much more secure and provides privacy for the voters and can include large databases with cryptography methods.

Conflict of Interest: It is necessary to express that the authors does not have any conflict of interests from the above discussions.

REFERENCES

1. ANI "Petition in Delhi HC seeking Aadhaar-based election voting system", Jul 15, 2019, Available at: http://www.ecoti.in/D8Us9b
2. Zack Whittaker, "A new data leak hits Aadhaar, India's national ID database", for Zero Day, March 23, 2018. Available at: https://zd.net/2EYYKtM
3. Rezwan, Rahil, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, and MdAbdur Rahman. "Biometrically secured electronic voting machine." In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pp. 510-512. IEEE, 2017.
4. D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada. Election security and economics: It's all about eve. Proc. Int. Joint Conf. Electron Voting, 2017, pp. 1–28.
5. S. Wolchok et al.,Security analysis of India's electronic voting machines. Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 1–14.
6. Singh, Ashish, and Kakali Chatterjee. SecEVS: Secure Electronic Voting System Using Blockchain Technology. 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 863-867. IEEE, 2018.
7. J. Stern. Votem—Voting for a Mobile World. Accessed: Jul. 31, 2018.
8. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, Blockchain challenges and opportunities: A survey. Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
9. López-García, Lourdes, Luis J. Dominguez Perez, and Francisco Rodríguez-Henríquez. A pairing-based blind signature e-voting scheme. The Computer Journal 57, no. 10 (2013): 1460-1471.
10. F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, Blockchain-based e-voting system. Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), San Francisco, CA, USA, Jul. 2018, pp. 983–986.
11. L. P. Alonso, M. Gasco, D. Y. M. del Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton. E-voting system evaluation based on the council of Europe recommendations: Helios voting. IEEE Trans. Emerg. Topics Comput., Nov. 2018.
12. N. Kshetri and J. Voas. Blockchain-enabled e-voting. IEEE Softw., vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.
13. Yang, Xuechao, Xun Yi, Surya Nepal, Andrei Kelarev, and Fengling Han. A secure verifiable ranked choice online voting system based on homo morphic encryption. IEEE Access 6 (2018): 20506-20519.
14. Devi, Gandhi Usha, KannanAnusha, and G. V. Rajyalakshmi. An Enhanced e-Voting System in Cloud Using Fingerprint Authentication. Advances in Computer Science and its Applications, pp. 1219-1224. Springer, Berlin, Heidelberg, 2014.
15. Kar, Nirmalya, Sharmistha Roy, AshimSaha, KunalChakma, and AnupamJamatia. A Biometric Based Design Pattern for Implementation of a Security Conscious E-Voting System Using Cryptographic Protocols.International Conference on Advances in Information Technology and Mobile Communication, pp. 78-85. Springer, Berlin, Heidelberg, 2012.
16. Saad, Amna, MohdIzzatMohamatRoseli, and Muhammad SaufiZullkeply. A smart e-voting system using RFID authentication method for a campus electoral. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, p. 31. ACM, 2014.
17. George, Vinodu, and M. P. Sebastian. Remote Internet voting: developing a secure and efficient frontend. CSI transactions on ICT 1, no. 3 (2013): 231-241.
18. Shashikumar, D. R., K. B. Raja, R. K. Chhotaray, and SabyasachiPattanaik. Biometric security system based on signature verification using neural networks. 2010 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6. IEEE, 2010.
19. Toygar, Önsen, EsraaAlqaralleh, and AymanAfaneh. Person Identification Using Multimodal Biometrics under Different Challenges. Human-Robot Interaction-Theory and Application. IntechOpen, 2017.
20. A. A. Ahmed and I. Traore. Biometric Recognition Based on Free-Text Keystroke Dynamics. IEEE Transactions on Cybernetics, vol. 44, no. 4, pp. 458-472, April 2014.
21. B. Jawed, O. O. Khalifa and S. S. NewajBhuiyan, Human Gait Recognition System. 2018 7th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, 2018, pp. 89-92.
22. K. Vasagiri and S. R. Parvata. Dorsal hand vein Biometric authentication using complex Walsh transform. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 533-537.
23. Saeed, Usman. Person identification using behavioral features from lip motion. Face and Gesture 2011, pp. 155-160. IEEE, 2011.
24. M. Sapkale and S. M. Rajbhoj. A biometric authentication system based on finger vein recognition. 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-4.
25. Fu, Qingqing, Mehmet Celenk, and Aiping Wu. An improved algorithm based on CLAHE for ultrasonic well logging image enhancement. Cluster Computing (2018): 1-10.