Anchor University Journal of Science and Technology (AUJST)
A publication of the Faculty of Natural, Applied and Health Science, Anchor University Lagos
URL: journal.aul.edu.ng
In AJOL: https://www.ajol.info/index.php/aujst
Vol. 5 No 1, August 2024, Pp. 14-21
ISSN: 2736-0059 (Print); 2736-0067 (Online)

Multimodal Biometric Identification System Based EEG (Electroencephalograph) and Fingerprint with Template Protection

[1]Nadamau, Mohammed Shehu, [2]Kabiru I. Musa, [3]Shehu I. Galoji
[1]Abubakar Tafawa Balewa University
[2]Abubakar Tafawa Balewa University
[3]Bauchi State University Gadau
***Corresponding author Email**: msnadamau@gmail.com
Submitted 11 November, 2023
Accepted 12 December, 2023
Competing Interests.
The authors declare no competing interests.

ABSTRACT

This research presents a multimodal biometric system that integrates EEG and fingerprint data using deep learning convolutional neural networks. The system addresses the limitations of unimodal biometric systems and enhances template security by implementing a fuzzy vault scheme. The system extracts frequency weighted power (WFP) features from EEG data and minutiae from fingerprints, combines them, and uses the combined features along with a secret key to create a database in the vault. Experimental results demonstrate that the proposed system outperforms other methods, achieving an Equal Error Rate (EER) of 0.25% for EEG, 0.20% for fingerprint, and 0.10% for multimodal unlike Liwen, (2010) with an Equal Error Rate (EER of 1.12%). The fuzzy vault biometric system also performed exceptionally well, achieving perfect accuracy (EER of 0.00) in differentiating between genuine and impostor samples, with a perfect ROC AUC value of 1.00 Unlike Suputra and Sukarno, (2019) with False Rejection Rate (FRR) of 8.9475% and False Rejection Rate (FAR) of 0.3520% equivalent to an Equal Error Rate (EER Of 0.045). The t-test analysis confirms that the difference in scores is statistically significant, providing further evidence of the system's robust performance. Overall, these results suggest that the fuzzy vault implementation is performing exceptionally well in terms of security and accuracy. This study is significant because it proposes a new method for fusion normalization of EEG brain signal and fingerprint with template protection scheme using fuzzy vault to provide better accuracy and high template protection. The feature work should use large data set for both the EEG and Fingerprint and also should use another model for classifier based score normalization.

Keywords: Biometric, Unimodal, Multimodal, Convolutional Neural Network, Fuzzy vault

1. INTRODUCTION

Biometric security has turned into a significant concern in the realm of data security (Rejasecar et al., 2022). A reliable system for identifying users is essential for many purposes, such as using sensitive personal data, making online bank transfers, interacting on social media platforms, operating mobile devices, and entering premises. Many people use password-based security systems to protect themselves from intruders, but these systems are vulnerable to different kinds of attacks. To improve security, multifactor authentication, which uses two, three or more factors of security based on what you have or who you are, has been used. However, token-based systems have problems, as they can be easily lost or stolen. Therefore, we need a better solution that is not easy to forget, lose, steal, guess, or copy. Biometrics offers a good solution to these problems (Raiz, et al, 2017). Biometric systems rely on physical features such as EEG, irises, fingerprints, or veins, or behavioral traits such as handwriting, voice, or typing rhythm to verify a person's identity. Fingerprint identification is the most common biometric technology (Kanjan et al., 2017) and is widely used in various domains, such as mobile device authentication. Biometric identification systems have gained popularity due to their potential to enhance data security. However, unimodal biometric systems, such as those relying solely on fingerprint or electroencephalograph (EEG), are faced with inherent challenges of low accuracy and privacy concerns.

https://dx.doi.org/10.4314/aujst.v5i1.2

Modak & Jha, (2019) reviewed the multi-biometric fusion strategy and its application and obviously clarify why additional research is required to get solution to the stated problems found in diverse biometric systems, and also the shortcomings of a variety of fusion methods. While there have been various research efforts on unimodal, multimodal and biometric template protection schemes, previous studies have highlighted certain limitations. For instance, the fusions of conventional fingerprint with EEG at the matching score level, as proposed by (Liwen, 2010).Some multimodal biometrics introduces challenges in the normalization process, leading to potential reductions in recognition rates and overall system performance (Modak & Jha, 2019).Moreover, existing studies, such as the work by Monsy and Vinod (2020), have introduced novel features for EEG-based biometrics, but the overall performance and efficiency of such features in a multimodal system have not been thoroughly explored. Additionally, although combining EEG biometric features with conventional biomet-rics, as suggested by Ling Chan et al. (2018), shows promise in compensating for weaknesses, there is still the need to address the overall robustness and security of the proposed multimodal system. Furthermore, while advancements in biometric security systems have been promising, the increasing attempts of attacks on these systems pose ongoing challenges. This necessitates the use of strong security measures, such as key binding schemes like the fuzzy vault proposed by by Albermany and Baqer (2020). However, the application of these schemes in multimodal biometric systems with fingerprint and EEG components requires careful consideration of factors such as uniqueness, intra-class variation, noisy data, and system performance.

Over the years, studies have done on the use of the EEG or the fingerprint as a biometric identification in unimodal biometric systems. The research employs EEG or fingerprint as a biometric identification is described in the sections that follow

According to Ling Chan et al., (2018), a hybrid approach of EEG biometrics and conventional biometrics can overcome the limitations of both methods. Fingerprint and facial recognition are preferable to traditional biometric techniques because they are more stable, widely used, and inexpensive.

Liwen (2010), a new system for personal identification using two biometric modalities was developed, which had excellent anti-spoofing and identification abilities. The system used both the fingerprint, a traditional biometric modality, and the Electroencephalogram (EEG), a new one, for the first time. The system combined these two modalities at the score level. The system performed better than the systems that used either of these modalities alone. However, the score level fusion required extra time for normalization, which could affect the system's performance and recognition rate (Modak & Jha, 2019).

According to Monsy and Vinod (2020), they proposed a novel feature called Frequency-weighted power (FWP) for EEG-based biometric identification, which can distinguish individuals better than the existing EEG features. They tested their method on resting-state EEG data from both the physioNet database and 16 subjects in their lab. They achieved an equal error rate (EER) of 0.0039 with a correlation-based classifier using 20 electrodes from eyes-closed resting-state EEG signals, which is almost five times lower than the best EER reported in the literature for the same number of electrodes. They also compared their FWP feature with the AR coefficients, which are a common parametric way of estimating the PSD of a signal. They found that the FWP feature performed better than the power feature and the AR coefficients in all frequency bands except 0.5 HZ in terms of EER. However, they also acknowledged some drawbacks of their study. One is that the score level fusion technique they used requires a lot of computation time for normalization

https://dx.doi.org/10.4314/aujst.v5i1.2

method can affect the recognition rate and the system performance (Modak & Jha, 2019). Another is that the small sample size and the lack of consideration of factors such as age, gender, and other variables that may affect the EEG signals may limit the validity and reliability of their results.

Gui et al. (2019) conducted a survey on brain biometrics, which have some unique features and benefits compared to conventional biometrics. This has led to more attention in this area. The feasibility of a biometric for authentication or identification depends on seven criteria: universality, uniqueness, permanence, collectability, performance, acceptance and circumvention. Recent research has shown that brain biometrics are resistant to spoofing and circumvention in terms of signal generation and collection. To overcome the limitations of both methods, ling Chan et al.(2018) suggested combining EEG biometric characteristic with traditional biometrics. EEG, facial and fingerprint IDs are good choices for conventional biometrics because they are efficient, stable, popular, and affordable.

According to Kanjan et al., (2017), fingerprint is a biometric authentication method that is secure and private. Fingerprints are considered to be unique for each person and each finger of the same person. Even indistinguishable twins with similar DNA have different fingerprints. However, fingerprints are not secret or confidential to the owner. They can be easily compromised by spoofing attacks (Gui et al., 2019).

Muntaheen and shaker's summary of quantitative comparative study of various physiological and behavioral biometric techniques that can be applied on mobile banking was published in Shaker and Muntaheen (2021). Analysis methods employed include those based on originality, uniqueness, universality, permanence, circumvention, performance, collectability and acceptability. According to the data, fingerprint recognition is the most accurate of the six biometric methods that were utilized to make the comparison. Muntaheen and Shaker(2021) did a thorough analysis of a number of physiological and behavioral biometric techniques, but unlike Gui et al. (2019), the neglected to emerging biometrics like EEG and ECG, which are crucial to any proposed research based on biometric trade.

By suggesting a model based on deep learning techniques, Bidgoly et al.,(2022) seek to solve the drawbacks of EEG-based authentication, including, including lack of universality, lack of privacy preservation, and ease of use. The distinctive benefits of EEG-based authentication, such as its resistant to spoofing attack and the presence of both physiological and behavioral traits, have been successfully emphasized by the authors. The paper does not, however, compare it to other EEG-based authentication models or biometric authentication techniques that are already in use. Additionally, it ignores the time needed for user authentication, which can be a crucial aspect to take into account for real-world applications.

The fuzzy vault's locking and unlocking algorithms, as well as the concept of the fuzzy vault, were first introduced by Juels and Sudan in 2002. A fuzzy vault scheme-based EEG authentication system was proposed by Albermany and Baqer (2020). The suggested approach investigates the feasibility of achieving authentication by fusing encryption and biometrics. Using the tent chaff points gives the system an advantage since it decreases the error that occurs when separating chaff points from the genuine point, which are the EEG signal features, because the initial seeds are known by both sender and receiver. The classification has a good accuracy of 96%. Although the proposed system offered security, the unimodal biometric-based system had a number of inherent issues, including lack of uniqueness, intra-class variation, non-universality, noisy

https://dx.doi.org/10.4314/aujst.v5i1.2

noisy data (dust on the sensor), a limited degree of freedom, an unacceptable error rate, and failure-to-enroll (Modak & Jha, 2019).

Saputra and Sukarno (2019) offered an improvement to the fuzzy vault approach in fingerprinting. The minutiae filter and candidate point's identification algorithms are two adaptations to the distance-based biometric method that are offered. The new approach produced FAR 0.3520% and %. a FRR 8.9475% while the previous method produced FAR 0.4515% and FRR 13.4375.

The proposed multimodal biometric system by Kaur and Sofat (2017) comprises a Fuzzy Vault template protection strategy with steps for encoding and decoding. Two window sizes, w1 with a value of 1 and w2 with a value of 5, are used to examine the performance of the proposed system utilizing various metrics such as FAR, FRR, and ROC with polynomial degrees ranging from 8 to 14.

Using a Score Level Fusion Approach, Joshi and Kuma (2020) designed a multimodal biometric system. It has been suggested to use a new efficient normalization. These normalized scores have been combined using a method based on the weighted sum rule. The combined experimental findings of four biometric modalities are presented. The study significantly reduced mistake rates using the proposed score level fusion technique implementation. With a multimodal system, the study were able to accomplish some intriguing work with FAR=0% and FRR=1.66%. The majority of score level fusion systems have been designed with the assumption that all scores from matching modules are available, but it is possible for certain scores to be absent.

To overcome the limitations of existing research and propose a robust solution, this study developed a multimodal biometric identification system that combines fingerprint and EEG modalities with template protection. The system used various normalization techniques, feature extraction methods, classifiers, and the work of Saputra and Sukarno (2019) on improving accuracy of fuzzy vault schemes based on distance-based methods for template protection schemes. By addressing the challenges associated with unimodal systems and building upon the strengths of existing research, this study provides an effective and reliable multimodal biometric authentication system for enhanced data security and user identification. The aim of this study is to propose a multimodal biometric identification system based on EEG brain signals and fingerprints with template protection using fuzzy vault. The specific objectives are: To propose a multimodal biometric identification system with a better error equal rate (EER) after fusion, and to evaluate the performance of the system using various metrics including accuracy, and t-test.

Material and Methods

In this study, a novel multimodal biometric system is developed, combining the Electroencephalograph (EEG) brain signal with the fingerprint modality using deep learning Convolutional Neural Network technique with template protection using fuzzy vault. The EEG signal was processed with a time-frequency feature extraction using the Frequency Weighted Power (FWP) algorithm in various frequency bands, and for the fingerprint modality, a novel approach for minutiae-based algorithms features used, and the convolutional neural network Model (CNN) Classifier-based score fusion algorithm is utilized for match score level fusion.

The study develop a multimodal biometric identification system based on EEG and fingerprint with template protection using the fuzzy vault, the study start by combining the two biometric modalities into a single feature vector using convolutional neural network model.

https://dx.doi.org/10.4314/aujst.v5i1.2

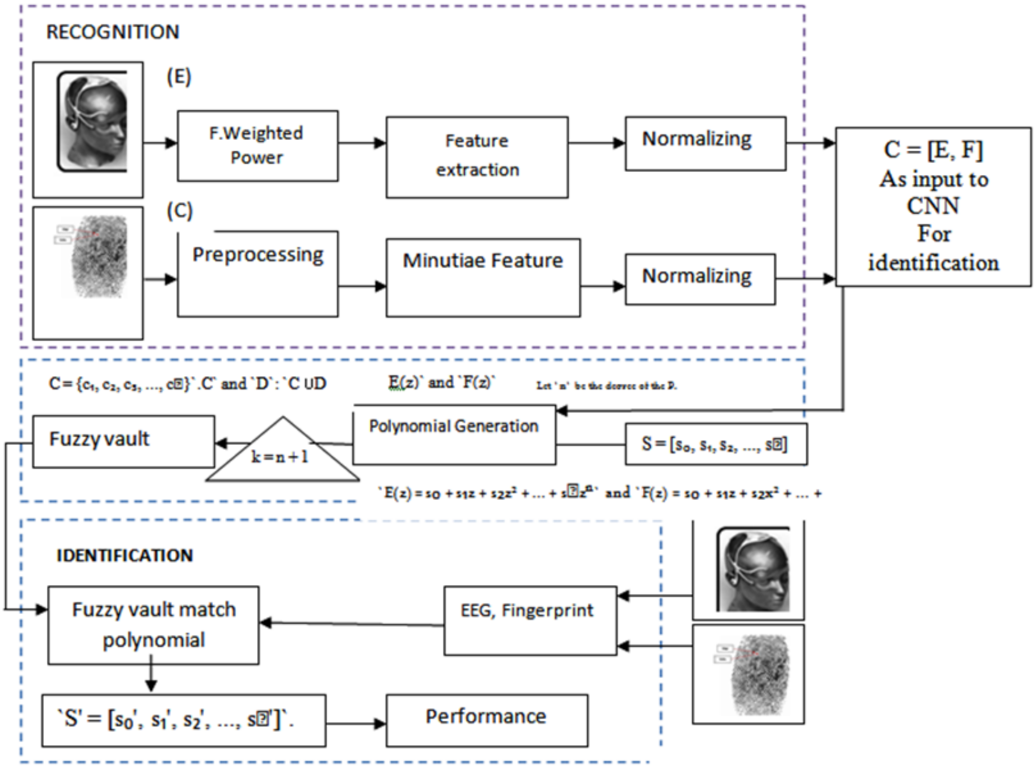

Figure 1. Novel multimodal biometric system

The study denotes the EEG features as vector E and the fingerprint features as vector F. The study can concatenates these two vectors to get a combined feature vector C:

C = [E, F], then the study used the combined feature vector as input to the CNN for Identification.

Next, the study utilized the fuzzy vault scheme to protect the templates. The fuzzy vault scheme is a cryptographic technique that allows secure storage and matching of biometric templates while maintaining their privacy. The following are the steps: Feature Extraction: Extract the relevant features from the combined feature vector C.

The following steps are the mathematical algorithms for the fuzzy vault scheme.

1. Rising the degree of the polynomial to get better security: Let `n` be the degree of the polynomial, and let `k` be the number of coefficients in the secret key. Then, by increasing `n`, we can increase `k`, which can improve the safety of the fuzzy vault implementation. Mathematically, this be able to be represented as: `k = n + 1`.

2. Locking algorithm: The locking algorithm can be represented mathematically as follows:

- Let `S` be the secret key, where `$S = [s_0, s_1, s_2, ..., s_n]$`.

- Let `E` and `F` be the numerical representations of the EEG and fingerprint data, respectively.

- Let `E(z)` and `F(z)` be the polynomial equations representing the EEG and fingerprint data, respectively.

- Then, `$E(z) = s_0 + s_1z + s_2z^2 + ... + s_nz^n$` and `$F(z) = s_0 + s_1z + s_2z^2 + ... + s_nz^n$`.

- The resulting encrypted polynomial equations, representing the locked data, are stored securely. The locking algorithms will use a polynomial of degree 14 to encrypt the secret key using the EEG and fingerprint data. This means that the secret key will have 15 coefficients and the polynomial equation will

https://dx.doi.org/10.4314/aujst.v5i1.2

use a polynomial of degree 14 to encrypt the secret key using the EEG and fingerprint data. This means that the secret key will have 15 coefficients and the polynomial equation will have form

Then, the polynomial equations are `$E(z) = 3 + 5z + 7z^2 + ... + 53z^{14}$` and `$F(z) = 3 + 5z + 7z^2 + ... + 53z^{14}$`.

- The values of `z` that satisfy the polynomial equations are the same as the EEG and fingerprint data, i.e., `$E(2) = F(2) = E(4) = F(4) = ... = E(32) = F(32)$`.

- The locking algorithm will then generate a set of points `(z, y)` that are either on the polynomial curve or randomly chosen from the finite field.

- The locking algorithm chooses some points from the polynomial curve that correspond to the biometric data, and some points that do not correspond to the biometric data. These points are called genuine points and chaff points, respectively. The genuine points and chaff points are mixed together to form the fuzzy vault, which can be stored or transmitted securely.

3. The unlocking algorithm uses Lagrange interpolation to find the coefficients of the polynomial from the points. Lagrange interpolation is a way of finding a polynomial function that passes through a given set of points. The locking algorithms have 15 points, the unlocking algorithms use Lagrange interpolation to find a polynomial of degree 14 that fits the points. The unlocking algorithm will then output the secret key if it matches the original one.

- Unlocking algorithm: The unlocking algorithm can be represented mathematically as follows:

- Let `S'` be the retrieved secret key, where `$S' = [s_0', s_1', s_2', ..., s_n']$`.

- Let `E'(x)` and `F'(x)` be the decrypted polynomial equations representing the unlocked EEG and fingerprint data, respectively.

- Then, `$E'(z) = s_0' + s_1'z + s_2'z^2 + ... + s_n'z^n$` and `$F'(z) = s_0' + s_1'z + s_2'z^2 + ... + s_n'z^n$`.

The lagrange equation for the statement is:

$$P(z) = \sum_{i=0}^{14} y_i \ell_i(z)$$

where y_i are the values of the polynomial at the points (z_i, y_i), $\ell i(z)$ are the Lagrange basis polynomials defined as:

$$\ell(z) = \prod_{j=0, j \neq i}^{14} \frac{z - zj}{zi - zj}$$

This equation can be used to reconstruct the polynomial equation that binds the secret key and the biometric data in the fuzzy vault scheme. By using Lagrange interpolation, the unlocking algorithm can find the coefficients of the polynomial from a subset of points that are close enough to the original biometric data. The unlocking algorithm will then output the secret key if it matches the original one.

Dataset Description: The performance of the proposed approach will evaluate using publicly available benchmark datasets. The following points will describe the datasets for the proposed multimodal approach.

1.The study used public available EEG dataset comprises 28 participants; with sampling frequency of 250HZ using the standard 10-20 montage with 19 channels: Fp1, Fp2, F7, F3, FZ, F4, F8, T3, C3, CZ, C4, T4, T5, P3, Pz, P4, T6, O1, O2.

2. The study used FVC2004 the Fourth International Competition on Biometric Authentication, which specifically emphasizes fingerprint verification algorithms and systems. It consists of 80 fingerprint samples and was organized to foster advancements in fingerprint of 28

person so as to be the same with of EEG which also 28. The Experiment Setup, Simulation will conduct on windows pc with 4GB ram and 500GB of hard disk, using Google Colab python. The choice of performance metrics for are accuracy, false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER)

Results and discussion

In this part, the experiment was divided into two parts: experimental scenario 1 and 2. The first experimental scenario was conducted to compare the EER of unimodal biometric identification system and Multimodal biometric identification system of the proposed thesis. The second experimental scenario was conducted to measure the performance of fuzzy of vault on proposed multimodal biometric identification system compare to the EER of the previous method Suputra and sukarno,(2019).

Experimental Scenario 1.

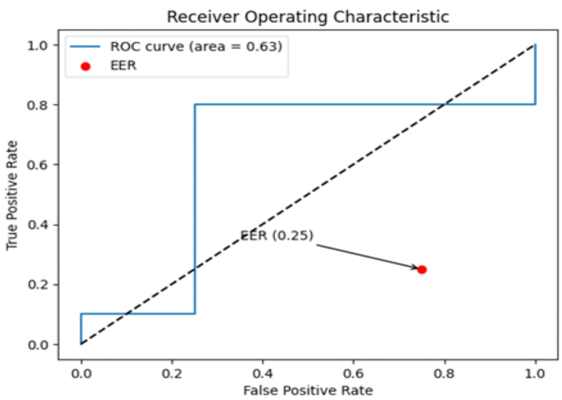

Figure1: Fingerprint Unimodal Biometric

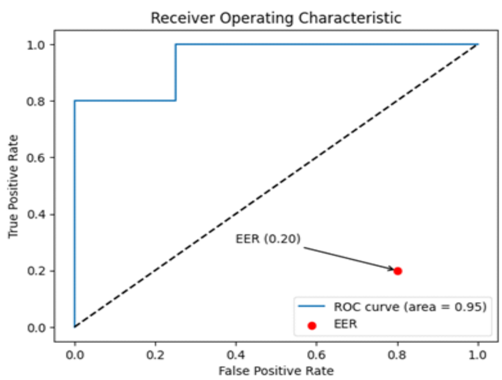

Figure 2:EEG Unimodal Biometric

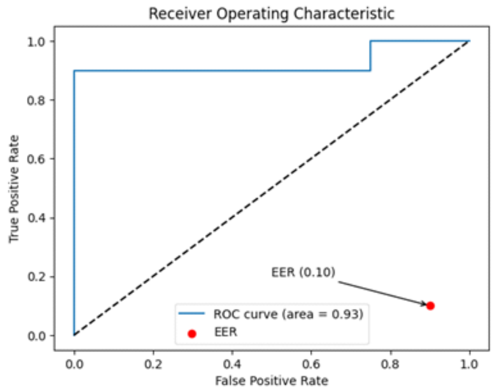

Figure3: Multimodal Biometric Identification

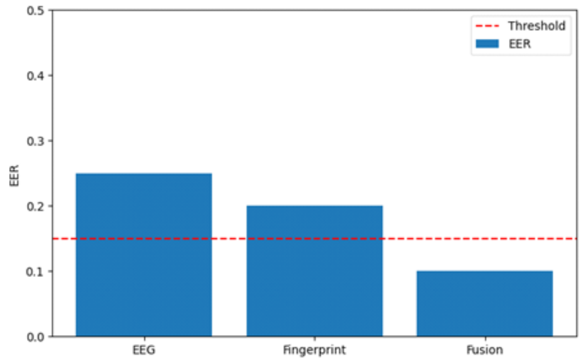

Figure 4: Comparison between unimodal EEG, Fingerprint and Multimodal fusion

In general, a higher value for the area under the ROC curve indicates superior performance, as it reflects the system's capability to distinguish between genuine and impostor matches at various threshold levels. As a result, the fingerprint unimodal system demonstrates the highest area under the ROC curve (0.95), indicating better discriminative power compared to the EEG unimodal system (0.63). The EER (Equal Error Rate) is the point on the ROC curve where the false acceptance rate (FAR) equals the false rejection rate (FRR). A lower EER signifies better performance, as it implies a more optimal balance between accepting genuine matches and rejecting impostor matches. In this scenario, the fusion of the two modalities achieves the lowest EER (0.10), representing the best trade-off between FAR and FRR Overall, based on the provided results, the combination of the EEG and Fingerprint modalities exhibits the best performance with a high area under the ROC curve (0.93) and a low

https://dx.doi.org/10.4314/aujst.v5i1.2

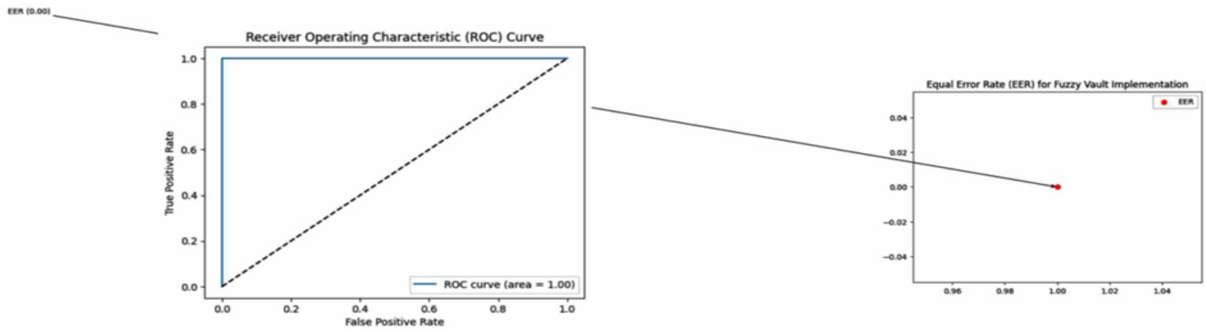

Figure 5: ROC for Fuzzy Vault Implementation

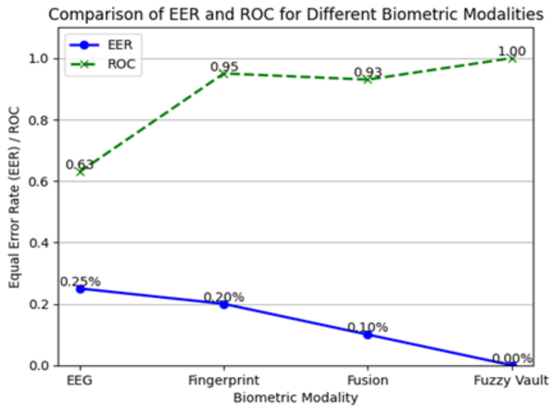

Figure 6: ROC and EER for different Modalities

Experimental scenario 2:

The results of the experiment show that the fusion of EEG and Fingerprint modalities exhibits the best performance with a high area under the ROC curve (0.93) and a low EER (0.10).unlike of Liwen, (2010) with (EER of 1.12%). The fuzzy vault biometric system also performed exceptionally well, achieving perfect accuracy (EER of 0.00) in distinguishing between genuine and impostor samples, with a flawless ROC AUC value of 1.00. unlike Suputra and sukarno (2019) with FFR of 8.9475% and FFR of 0.3520% which is equivalent to (EER Of 0.045)The t-test analysis confirms that the difference in scores is statistically significant, providing further evidence of the system's robust performance. Overall, these results suggest that the fuzzy vault implementation is performing exceptionally well in terms of security and accuracy.

Conclusion

The aim of this research is to propose a multimodal biometric identification system based on EEG and fingerprint with template protection using fuzzy vault. This study presents a multimodal biometric identification system that combines fingerprint and EEG modalities to enhance accuracy, security, and efficiency. The system incorporates various normalization techniques, feature extraction methods, classifiers, and template protection schemes. The best performance was achieved when the two modalities were combined, resulting in an ROC curve area of 0.93 and an EER of 0.10%. Additionally, the fuzzy vault biometric system performed exceptionally well, achieving perfect accuracy (EER of 0.00) in distinguishing between genuine and impostor samples. Therefore, the study from the results suggest that the fuzzy vault implementation is performing exceptionally well in terms of security and accuracy and it is also important for developers of biometric authentication devices.

REFERENCES

Atighehchi, K., Ghammam, L., Barbier, M.,

https://dx.doi.org/10.4314/aujst.v5i1.2

& Rosenberger, C.(2019). Grayc-Hashing: Combining biometrics and secret for enhancing the security of protected templates. Future Generation Computer Systems 101,819–830.

Albermany S., and Baqer F.M, (2021): EEG authentication system using fuzzy vault scheme, Journal of Discrete Mathematical Sciences and Cryptography, DOI: 10.1080/09720529.2020.1859798.

Bidgoly, J.A., Bidgoly, J.H, and Arezoumand, Z.(2022). Towards a universal and privacy preserving EEG-based authentication system. Scientific reports.

Gui Q., Ruiz-blondet M. V., Laszlo, S. and Jin Z. (2019). A Survey on Brain Bio metrics. *ACMComput. Surv. 51, 6, Article 112, 38 pages.*

Gui, Q. Jin, Z., Ruiz B. M., Laszlo., S. & Xu, W. (2015) Towards EEG Biometrics: Pattern identical twin fingerprints. *Pattern Recognition*, 35(11):2653–2663.

Habibu, T. Talina, E Anael, L., Sam E. (2019). Developing an Algorithm for Securing the Biometric Data Template in the Database. *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 10, 2019.*

Joshi S. and Kumar A.(2020): Multimodal Biometrics System Design using Score Level Fusion Approach, *International Journal on Emerging Technologies* 11 (3): 1005-1014.

Jules, A. & Sudan. M. (2002) A fuzzy vault scheme. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, page 408.

Kanjan, N., Patil, K., Ranaware S., & Sarokte P.(2017). A Comparative Study of Fingerprint Matching Algorithms.Volume: *International Research Journal of Engineering and Technology*

Kaur M and Sofat S. (2020): Fuzzy Vault template protection for Multimodal Biometric System. *IEEE International Conference on Computing, Communication and Automation*

Liwen, F., Anni Cai X. (2010) A Dual-Biometric-Modality Identification System Based on Fingerprint and EEG. *IEEE*

Modak S.k and Jha V.K (2018): Multibiometric Fusion strategy and its Applications: A Review, doi:https://doi.org/10.1016/j.inffus.2018.11.018.

Monsy C., Vinod A.p (2020):EEG-based biometric identification using frequency-weighted power feature.IET Journal, Vol. 9 Iss. 6, pp. 251-258

Muntaheen ASM., Shaker MA., (2021). Biometric Authentication in Mobile Banking. *Am J Comput Sci Eng Surv Vol. 9 No. 1:18.*

Rajasekar V., Predic B, Saracevic M., Elhoseny M., Karabasevic D., Stanujkic D and Jayapaul P. (2022).Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. https://doi.org/10.1038/s41598-021-04652-3. *Recognition. Chapter 1.4, pages 8–11. Springer, New York, second edition.*

Riaz, N., Riaz, A., & Ali Khan, S. (2017) .Biometric template security: an overview. Sensor Review, https://doi.org/10.1108/SR-07-2017-0131.

Saputra J. and Sukarno, (2019): Improving the Accuracy of Fuzzy Vault Scheme in Fingerprint Biometric, *IEEE 7th International Conference on Information and Communication Technology.*