IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

REAL TIME SECURE CLICKBAIT AND BIOMETRIC ATM USER AUTHENTICATION AND MULTIPLE BANK TRANSACTION SYSTEM

Miss. R. Haripriya, (M.C.A) [1], Mrs. R. Vijayalakshmi, M.C.A, M.Phil., (Ph.D.) [2]

Department of MCA, Krishnasamy College of Engineering and Technology[1]

Associate professor, Department of MCA, Krishnasamy College of Engineering and Technology[2]

Abstract: ATM or Computerized Teller Machines are generally utilized by individuals these days. Performing cash withdrawal exchange with ATM is expanding step by step. ATM is vital gadget all through the world. The current traditional ATM is helpless against violations as a result of the fast innovation improvement. A sum of 270,000 reports have been accounted for with respect to check card extortion and this was the most detailed type of data fraud in 2021. A protected and effective ATM is expected to expand the general insight, ease of use, and comfort of the exchange at the ATM. In this day and age, the area of PC vision is progressing dangerously fast. The new advancement in biometric ID strategies, including finger printing, retina filtering, and facial acknowledgment has put forth an extraordinary attempt to save what is happening at the ATM. In particular, the objective of this venture is to give a PC vision strategy to tackle the security risk related with getting to ATM machines. This task proposes a programmed teller machine security model that utilizes electronic facial acknowledgment utilizing Profound Convolutional Brain Organization. In the event that this innovation turns out to be broadly utilized, appearances would be safeguarded as well as their records. Face Check Misleading content connection will be created and shipped off ledger holder to confirm the character of unapproved client through a few devoted fake savvy specialists, for distant certificate. In any case, clearly man's biometric highlights can't be repeated, this proposition will go quite far to take care of the issue of record security making it feasible for the genuine record proprietor alone approach his records. This wipes out the chance of extortion coming about because of ATM card burglary and replicating by utilizing this continuous dataset, the proposed framework accomplishes the most noteworthy precision with 97.93%.

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers. ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch Most ATM transactions can be availed with the use of a debit or credit card. There are some transactions that need no debit or credit card. In 1960, an American named Luther George Simjian invented the Bank graph, a machine that allowed customers to deposit cash and checks into it [1]. The first ATM was set up in June 1967 on a street in Enfield, London at a branch of Barclays bank. A British inventor named John Shepherd-Barron is credited with its invention. The machine allowed customers to withdraw a maximum of GBP10 at a time. Automated Teller Machines (ATMs) are mainly of two types. One is a simple basic unit that allows you to withdraw cash, check balance, change the PIN, get mini statements also, get account refreshes. The more intricate units give offices of money or really look at stores and credit extension and bill installments. There are likewise on location and offsite Mechanized Teller Machines the on location ATMs are inside the bank premises, dissimilar to the offsite ones which are available in various niches and corners of the country to guarantee that individuals have fundamental financial offices and moment cash withdrawals on the off chance that they can't go to a bank office. ATMs can likewise be sorted in light of the names relegated to them [2]. A portion of these names are recorded beneath Green Mark ATMs Utilized for horticultural purposes. Yellow Mark ATMs-Utilized for web based business transactions Orange Mark ATMs-Utilized for share transactions. Pink Name ATMs-Explicitly for females to assist with keeping away from the long lines and holding up time. White Mark ATMs - Presented by the Goodbye bunch, white name ATMs are not claimed by a specific bank but rather substances other than the bank. Brown Name Banks-Worked by an outsider other than a bank [3]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

II. PROBLEM STATEMENT

Financial fraud is a very important problem for Banks and current secure information in the ATM card magnetic tape are very vulnerable to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be confirmed as the card owner. Face Based ATM login Process the ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. When there are “Shoulder Surfers" who try to peek over the cardholder’s shoulder to obtain his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be cautious. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are removed. The use of facial recognition enables to deliver more advanced transactions at its ATMs because facial recognition provides an extra layer of security for both the cardholder and the bank [4].

Bank customers can use their Debit/Credit card at the ATM to access their accounts, rather than being limited to only those accounts associated with their ATM card. With facial recognition, Bank can now guarantee its customers the most rigorous security along with the convenience of open banking. The process used by the bank is to capture the facial images of their customers in the bank branch and then store the images in a secure biometric database. When the customer taps their ID card or inserts their bank card at the ATM, Deep Face activates biometric software supplied by DL Model. The system captures multiple facial images and determines the best image to be used for recognition. In the event that none are deemed to be suitable, the customer will be prompted to move closer, step back, remove their hat or sunglasses or whatever is needed to capture a suitable image.

The captured image is sent to the biometric processing system where it is compared to the customer’s image stored in the bank’s ID database. Once verified, the customer can access their accounts and perform authorized transactions. It’s not Verified, ATM Camera to capture the user facial image. Internet-friendly mobile communication device, which is accessible on 24/7 bases, is required for the bank account owner to handle the remote certification.

Dedicated intelligent agents for intelligent monitoring of initiated transactions and real-time feedbacks (alerts) to appropriate banking security points. Robust Internet and GSM networks are needed to enable multimedia messaging services (MMS) for certification and authorization processes. There are numerous anti-fraud measures built into the system to add to its security. One such measure is the support of an infra-red lens to capture additional facial details to prevent fraud attempts [5].

ADVANTAGES

- The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user.
- It can be used to reduce fraudulent attempts.
- To prevent theft and other criminal activities.
- Secure facial authentication platform that users can trust
- Provide safe and secure lifestyle infrastructure
- Prevent unauthorized access using Face verification Link.
- Fast and Accurate Prediction

ALGORITHM OF DCNN

Profound convolutional brain organizations (CNN or DCNN) are the sort most usually used to recognize designs in pictures and video. DCNNs have developed from conventional counterfeit brain organizations, utilizing a three-layered brain design motivated by the visual cortex of creatures

DCNN calculations were made to consequently distinguish and dismiss ill-advised face pictures during the enrolment interaction. This will guarantee appropriate enrolment and accordingly the most ideal execution.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

SYSTEM ARCHITECTURE DIAGRAM

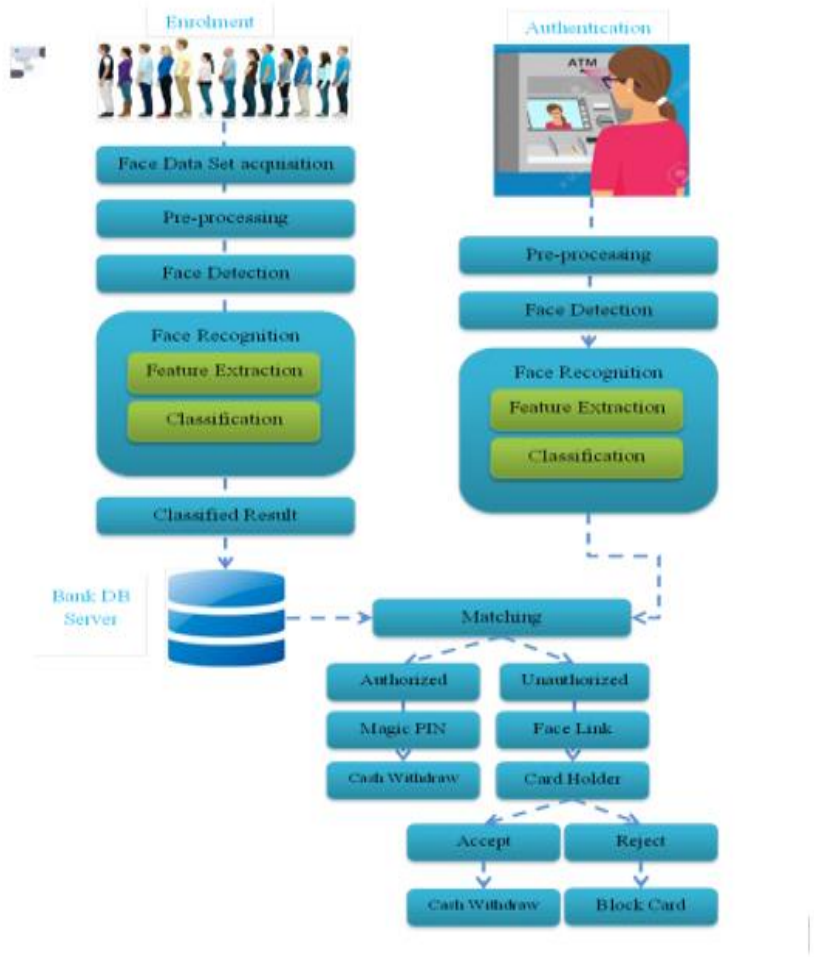


Fig 2.1 system architecture diagram

III. SYSTEM ANALYSIS

1.ATM SIMULATOR

ATM Test system is a Cutting edge testing application for XFS-based ATMs (otherwise called Progressed Capability or Open-Engineering ATM Test system is a web innovation to permit ATM testing with a virtualized rendition of any ATM.ATM Test system utilizes virtualization to furnish with sensible ATM reproduction, combined with computerization for quicker, more productive testing for face validation and pin confirmation and obscure Face Forwarder Procedure [6].

2. FACE RECOGNITION MODULE

2.1. Face Enrollment

This module starts by enlisting a couple of front facing face of Bank Recipient layouts. These layouts then become the reference for assessing and enrolling the formats for different postures: shifting up/down, drawing nearer/further, and turning left/right.

2.1.1. Face Image Acquisition

Cameras should be deployed in ATM to capture relevant video. Computer and camera are interfaced and here webcam is used.

2.1.2. Frame Extraction

Outlines are removed from video input. The video should be isolated into grouping of pictures which are additionally handled. The speed at which a video should be isolated into pictures relies upon the execution of people. From we can say that, generally 20-30 edges are taken each subsequent which are shipped off the following stages.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

2.1.3. Pre-processing

Face Image pre-processing are the steps taken to format images before they are used by model training and inference. The steps to be taken are:

- Read image
- RGB to Grey Scale conversion

Resize image Original size (360, 480, 3) — (width, height, no. RGB channels). Resized (220, 220, 3)

- Remove noise smooth our image to remove unwanted noise. We do this using.
- Binarization- Image binarization is the process of taking a grayscale image and converting into black-and-white, essentially reducing the information contained within the image from 256 shades of grey to 2: black and white, a binary image [7].

2.1.4. Face Detection

Accordingly, in this module, Locale Proposition Organization (RPN) produces returns for money invested by sliding windows on the component map through secures with various scales and different viewpoint proportions. Face discovery and division technique in light of further developed RPN. RPN is utilized to create returns for money invested, and return on initial capital investment Adjust loyally saves the specific spatial areas. These are liable for giving a predefined set of jumping boxes of various sizes and proportions that will be utilized for reference while first foreseeing object areas for the RPN.

RPN

A **Region Proposal Network**, or **RPN**, is a fully convolutional network that simultaneously predicts object bounds and objectless scores at each position. The RPN is trained end-to-end to generate high-quality region proposals. It works on the feature map (output of CNN), and each feature (point) of this map is called Anchor Point. For each anchor point, In place 9 anchor boxes (the combinations of different sizes and ratios) over the image. These anchor boxes are cantered at the point in the image which is corresponding to the anchor point of the feature map.

Training of RPN

To know that for each location of the feature map have 9 anchor boxes, so the total number is very big, but not all of them are relevant. If an anchor box having an object or part of the object within it then can refer it as a **foreground**, and if the anchor box doesn't have an object within it then can refer it as **background**. So, for training, assign a label to each anchor box, based on its Intersection over Union IOU with given ground truth. In the basically assign either of the three (1, -1, 0) labels to each anchor box.

Label = 1 (Foreground): An anchor can have label 1 in following conditions,
If the anchor has the highest IOU with ground truth. If the IOU with ground truth is greater than 0.7. (Iou >0.7).
Label = -1 (Background): An anchor is assigned with -1 if IOU < 0.3.
Label = 0: If it doesn't fall under either of the above conditions, these types of anchors don't contribute to the training, they are ignored. After assigning the labels, it creates the mini-batch of 256 randomly picked anchor boxes, all of these anchor boxes are picked from the same image.
The ratio of the number of positive and negative anchor boxes should be 1:1 in the mini-batch, but if there are less than 128 positive anchor boxes then we pad the mini-batch with negative anchor boxes.
Now the RPN can be trained end-to-end by backpropagation and stochastic gradient descent (SGD).

The processing steps are

- Select the initial seed point
- Append the neighbouring pixelsintensity threshold
- Check threshold of the neighbouring pixel
- Thresholds satisfy-selected for growing the region.
- Process is iterated to end of all regions.

2.1.5. Feature Extraction

After the face detection, face image is given as input to the feature extraction module to find the key features that will be used for classification. With each pose, the facial information including eyes, nose and mouth is automatically extracted and is then used to calculate the effects of the variation using its relation to the frontal face templates.

2.1.6. Face Classification

The CNN creates feature maps by summing up the convolved grid of a vector-valued input to the kernel with a bank of filters to a given layer. Then a non-linear rectified linear unit (RELU) is used for computing the activations of the convolved feature maps. The new feature map obtained from the RELU is normalized using local response normalization

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

(LRN). The output from the normalization is further computed with the use of a spatial pooling strategy (maximum or average pooling). Then, the use of dropout regularization scheme is used to initialize some unused weights to zero and this activity most often takes place within the fully connected layers before the classification layer. Finally, the use of softmax activation function is used for classifying image labels within the fully connected layer.

2.2. FACE AUTHENTICATION

After capturing the face image from the ATM Camera, the image is given to face detection module. This module detects the image regions which are likely to be human. After the face detection using Region Proposal Network (RPN), face image is given as input to the feature extraction module to find the key features that will be used for classification. The module composes a very short feature vector that is well enough to represent the face image. Here, it is done with DCNN with the help of a pattern classifier, the extracted features of face image are compared with the ones stored in the face database. The face image is then classified as either known or unknown. If the image face is known, corresponding Card Holder is identified and proceed further [8].

Prediction

In this module the matching process is done with trained classified result and test Live Camera Captured Classified file. Hamming Distance is used to calculate the difference according to the result the prediction accuracy will be displayed.

3. UNKNOWN FACE FORWARDER MECHANISM.

Unknown Face Verification Link will be generated and sent to card holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system [9]

4. TRANSACTION MODEL

4.1. Enter the Withdrawal Money

Enter your withdrawal amount and press enter. But make sure your withdrawal amount does not exceed your balance in the account otherwise transaction will fail.

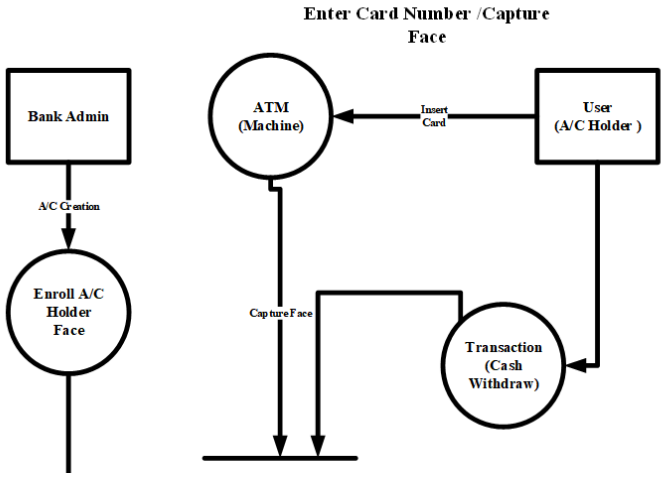
4.2. Collect the Cash

To collect your money from the lower slot of the machine. Take your money before 30 seconds [10].

IV. DIAGRAM

1.DATA FLOW DIAGRAM

A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

V. CONCLUSION

In conclusion, Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level. The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the bank account owner in all the available and accessible transactions.

OUTPUT

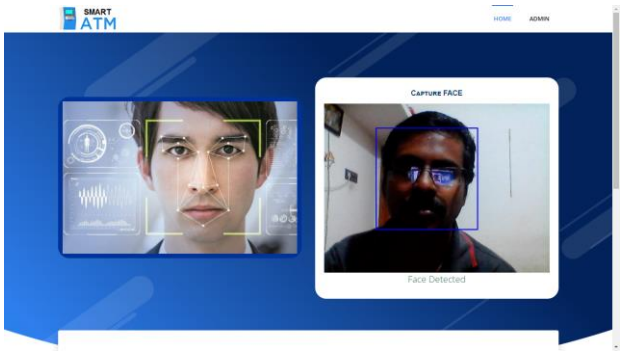


Fig 6.1 To capture face

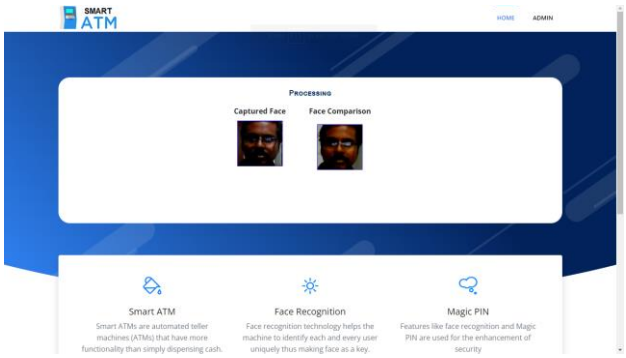


Fig 6.2 To processing the capture face and face Comparison

Fig 6.3 Waiting for account holder approval

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12678

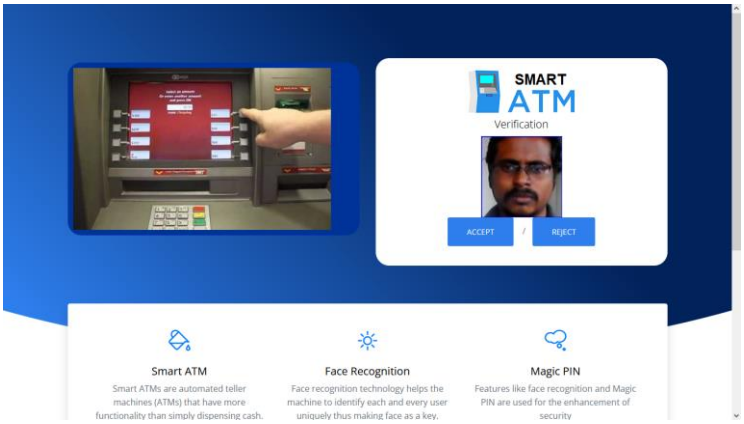


Fig 6.3 verification

Fig 6.4 holder rejected

VI. FUTURE ENHANCEMENT

In future, the recognition performance should be further boosted by designing novel deep feature representation schemes.

REFERENCES

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.

[2] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detection and recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.

[3] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ``Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.

[4] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring system using RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1-4.

[5] J. Y. Zhu, C. Sun, and V. Li, "Granger-Causality-based air quality estimation with spatio-temporal (ST) heterogeneous big data," presented at 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2015.

[6] C. J. Wong, M. Z. MatJafri, K. Abdullah, H.S. Lim, and K. L. Low, "Temporal air quality monitoring using surveillance camera," presented at IEEE International Geoscience and Remote Sensing Symposium, IEEE, 2007.

[7] S. Y. Muhammad, M. Makhtar, A. Rozaimee, A. Abdul, and A. A. Jamal, "Classification model for air quality using machine learning techniques," International Journal of Software Engineering and Its Applications, pp. 45-52, 2015.

[8] A. Sarkar and P. Pandey, "River water quality modelling using artificial neural network technique," Aquatic Procedia, vol. 4, pp. 1070-1077, 2015.

[9] E. Kalapanidas and N. Avouris, "Applying machine learning techniques in air quality prediction," Sept. 1999.

[10] H. Zhao, J. Zhang, K. Wang, et al., "A GA-ANN model for air quality predicting," IEEE, Taiwan, 10 Jan. 2011.