Paper Presentation: Protection on Exam Paper Leakage Using Biometric

DR.Siddappa M[1],Prajwal T.G[2],Rohit Raj M[3],Sevanth T.P[4],Jeevan N.S[5]

[1]Professor,Dept of CSE, Sri Siddhartha Institute of Technology, Tumkur

[2,3,4,5] Students, Dept. of CSE, Sri Siddhartha Institute of Technology, Tumkur

ABSTRACT

Examination paper leakage poses a serious threat to the integrity and fairness of academic evaluations. This paper presents a secure and innovative solution to prevent exam paper leakage using biometric authentication technology. The proposed system ensures that only authorized personnel can access, handle, and distribute exam papers by integrating biometric verification methods such as fingerprint or iris recognition. By replacing traditional manual or password-based access systems, biometrics provide a higher level of security, minimizing the risks of unauthorized access or identity fraud. Additionally, the system can maintain detailed logs of access attempts, further enhancing transparency and traceability. This approach not only strengthens the confidentiality of examination processes but also builds trust in academic institutions by upholding the sanctity of examinations. The implementation of biometric-based security in exam paper handling marks a significant step forward in modernizing and safeguarding educational assessments.

Keywords: Biometric authentication, exam paper security, fingerprint recognition, iris recognition, data protection, academic integrity, paper leakage prevention, secure examination system, access control, identity verification.

I. INTRODUCTION

The integrity of examinations is a growing concern in today's educational environment due to increasing instances of question paper leaks and unauthorized access to confidential academic materials. Traditional security mechanisms, such as locked cabinets, sealed envelopes, password-protected files, and encrypted emails, have proven inadequate and are vulnerable to sharing, hacking, misplacement, theft, human error, or manipulation. This highlights the urgent need for advanced, tamper-proof, and intelligent systems to ensure secure and traceable access to sensitive documents like question papers.

II. METHODS AND MATERIAL

A. System Overview

The proposed system integrates biometric authentication to control and monitor access to examination papers. The main goal is to ensure that only authorized personnel can retrieve, store, or distribute the papers during the entire exam process.

B. Biometric Authentication

Biometric methods such as **fingerprint recognition** or **iris scanning** are implemented using secure biometric modules. Each authorized user is pre-registered into the system database. During any attempt to access exam papers, the user must pass biometric verification.

C. Hardware Components

- **Biometric Scanner**: For capturing fingerprint or iris data.
- **Microcontroller (e.g., Arduino/Raspberry Pi)**: Controls the access mechanism.
- **Secure Locking System**: Electronically locks/unlocks exam storage based on authentication.
- **Power Supply Unit**: Ensures stable power to the components.
- **Display/LED Indicators**: Shows system status (Access granted/denied).

D. Software Components

- **Authentication Software**: Matches biometric input with stored templates.
- **Database System**: Stores authorized user data and access logs.
- **Interface Program**: Controls the interaction between hardware and software modules.

E. Process Flow

1. Admin registers biometric details of authorized staff.
2. At the time of paper handling, the staff must authenticate using their fingerprint/iris.
3. Upon successful authentication, access is granted, and the event is logged.
4. Unauthorized attempts are denied and logged with alerts.

F. Security Measures

- Encrypted storage of biometric data
- Timestamp logging of every access
- Real-time alerts on failed access attempts

- Multi-level verification if required

III. RESULTS AND DISCUSSION

A. System performance

The developed biometric-based security system was deployed and tested in simulated real-world conditions. The primary objective was to evaluate its performance in controlling access to confidential examination papers. The system functioned reliably across multiple test sessions involving different users. It consistently allowed access to registered and authenticated individuals while denying access to unauthorized persons. This ensured that the integrity of the examination material was maintained at all times. The system handled concurrent operations efficiently and showed no signs of lag or performance degradation. This proves its suitability for use in academic institutions where examination security is a critical concern.

B. Accuracy and reliability

The fingerprint biometric module used in the system was tested for both false acceptance rate (FAR) and false rejection rate (FRR). It achieved an average accuracy of over 95%, with a FAR of less than 2% and a FRR of about 3%, which is acceptable for academic security systems. Moreover, the system's ability to log every successful and unsuccessful attempt added an extra layer of accountability. These logs included timestamped records of user ID, access status (granted or denied), and location. This made it easy to trace any irregularities or attempts to breach the system, thus increasing institutional trust in the process.

C. Security enhancements

The introduction of biometric verification drastically improved the security of examination materials compared to conventional systems. Traditional password-based methods are vulnerable to social engineering, sharing, or theft. However, biometric traits are unique and cannot be easily duplicated. The system also encrypted stored biometric templates using a secure hashing algorithm, ensuring that even in case of a breach, the raw biometric data remained protected. Furthermore, multi-level authentication—using both biometrics and a unique user ID—was implemented to strengthen access control. This dual-layer verification minimizes internal threats as well as external intrusions.

D. User experience

One of the key strengths of the proposed system was its ease of use. The interface was designed keeping in mind the academic environment where staff might not be highly tech-savvy. Users were able to complete the authentication process within 2 to 3 seconds on average, ensuring fast and efficient access. Visual cues such as green and red LEDs, along with on-screen messages, helped guide the user through each step of the process. The feedback from test users indicated high levels of satisfaction in terms of convenience, response time, and perceived security.

E. Limitations and future enhancements

While the system performed well overall, some limitations were noted. Environmental factors such as wet fingers, smudged sensors, or damaged fingerprint patterns sometimes led to recognition issues. To overcome this, future versions can implement multi-modal biometric systems, combining fingerprint recognition with facial or iris scanning. This would increase accuracy under variable conditions. Furthermore, integrating cloud-based storage and remote monitoring would allow centralized control in multi-campus institutions. The addition of features like SMS/email alerts on unauthorized attempts, mobile app integration, and AI-based anomaly detection could further enhance the system’s effectiveness and scalability.

IV. CONCLUSION

In this paper, a biometric-based security system was proposed and implemented to prevent the leakage of examination papers. The use of fingerprint authentication provided a reliable and secure method to ensure that only authorized personnel could access sensitive examination content. The system demonstrated high accuracy, quick response time, and strong resistance against unauthorized access compared to traditional methods such as passwords or manual handling. Logging and encryption further enhanced the security and traceability of access events.

Although a few limitations were observed, such as issues with wet or damaged fingerprints, the system showed significant potential for improving examination security in educational institutions. Future improvements, including the integration of multi-modal biometrics and cloud-based monitoring, could further increase the robustness and scalability of the solution. Overall, the proposed system offers a practical and efficient approach to protecting examination materials and maintaining the integrity of academic evaluations.

V. REFERENCES

[1] A. R. Sharma, *"Biometric Security Systems in Education"*, in *Security in Digital Academic Environments*, 2nd ed. New Delhi, India: TechEdu Press, 2021.

[2] R. Kumar and S. Mehta. 2020. *International Journal of Scientific Research in Science, Engineering and Technology*. (Apr 2020), ISSN NO: 2394-4099. DOI:10.32628/IJSRSET2002257

[3] M. J. Thomas and R. Gupta. 2019. *International Journal of Computer Applications Technology and Research*. (Dec 2019), ISSN NO: 2319-8656. DOI:10.7753/IJCATR0901.1003

[4] P. Singh, *"Securing Examination Systems Using Biometrics,"* in *Advances in Educational Technology and Security*, 1st ed. Mumbai, India: Academic Scholar Publishing, 2020.

[5] N. Desai and A. K. Rao. 2021. *Journal of Education Technology and Society*. (Sept 2021), ISSN NO: 1436-4522. DOI:10.21745/JETS.091253