AADHAR Integrated Biometric Vigilance System-
A digital measure to curb malpractices in entrance tests

Dr Surekha B [a*], Dr Viswanadha Raju S [b]

[a] Professor, Dept. of ECE, K. S. Institute of Technology , Bangalore, Karnataka, INDIA
borrasurekha@gmail.com

[b] Professor, Dept. of CSE, JNTUHCEJ, JNT University, Hyderabad, Telangana, INDIA
svraju.jntu@gmail.com
*Corresponding author

Abstract- In recent years, increase in unemployment and corruption has raised the irregularities in entrance exams conducted by the state public service commission. Tricks such as impersonation, copying, manipulation of records/answer sheets are used to offer high marks for undeserving candidates, in exchange for kickbacks. Though there are various layers of security measures, the problem is deep rooted in entire process. Measures to strengthen the examination process and devoid it of corruption and malpractices is required to protect better human resources and skills. Further, providing transparency, fairness and accountability in exams conducted ensures equality, justice and build faith in citizens. In order to curb and check the corrupt practices in entrance tests, a digital registration and real time vigilance system is proposed in this paper. Registration of AADHAR number of candidates, invigilators, evaluators and board officials, and verification of their multi-biometrics at various stages of recruitment process solves bogus candidates, mismanagement of applications, verification of antecedents and nepotism. Installation of hi-tech electronic equipment like surveillance cameras and RF detectors in exam centre instil vigilance and stops impersonation and copying. Captured video data is also stored for future investigations, and scrutiny and accountability of invigilators and evaluators. Real time implementation of image processing techniques on high resolution video streams collected from networked surveillance cameras is used for face identification and anomaly detection on the spot. Further, the problem of manipulation of answer sheets is solved by employing coding techniques and visual secret sharing concepts of scanned answer sheets in the proposed method. Though the proposed system is costly, it is robust and will help bolster public trust, and resolves the nightmare of the candidates and authorities conducting the exam. Further it brings genuine candidates at the helm of administration, which is essential for realizing ethics in governance.

Keywords: AADHAR, Automated Surveillance Systems, Biometrics, Compressive Theory, Entrance tests, Impersonation, Image Processing, OMR, Visual Cryptography

1. Introduction

With an increase in rising competition, unemployment and desire to get into civil services, malpractices and corruption are in rise at every stage of examination/recruitment process. The series of incidents like Vyapam scam (Web-1), cancellation of Uttar Pradesh Provincial Service Examination, charges against chairman of Rajasthan Public Service commission's chairman and arrest of CM of Haryana, All India Pre Medical Test exam etc. shows that there is rampant corruption and abnormalities in State level Public Services Commissions. The corruption is widespread and is involved in almost every stage starting from the selection of members conducting the examinations, application filling, and malpractices in actual exam, evaluation, and interview. Tricks such as impersonation, copying, manipulation of records/answer sheets has become more common.

The recruitment or admission process of public service commission has become the nightmare to the candidates and authorities conducting the exam. Malpractices in such prestigious exams leads to social and economic inequality rises as only well to do can utilize power and money to get job or

admission and is a psychological setback for youth and family (Web-2). This not only discourages the honest and hardworking candidates but also is a serious threat to internal security, law and order. The rescheduling of exams also adds the cost of conducting exam and stress to the candidates. The main cause for the corruption is lack of fairness, transparency and accountability. This can be tackled at different stages by employing digital technology wherever possible.

So, it is the high time for commissions conducting exams to incorporate measures and to rectify the related concerns with the help of technological innovations to reinstate the confidence in the citizens and to make the examination/recruitment system robust.

Section 2 identifies the security requirements of written tests and the relevant work. Section 3 defines the frame work of the proposed vigilance system. Section 4 draws the conclusion.

2. Literature Survey

In the present scheme of written tests, candidates are allocated a particular exam centre where they are allowed to take the exam under the surveillance of an invigilator assigned by the concerned authority. If the invigilator is not strict to his duty then the students may avail the restricted resources (i.e. books, notes, impersonation, and guidance from third party, electronic media, and mobiles/pagers) which will decline the standard of the exam. Recent highlighted scams in entrance tests indicate that the present systems are prone to challenges associated with impersonation and manipulation of answer sheets.

The concern of prevailing corruption & malpractices in recruitment exams is considered seriously by the states of India and are trying to curb such practices. Recently, the states of Telangana, Haryana and Rajasthan Public Service Commission have taken initiative to curb impersonation issues by implementing the practice of fingerprint recording. The Himachal Pradesh state Public Service Commission provided a copy of OMR answer sheet to the candidates after completing the exam to ensure transparency. While the idea of a candidate taking a copy of answer paper (Web-3) has gained support from candidates, there are also many who strongly object as they encourage poorly performed candidates to involve in malpractices. Further, they institute frivolous complaints and make baseless allegations (Web-4) which delay the entire examination process.

Many states also employed distributed video surveillance systems for monitoring the conduction of exams. Though the mounting of surveillance cameras is cheap, availability of human resources to constantly observe the output is expensive. Further, captured video data is currently used only as a forensic tool, thus losing its primary benefit as an active, real-time medium. Hence, a real time vigilance system is needed for continuous monitoring of surveillance video to alert security officers when a suspicious activity is in progress and while there is still time to prevent the crime.

Sabbah et al. (2012) presented an automated model based on multi-biometric and video matching for continuous authentication of examinees using keystroke dynamics and fingerprints and utilizes a combination of automatic video matching and continuous. This model aims to achieve minimum cheating in e-assessment only. Ko et al. (2004) used a Webcam to prevent cheating by randomly transmitting pictures of students during exams. However, several soundless pictures of a student do not show what that student is doing or chatting. Apampa et al. (2010) proposed a blob based object tracking algorithm which uses the geometric statistics of binary images to detect, verify and classify a student's presence throughout the test session for the likelihood of abnormal activities. Bella et al. (2014) presented WATA IV, a protocol that meets several exam security requirements even when an exam manager is malicious. However, this protocol cannot detect or avoid cheating of the candidates during testing is an interesting topic for a future research after the recent system fraud scandals.

This paper explores transparency and accountability issues related to impersonation, copying, connivance, use of prohibited material, modification of answer scripts etc., and propose an automatic system for alarming the officials about the notified abnormalities. The vigilance system does not eliminate completely the use of a human invigilator but automates the monitoring of the imperfection of examinees and invigilators during the exam without the need for continuous monitoring by a person

sitting in front of surveillance monitor and reduce the strain of officials observing multiple frames per screen. Though the proposed system is costly, it is robust and helps bolster public trust, and resolves the nightmare of the candidates and authorities conducting the exam. Further, the government should take measures: to select a well qualified and active structural body, reduce overall unemployment, take strict action and quick disposal of cases against any kind of malpractice, enhance security and surveillance, prefer online exams where ever possible, adopt election commission like approach in recruiting invigilators and valuators from a different district, and work towards the long-term psychological measure such as public behavioural change, political accountable system etc.,

3. Proposed method

Typically, an entrance test consists of at least four phases: Registration, conduction of exam, evaluation and announcement of results. In the proposed system the candidate has to register for the exam in person at any AADHAR (Web-5) card issue office. The applicant along with personal details writes his AADHAR card number in the application. The official first checks if the candidate is eligible for the exam and if so, collect and enters the candidates personal details along with AADHAR number in a computer which is networked with the AADHAR database. If the personal details (i.e., name, surname, enrolment number and email address) match with the database, the official collects the fingerprint and signature of the candidate and check if they match with the existing AADHAR database. If everything matches, official collecting the application creates an identifier for each new applicant. The official then takes photo of the candidate and uploads it to computer, where it is resized into a standard size and transformed into a binary image using half tone techniques. The computer then generates two random expanded binary images (A and B) from half tone image using the concept of (2, 2) visual cryptography (Noar et al.). The image A is printed on the hall ticket along with time stamp, identifier and personal details and is issued to the candidate. The other image B, along with the original photo is stored in the board database for further authentication and impersonation check during exams. Since the original photo is not available on the hall ticket, the candidates cannot manipulate the authorities by changing photos during exam. To ensure that the right candidates are writing the exam, finger prints of candidates are collected by hand held devices during the exam and also at subsequent stages, and are matched online with AADHAR database. A multi biometric system designed to integrate fingerprint, signature, and video modalities using heterogeneous feature concatenation can improve the recognition accuracy. Registration of AADHAR number of invigilators, evaluators and board officials involved in exam, and verification of their multi-biometrics at various stages of recruitment process solves issues related to antecedents and nepotism.

RF detectors and surveillance cameras are installed in exam centres to instil vigilance and minimize impersonation and copying. A centralized intelligent real time vigilance system with a centrally operated (Valera et al. 2005) control room has an ability to recognise objects, faces, humans, describe their actions and interactions from the data acquired by hi-tech cameras which are networked and installed in the authorized registration, exam, collection, evaluation centres and strong rooms. This system performs real time monitoring of moving and static objects, automatic interpretation of exam hall scenes, understand it, and predict the actions of people in the exam hall such as interactions with others, copying from others papers, use of prohibited material, exchanging places, exchange of answer scripts etc. Multiple high end algorithms capable of processing high resolution video streams in real time, automatic learning of scene variability and patterns of behaviour analysis are employed for anomaly detection on the spot. Algorithms based on compressive theory (Web-6) are preferred as they are effective in providing high stability even under illumination changes, pose variation, abrupt motion, rotation and background clutter. They have low computational complexity and are best suitable for real time tracking. The main components of the intelligent algorithms are: multiple moving and static object detection (Zhao et al. 2007), recognition

and localization (Anand et al. 2012), object counting (Conte et al. 2010), object tracking (Yun et al. 2015), object classification with online update, human behavioural analysis (Nguyen et al. 2003) and alarming by sending SMS, mails, popup messages to officials. Further, captured video data is also stored for future investigations, and scrutiny and accountability of officials, invigilators and evaluators.

The goal of OMR security is that an examinee must be ensured that their answer paper is not modified and that the intended marks are included in the final tally. The issue of getting the candidate's trust about the integrity of OMR (Sumit et al. 2014) answer sheet is resolved by a method that provides candidates, a coded version of OMR answer sheet receipt that reflects their answer paper but does not reveal it to anyone else. A Digital Recording Equipment (DRE) such as the ones used for electronic voting (David 2004) is used in each exam hall to record, process and transfer OMR sheets and the related data to a central location through a secure online channel. DRE machines first scan the OMR sheet, convert it to a binary image, and generate two binary images (namely shares) from the binary OMR image using the concept of *(2, 2)* Visual Cryptography. Only one part of the OMR sheet where the actual answer marking is done is encoded, and appear noisy. The other part where the student details appear in the OMR sheet remains unchanged (usually the top portion). One of these shares is called candidate share, is Quick response (QR) coded and is printed on the hall ticket of the candidate. The other share called official share and the original scanned OMR answer sheet is saved in the database of the authorised board that is conducting the exam. The OMR answer sheet can be decoded only after release of answer key by the commission to help candidates cross check their answers. If a candidate wants a copy of his answer sheet he can enter the scanned QR code printed on his hall ticket in the official website provided for that purpose. The QR code is decoded to obtain the candidate share. The original OMR answer sheet is retrieved by performing logical XOR operation on the candidate and official share, followed by reduction operation. This system improves the security of OMR sheets as they are scanned and communicated to the official database immediately after exam and hence helps in curbing the malpractices which occur during transport and storage of answer papers. Further, storing papers on electronic media requires much less physical space, and the data can be easily retrieved for forensic purposes in case of issues. Another advantage is that as the OMR sheets are readily available, the counting process can be done at any time.

4. Conclusion

In order to avoid detrimental effects in the future, a fair examination process is essential to discourage any form of nepotism or favouritism. Studies show that the malpractices have thrived in examinations primarily because of lack of transparency and accountability mechanism. An AADHAR integrated biometric authentication method along with an automated centralized video surveillance system is presented as a solution to curb a variety of malpractices in general entrance tests. The system monitors, stores and uses advanced image processing techniques to interpret the scene in real time, understand and predicts the actions of the static and dynamic objects in specific environments such as exam halls for situations of interest and alert the officials accordingly. Real time implementation of image processing techniques on high resolution video streams collected from networked surveillance cameras is used for face identification and anomaly detection on the spot. Since the coded version of OMR answer sheet is issued to the candidates, instead of an exact copy of answer sheet, this system maintains confidentiality of exams. Further, it avoids unnecessary delays in the exam process due to doubts and disputes by candidates. Employing digital measures at every stage of examination process and integration to AADHAR database, from application form submission to result declaration ensures maximum vigilance on officials and candidates in the proposed system.

References

Anand, S.J. (2012). The state-of-the-art in visual object tracking. " Informatica". Vol. 36, pp. 227-248.

Apampa, K.M, Gary Wills, David Argles. (2010). Towards a blob-based presence verification system in Summative E-assessments. "Proc. of the International Computer Assisted Assessment Conference Research into E-Assessment", Southampton, UK, July 20-21.

Asakpa, S.O., Alese, B. K., Adewale, O.S., Adetunmbi, A.O. (2014). Secure face authentication using visual cryptography, Conf. Proc. 25th National conference on Knowledge based economy, Vol.25, 99, pp. 61-66.

Bella G., Rosario Giustolisi, and Gabriele Lenzini. (2014). Secure exams despite malicious management. "Proc. of Twelfth Annual Conference on Privacy, Security and Trust (PST)", pp.274-281.

Conte, D., Foggia, P., Percannella, G., Tufano,F., M. Vento. (2010). A method for counting people in crowded Scenes. "Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance". pp. 225-232.

David Chaum. (2004). Secret-ballot receipts: True voter-verifiable elections. "IEEE Security and Privacy", Vol. 2, No. 1, pp.38–47.

Ko, C.C., Cheng, C.D. (2004). Secure internet examination system based on video monitoring, "Internet research", Vol.14., No. 1, pp. 48-61.

Naor, M., Shamir, A. (1995), Visual cryptography. "Advances in cryptology –Eurocrypt '94. Lecture Notes in Computer Science", Springer-Verlag, Berlin, Vol. 950.pp.1-12.

Nguyen, N.T., Bui, H.H., Venkatesh, S., and West, G. (2003), Recognising and monitoring high-level behaviour in complex spatial environments. "IEEE Int. Conf. on Computer Vision and Pattern Recognition", Wisconsin, pp. 1–6

Sabbah, Yousef W., Imane A. Saroit, and Amira M. Kotb. (2012). A smart approach for bimodal biometric authentication in home-exams (SABBAH Model). "Biometrics and Bioinformatics", 4.1, 32-45.

Sumit Tiwari, Sandeep Sahu. (2014). A novel approach for the detection of OMR sheet tampering using encrypted QR code. "IEEE International Conference on Computational Intelligence and Computing Research", Coimbatore, pp.1-5.

Valera M, Velastin S.A. (2005). Intelligent distributed surveillance systems: a review. "IEE Proc.-Vis. Image Signal Processing", Vol. 152, No. 2, pp. 192-204.

Yun Gao, Hao Zhou, Xuejie Zhang. (2015). Enhanced fast compressive tracking based on adaptive measurement matrix. "IET Computer Vision",Vol. 9, No. 6, pp. 857–863.

Zhao T, Nevatia R, Wu. (2007). Segmentation and tracking of multiple humans in crowded environment. "IEEE Transactions on Pattern Analysis and Machine Intelligence", Vol.30, No. 7, pp. 1198-1211.

Web sites:

Web-1:https://en.wikipedia.org/wiki/Vyapam_scam.htm consulted 23 Nov. 2015.
Web-2:http://www.insightsonindia.com/2015/09/14/3-in-recent-years-corruption-and-malpractices-in-job-recruitment-exams-conducted-by-state-public-service-commissions-are-on-the-rise-in-your-opinion-what-measures-need-to-be-taken-by-these-commissi.htm consulted 23 Nov. 2015
Web-3:http://career99.com/another-initiative-by-tspsc-towards-transparency-in-recruitment-process/ consulted 23 Nov. 2015.
Web-4:http://mrunal.org/2013/07/rti-upsc-explains-why-it-cant-release-the-answerkey-before-entire-examination-process-is-over.html consulted 23 Nov. 2015.
Web-5:http://aadharcarduid.com/ consulted 23 Nov. 2015.
Web-6:http://www4.comp.polyu.edu.hk/~cslzhang/CT/CT.htm consulted 23 Nov. 2015.