ISSN: 2454-1907

International Journal of Engineering Technologies and Management Research
November 2020, Vol 7(11), 69 – 76
DOI: https://doi.org/10.29121/ijetmr.v7.i11.2020.819

FINGERPRINT EMPLOYEE CLOCKING SYSTEM FOR UNIVERSITIES

Debrah Joshua Osei [1], Alfred Elolo Konglo [2], Mohammed Issah Adinkrah [1], Lord Anertei Tetteh [3], Kojo Boakye [1], Abigail Mba [1], Victoria Quansah [4]

[1] Department of Computer Science and Informatics, the University of Energy and Natural Resources, Sunyani-Ghana

[2] IT Directorate, Ho Technical University, Ghana

[3] Department of Electrical and Telecommunication engineering, Koforidua Technical University, Ghana

[4] Department of Education, Catholic University College, Fiapre-Ghana

DOI: https://doi.org/10.29121/ijetmr.v7.i11.2020.819

Article Citation: Debrah Joshua Osei, Alfred Elolo Konglo, Mohammed Issah Adinkrah, Lord Anertei Tetteh, Kojo Boakye, Abigail Mba, and Victoria Quansah. (2020). FINGERPRINT EMPLOYEE CLOCKING SYSTEM FOR UNIVERSITIES. International Journal of Engineering Technologies and Management Research, 7(11), 69-76. https://doi.org/10.29121/ijetmr.v7.i11.2020.819

Published Date: 30 November 2020

Keywords:
Fingerprint
Biometric Data
Employee Attendance
Employee Clocking System
Truancy of Employees

ABSTRACT

A system that is used for time-clocking, creating an all-inclusive electronic record of the process involved in how employees logs in and out of work on working days are referred to as a clocking system. The system has an additional feature of calculating an accurate payroll system, which in turn, can lead to a precise amount the company spent on labour. In essence, an employee clocking system is a process of monitoring the attendance, presence and truancy of employees in a work environment. In this project, the University of Energy and Natural Resources was used as a case study. The existing method of recording the presence of staff to work is by a manual process where employees record their attendance on a paper. The challenge of the current employee attendance system is the difficulty in tracing old records, safekeeping, lack of confidentiality and the chances of other employees logging in for their truant colleagues. This paper sought to introduce a biometric employee clocking system to help overcome the high level of truancy in workplaces. The results of the experiment we conducted indicate a high accuracy in our system with TAR value of 99.7%. This accuracy rate is much better than the results other researchers obtained. The excellent accuracy implies that employees will have difficulty to check-in or out for their truant colleagues. The high accuracy results will help improved security of attendance, improved employee performance, ensures fast and easy retrieval of data, easy monitoring of staff, and prevent impersonation in the attendance logs.

1. INTRODUCTION

Employee Clocking System (ECS) is an electronic process of monitoring the attendance in the work environment to minimize economic, time, productivity and loss revenue due to employee absenteeism, lateness and truancy. Attendance monitoring and evaluation have been done conventionally using employee attendance books (the manual way of taking employee attendance). However, attendance monitoring and evaluation goes beyond only attendance, but it ensures efficient time utilization which maximizes and motivates employee attendance. Employee Clocking System is the best modern techniques of monitoring of employees' attendance. Employee Clocking System

is useful for attendance tracking, annual leave management, check truancy, calculation of overtime and transmission of data on salary to the payroll system [1].

The current employee attendance framework or system, requires the workers to physically log the attendance sheet each time they go to their workplace, and when they close [2]. Regularly, such a framework needs mechanization since it is not an electronic framework and might produce various issues. These issues may incorporate the time superfluously devoured by the worker to discover and sign their names in the attendance book and the way that attendance book may get lost or avoided employees because of suspected wrong exercises. The turn of events and execution of this framework will assist Universities to deal with their workers' information critically. The framework has an information base that contains worker's data, and it will help the administrator to control information and update the data set [2], [3].

In today's business transactions, it is always expected that the clients authenticate themselves for services rendered to them with authentication control mechanisms [4]. Identification and access control mechanism plays a vital role in ensuring a protected and safe Employee Clocking System deployment. To make the identification and access control mechanism safe and reliable for authentication, the Employee Clocking Systems must have integrated biometric data as an added feature. The advancement of technology towards digitization era is being accelerated globally to meet the evolving digital and smart system development[5],[6].

2. LITERATURE REVIEW

In biometric attendance systems, according to [7],[8],[9], employees attendance are collect electronically with using biometric fingerprint system to capture the fingerprint of employees before and after work. These collected fingerprints records are then saved for subsequent operations analysis. Authors of [10],[11],argued vehemently that, biometric systems are an authentication method. As suggested in [7],[12],[13], biometric systems identify people by using a recognition mechanism of physical characteristics. This verification and authorization technique has gained universal recognition as the best way of providing authentication. According to literature, fingerprints biometric is known to be the most convenient form of biometric identification since the technology is secure to use and easily accessible for use [11],[12],. Therefore, this study is concerned with the implementation of a biometric fingerprint authentication system which is an automated technique used to match and verify the similarity of some physical characteristics of persons who seek to gain access or entry to a system. Employee clocking system adopts fingerprint biometric and identification technique as an advanced automated system to collect fingerprint data, analyze and then use it to compute the attendance of employees [13],[14],[15],. The captured data is also used for the computation of daily and monthly attendance of employees in order to reduce human errors in the data capturing and processing stages. This paper present a high level analysis of captured biometric fingerprint data which provides the best accuracy in performance. Our system was designed and tested in a selected University campus in curbing the problems of ghost names (people whose names are on the payroll and receiving pay, yet are not delivering any services to the institution), the lateness of workers to their various posts, impersonation by colleague workers and truancy in any institution[17],[18].

2.1. COMPUTERIZED BIOMETRIC EMPLOYEE CLOCKING SYSTEM AND OPERATIONAL PERFORMANCE

When electronic biometric employee clocking systems are being planned, it is imperative to guarantee that physiological and social highlights are contemplated [16]. A definitive presentation of the biometric framework will rely upon how well the physiological and conduct highlights were considered in the biometric system plan. The highlights that should be considered incorporate the uniqueness of individual users, performance, acknowledgement, and hardness of the biometric system and its levels of satisfaction[13]. Biometrics systems help in powerful attendance management which helps in expanding employees or workers' efficiency and produce time and overhead cost reserve funds to upgrade the organization' performance by using the mechanized time the management system to track worker time spent at work and attendance [8],[13]. Attendance timing management helps in controlling our techniques for managing working hours. The moves that are taken to improve proficiency depended on the rule of time management [7],[19].

3. METHODOLOGY

The research was localized at the UENR campus, as a case study. A web application was designed and installed on three computers. Each computer had a fingerprint scanner device attached to the computer to receive or reject fingerprints images. In this study, 1000 participants (population) were selected for the fingerprint experiment. The participants included students, teaching and non-teaching staff. The design phase of the employee clocking system integrated the biometric fingerprint scanner to a web application[20],[21]. The web application is a common platform for all the fingerprint devices which connect to a single database[22],[23]. It involved dividing the whole system into modules and defining the relationship among the constituent modules. This process of dividing the system into modules is repeated until each module is sufficiently small enough to be conveniently coded as an independent entity that performs a clearly defined operation.

3.1. THE POPULATION OF THE STUDY

A total population of 1,000 employees and students at UENR were selected randomly to participate in the biometric fingerprint experiment. The distribution of the population has been represented in table 1.

Table 1: Population distribution

Participants	Male	Female	Total
Students	380	120	500
Teaching staff	145	55	200
Non-teaching staff	250	50	300

3.1.1. SAMPLING PROCEDURE AND SAMPLE SIZE

The sampling process has been divided into two phases. The first phase randomly selected 500 students. The system is envisaged to be used in the classroom to monitor students' class attendance. The second phase was a careful selection of teaching and non-teaching staff. In all these phases, the availability of the participants for the experiment was taken into consideration. Table 1 represents the sample size for the research. The sample size has been calculated through Slovin's formula [17] by using a confidence level of 85%.

$$n = \frac{N}{1+Ne^2}$$

In the Slovin's formula, ***N*** is the total population, ***e*** is the error of tolerance, and ***n*** is the sample size. The total population consists of 7,200 participants selected from the University. With the help of Slovin's formula, 1,000 sample size has been calculated to conform to the population segmentation with a response rate of 98%.

3.1.2. RESEARCH DESIGN AND ANALYSIS

The study has been designed to improve employee attendance at the universities and other related organizations. The employee clocking system comprises of a database, web application [20] and the finger. The fingerprint's Software Development Kit (SDK) we used to design the web application, and the database [22] includes JavaScript, PHP, MySQL and C#. The analysis of the result was done by using SPSS software and M.S. Excel and visual studio. The system [24],[25] consists of the developed attendance software installed on an HP 630 Laptop and the fingerprint scanner. Three computers were used to test the system. The three computers were labelled as System 1, System 2 and System 3.

3.2. FLOWCHART OF THE EMPLOYEE CLOCKING SYSTEM

Figure 1 shows the visual representation of the sequence of steps and decisions adopt to perform the technical processes involved in the ECS development. Each step in the sequence is clearly indicated within a diagram which have connecting lines and directional arrows that link each step to another step. This allows readers to view the logical flow of the process from the beginning to the end. The presented ECS flowchart is a robust algorithm with adequate construction design which communicates the steps in the ECS processes very effectively and efficiently.

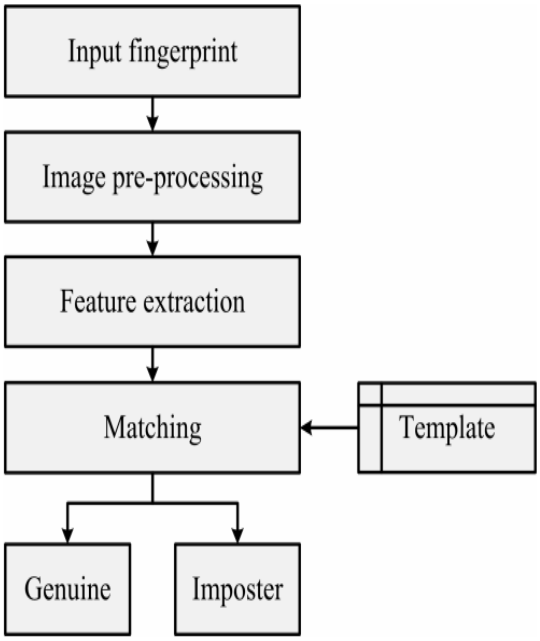

Figure 1: research framework of the employee clocking system

3.3. PERFORMANCE EVALUATION METRICS OF ECS

One of the fundamental variables in the achievement of a biometric system is its exactness and accuracy in performance. The system performance is a measure of how well the system can accurately map the biometric data from the same individual and try not to erroneously check biometric data from various individuals. The estimation of biometric exactness is normally communicated as a percentage of the experimental resulted [24],[25]. This paper used both percentage and proportion in its performance assessment as defined as follows:

False rejection rate (FRR): The proportion of employees who are incorrectly denied by the biometric system. If the system allows a single attempt, then the false rejection rate is given by:

$$FRR(\tau) = FTA + FNMR(\tau) * (1 - FTA) \quad (1)$$

False acceptation rate (FAR): The proportion of impostors who are accepted by the biometric system. If the system allows a single attempt, the false acceptance rate is given by:

$$FAR(\tau) = FMR(\tau) * (1 - FTA) \quad (2)$$

False-negative identification-error rate (FNIR.): The proportion of employees enrolled in the system in which the employees' correct fingerprint is not among those returned. For an identification process consisting of one attempt against a database of size N, it is defined as:

$$FNIR(\tau) = FTA + (1 - FTA) * FNMR(\tau) \quad (3)$$

False-positive identification-error rate (FPIR.): The proportion of identification process by employees who are not enrolled in the system, where an identifier is returned. For an identification process consisting of one attempt against a database of size N, it is defined as:

$$FPIR = (1 - FTA) * (1 - (1 + FMR)^{N}) \quad (4)$$

4. RESULTS AND DISCUSSION

The three systems were connected to the same database, which simultaneously checks the fingerprint images with those in the databases. The testing of the system was done three weeks after the employee enrollment was done. The test ensured the all the participants had their biodata tested with the data stored in the database. After four days of testing, we realized that some of the participants had difficulty with the authentication process. To measure this anomaly, we used the four-performance evaluation matrix to determine the accuracy of the test. The four performance evaluation metrics used to test the results includes True Acceptance Rate (TAR), False Acceptance Rate (FAR), True Rejection Rate (TRR) and False Rejection Rate (FRR).

Other parameters, such as receiver operating characteristics and Cumulative match characteristic, were represented graphically to determine the performance of the system, which directly ensure that we achieve the objectives of this work. An illustration of a ROC curve has been presented in Figure 2.

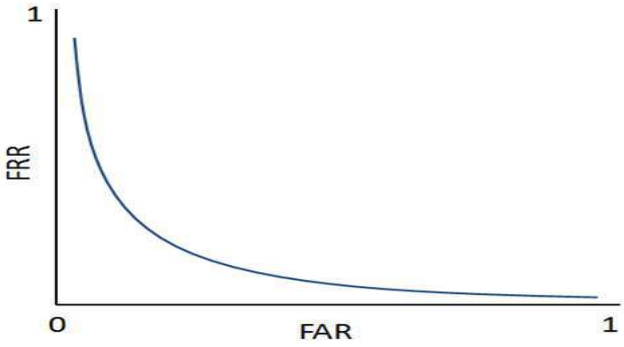

Figure 2: ROC for FAR against FRR

Cumulative match characteristic curve (CMC): this is the graphical representation of results of the identification test, plotting rank values on the x-axis and the probability of correct identification at or below that rank on the y-axis. The CMC curves have been given in Figure 3.

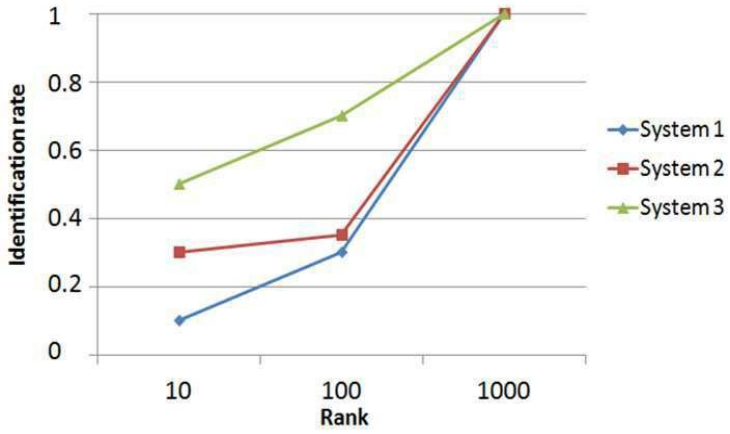

Figure 3: CMC Curves of the three systems.

The study found a few errors (0.5% to 1.5%) caused by filing fingerprints with the wrong personal information than it found false acceptances by the biometric system. It also found a strong relationship between the quality of the fingerprint images stored at enrollment and the accuracy during verification comparisons.

Table 2: Performance Evaluation Matrics

Device	FMR	FTE	TMR	FTA
System 1	0.088	0.079	0.02	0.09
System 2	0.082	0.071	0.02	0.09
System 3	0.089	0.079	0.02	0.09

The best images had TAR=98% at FAR=0.01%, while the worse images had TAR=47% at FAR=0.01%. Finally, this study also showed the value of combining two fingerprints at verification time. When this was done, the accuracy increased to TAR=99.7% when FAR=0.01%, as indicated in table 2, table 3 and table 4.

Table 3: Identification System Performance Metrics

Device	FNIR	FPIR	FNMR	IR
System 1	0.0012	0.001	0.0016	0.0012
System 2	0.0016	0.001	0.0016	0.0012
System 3	0.0022	0.001	0.0016	0.0012

Overall, fingerprint matching accuracy suggests that the performance was quite good with high-quality fingerprint images. Caution was appropriate; however, because the results were from a real-world experiment, the actual accuracy much better than the results obtained by [11],[13],[18]

Table 4: Verification System Performance Metrics

Device	FRR	FAR	EER	TRR	TAR
System 1	0.001	0.01	0.021	0.098	0.097
System 2	0.001	0.01	0.021	0.098	0.099
System 3	0.001	0.01	0.021	0.099	0.099

5. CONCLUSION

The truancy of employees has affected the productivity of many organizations. This situation has resulted in the loss of revenue, among many other adverse effects. This paper sought to introduce a biometric employee clocking system to help overcome the high level of truancy in workplaces. The results of the experiment we conducted indicate a high accuracy in our system with T.A.R. value of 99.7%. This accuracy rate is much better than the results other researchers obtained. The implication of the good accuracy is that employees will have difficulty to check-in or out for their truant colleagues. The high accuracy results will help improved security of attendance, improved employee performance, ensures fast and easy retrieval of data, easy monitoring of staff, and prevent impersonation in the attendance logs. The automated process, with the aid of fingerprint biometrics, does not give room for impersonation. Once an employee has been enrolled, it cannot be verified by another person.

SOURCES OF FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENT

The authors are grateful to the authorities their final project supervisor whose efforts, proofreading and critique helped to improve the quality of this paper.

REFERENCES

[1] Abhilash K. Sharma, (2015). Biometric System – A Review. International Journal of Computer Science and Information Technologies, September, 2015.
[2] Acuity Market Intelligence (2008). Biometrics: high-value workforce management: The critical role of biometric time and attendance to workforce management solutions, White Paper, February 2018.
[3] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1179–1192, Jul. 2017.
[4] Tan, T. N., & Lee, H. (2019). High-secure fingerprint authentication system using ring-LWE cryptography. IEEE Access, 7, 23379-23387.
[5] Pang, S., Jinchun, Y. E., Xu, H., & Li, H. (2019). U.S. Patent No. 10,496,804. Washington, DC: U.S. Patent and Trademark Office.
[6] Harikrishnan, D., Sunil Kumar, N., Joseph, S., & Nair, K. K. (2019). Towards a fast and secure fingerprint authentication system based on a novel encoding scheme. The International Journal of Electrical Engineering & Education, 0020720919883803.
[7] Liu, F., Zhao, Q., & Zhang, D. (2020). 3D Fingerprint Authentication. In Advanced Fingerprint Recognition: From 3D Shape to Ridge Detail (pp. 33-57). Springer, Singapore.
[8] Adewole K., Adbulsalam S., Babatunde R., Shittu T. & Olotede M. (2014). Development of finger biometric attendance system for non-academic staff in a tertiary institution. Computer Engineering and Intelligent Systems Review, 5, 2.
[9] Akinduyite C.O, Adetunmbi A.O, Olabode O.O. & Ibidunmoye E.O, (2013) Fingerprint-based attendance management system. Journal of Computer Sciences and Applications, 2013, 1(5), 100-105
[10] Cupido, (2011). The implementation of a time and attendance system at Stellenbosch Municipality – a change management perspective masters project in public administration. University of Stellenbosch.
[11] Danny Thakkar (2019). Biometric System, Biometrics Comparison – biometrics performance metrics can help you select the right biometric solution
[12] Dermatoglyphics.org. (2017). 11 Basic Patterns of Fingerprint. [online] Available at: http://dermatoglyphics.org/11 Basic Patterns of Fingerprint / [Accessed 17 July. 2017].
[13] Krishna Prasad, K. and Aithal, P. S. (2017). A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques. International Journal of Applied Engineering and Management Letters.
[14] Krishna Prasad, K. and Aithal, P. S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. International Journal of Management, Technology and Social Sciences (I.J.M.T.S.), 2(2), 8.19. DOI: https://dx.doi.org/10.5281/zenodo.835608
[15] Kuntal Barua, Samayita Bhattacharya, Kalyani Mali (2015). Fingerprint Identification, April,2015.
[16] Karani, K. P., Aithal, P. S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. International Journal of Applied Engineering and Management Letters (I.J.A.E.M.L.) ,1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678
[17] Obansola O. Yemi, Makinde O. Ezekiel, Adeshina A. Henry & Adebayo O. Bunmi (2016) Development of Staff Attendance Management System Using Fingerprint Biometric Identification Technique, November, 2016.
[18] Omobayo, A. (2015). Optimization of bimodal biometrics system for access control authentication in Kenya, School of Computing, College of Science, Engineering and technology, University of South Africa.
[19] Ononiwu G. C.& Okorafor, G. N (2012). Radio frequency identification-based attendance system with automatic door unit. Academic Research International, 2(2), March, 2012.

[20] Appiah, V., Nti, I. K., & Nyarko-Boateng, O. (2017). Investigating Websites and Web Application Vulnerabilities: Web master's Perspective. International Journal of Applied Information Systems (I.J.A.I.S.) – ISSN: 2249-0868 Foundation of Computer Science F.C.S., New York, U.S.A. Volume 12 – No. 3, June 2017. I.J.A.I.S. Publications.

[21] Vincent Appiah, Michael Asante, Isaac Kofi Nti and Owusu Nyarko-Boateng (2018). Survey of Websites and Web Application Security Threats Using Vulnerability Assessment. Journal of Computer Science 2018. Science Publication. 2019, 15 (10): 1341.1354. DOI: 10.3844/jcssp.2019.1341.1354.

[22] Nyarko-Boateng, O., Asante, M., & Nti, I. K. (2017). Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization. International Journal of Science and Engineering Applications, volume 6 Issue 3, 2017. p88-94. ISSN-2319-7560. I.J.S.E.R. Publications

[23] Owusu Nyarko-Boateng, Benjamin A. Weyori and Lord Anertei Tetteh (2020). Optimized Authentication Model for Online Transaction Payments. Science publications- Journal of Computer Science. Volume 16, Issue 2. Pages 225-234. DOI: 10.3844/jcssp.2020.225.234

[24] Owusu Nyarko-Boateng, Alfred Kuranchie and Justice Anning (2017). The Relevance of E-Library Facility to the Delivery of Education at the High School: An Example from Ghana. International Journal of Scientific & Engineering Research. Vol 8, Issue 5, p 910-918. ISSN 2229-5518. I.J.S.E.R. Publications.

[25] Nyarko-Boateng, O., & Adekoya, A. F. (2019). Evaluation and analysis of key performance indicators which affect the QoS of mobile call traffic. International Journal of Computer Networks (I.J.C.N.), 9 (1), 14-30