EEG-based authentication using binary classification neural networks

Judah Cooper, Eva Blainey, Matthew Rezkalla, Quinn Spence, Mark Benhamu, Daniel Harrington, Michael Barrack, Daniel David, Ayaz Vural

4-7-2021

ABSTRACT

Brain-computer interfaces (BCI) have shown recent potential as a security tool in the field of biometric encryption. Most modern devices contain some form of biometric security such as facial recognition or fingerprint authorization however these methods have proven to be fallible. Brain data collected through electroencephalography (EEG) can be used in high-security applications to authenticate the correct user and inhibit fraudulent attempts at accessing sensitive data. The system designed in this research takes a different approach than other EEG encryption algorithms created in the past as the distributed nature of the system allows for greater scalability and security. Users of the system perform motor movements in sequence to create a unique password that trains an artificial neural network to correctly identify their specific brain patterns. The brain data collected by the EEG is distilled using independent component analysis and subsequently processed by the binary classification neural network to determine if the user will be authenticated. The machine learning algorithms are trained using the PhysioNet EEG Motor Movement/Imagery Dataset and achieve an accuracy of 100% in the task of deciphering correct brain data from invalid data provided by a different subject. The designed system can be deployed in industries such as banking and finance since the security of this algorithm is unparalleled by other forms of biometric encryption.

INTRODUCTION

The current EEG encryption techniques in modern research rely upon a centralized algorithm for authenticating input brain data [1]. These systems can perform extremely well in terms of subject identification accuracy but fall short in practical application as there are critical design flaws plaguing the security or scalability of the system. Several EEG encryption algorithms use some form of multi-class classification to predict the specific user and allow authentication if the predicted user is the correct user [2]. This system requires a single server to process all requests for authentication and the server must be updated with current user information thereby diminishing the security and scalability of the application. Since there is one server that processes all the requests, a cybercriminal could theoretically breach the server and compromise the system. Furthermore, the scalability is harmed by the fact that all new users must train their specific brain data on the same network requiring more computational resources as the number of users grows. A 2017 attempt at creating an EEG encryption algorithm used alphanumeric passwords to hash the brain data and make it easier for the machine learning model to predict the correct user [1]. The use of alphanumeric passwords undermines the nature of biometric encryption since it has no connection to biophysical data. The system designed and proposed in this paper improves upon prior limitations with the implementation of a binary classification model.

In this experiment, motor movement was chosen as the physical action to be performed and repeated to authenticate the user. The EEG BCI dataset was used to train and test the subject identification algorithm [3]. The dataset contains recordings of 109 subjects each performing various motor movement and motor imagery tasks. The individual tasks do not provide enough information for an algorithm to differentiate between users so different tasks of the same user are concatenated to increase the length of the passkey. This further enhances the security of the system since a fraudulent user would have to recreate the brain patterns of the correct user and execute them in the correct order to be authenticated. The concatenated motor movements are fed into a binary classification neural network separately trained for each specific user. The network is designed to predict if the user is authentic or fraudulent. Randomized chains of incorrect user movements are fed into the network to train the model to differentiate the correct

data. This isolated perception of the network allows for much greater scalability and security as the algorithm is purely focused on authenticating a single user. In a broader sense, each user would have their own network that is specifically trained to identify their unique neural data so that if a device is compromised, all other subject identification systems are unharmed.

METHODS

System Overview

The system starts by organizing four raw EEG recordings of a specific user performing various motor movements into an array. The first and last two recordings are concatenated to form a motor movement pair. This step makes the subsequent preprocessing step much faster while maintaining the complexity of the unique motor movement data. The concatenated raw data is then processed using independent component analysis (ICA) [4] to identify the independent brain patterns involved in each motor movement. The ICA algorithm outputs a 64 by 15 array of post-processed data. Once all the user brain data is processed with ICA, a binary feed-forward neural network uses this data to train and authenticate users. Through one hot encoding each correct user input, the binary network is trained to differentiate the correct user from incorrect users. If the neural network outputs a 1, the user is authenticated.

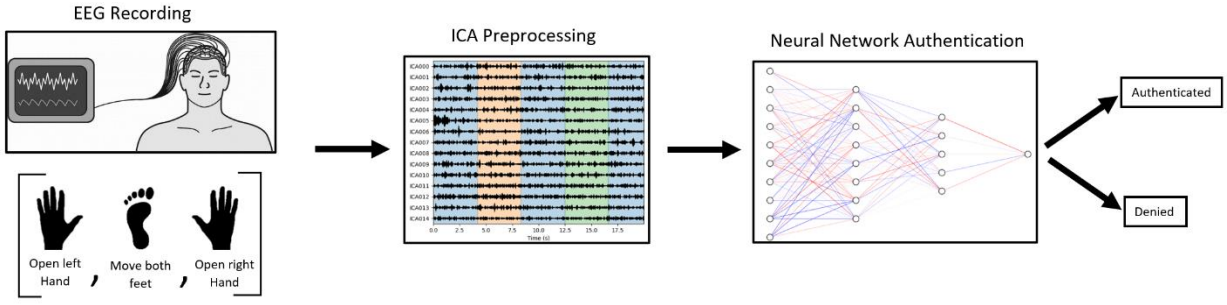

Figure 1 details the architecture of the system showing how the data flows through each step.

Data Preprocessing

The initial step in recording brain data is signal processing. MNE is the Python package used to preprocess the raw EEG data before input to the subject identification algorithm [5]. The

frequency is filtered to include 14 to 30 Hz such that the beta wave range is analyzed exclusively. Independent component analysis was used to further process the data. Fast ICA provided a reliable and efficient solution to separating the signal into subcomponents. The fifteen subcomponents represent different groupings of the electrode sensors that coordinate to describe the motor movements. This process of feature engineering increases the accuracy of the system since the data is segmented and the differences between users are much easier to identify for the subsequent neural network step. The following figure illustrates the fifteen ICA components.

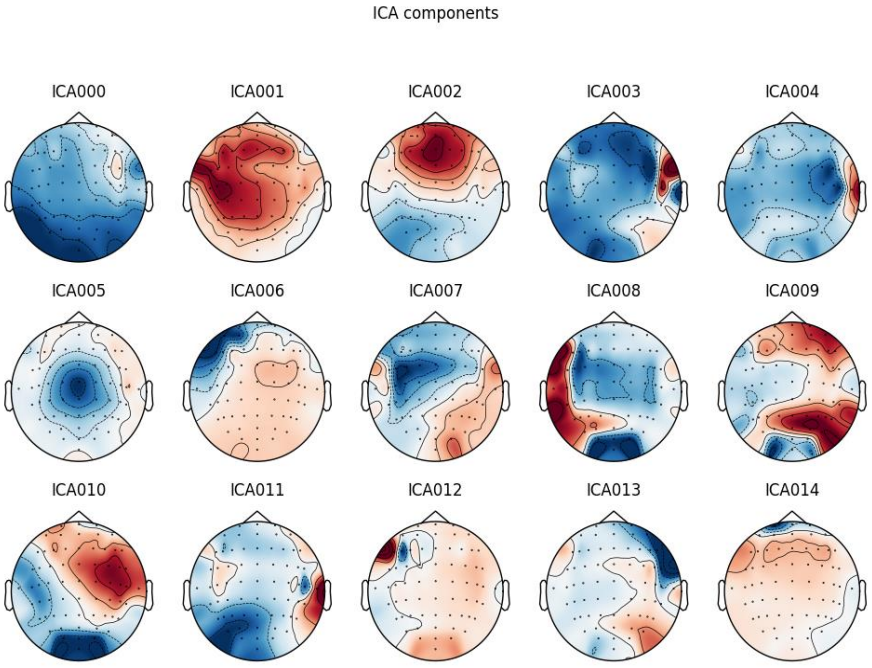

Figure 2 shows an example of the heat maps created from the ICA of one subject's EEG data. The 15 components each contain a different combination of electrodes that contribute to the component at various magnitudes.

Resampling

Since the dataset provided 14 separate recordings of each subject, new data was simulated from the original data to expose the model to more training. The dataset provides three recordings of hand movements and three recordings of feet movements per user. In this experiment, the passkey was, “open hands”, “move feet”, “open hands”. The EEG BCI dataset provides three separate recordings for each of the movements so that there is enough data for 27 correct keys per person. The data sampling technique took a random sample of 15 keys from each user all with the same order of movement but different recordings for each movement. Synthetic Minority Over Sampling Technique (SMOTE) was used to generate more data for the model to

train and test on [6]. SMOTE creates synthetic samples in the minority class which in this case is the data of the authentic user as there is one authentic user and 108 incorrect users. This resampling method was chosen because it ensures that the new data preserves the general features of the organic data but introduces an element of variability to create new samples.

User Authentication Network

The user authentication algorithm is designed with a binary classification neural network. The network takes in a 64 by 45 array that represents the three motor movements that have been concatenated after ICA preprocessing. This array is flattened and passed through the input dense layer. The network consists of an input layer with 30 nodes and two hidden layers each containing 15 and 10 nodes respectively. The output layer has one node as it will return a binary value indicating if the user has been authenticated. The input and hidden layers use the rectified linear unit activation function, and the output layer uses the sigmoid activation function. Dropout layers are used as a regularization technique to prevent overfitting. The neural network trained over 30 epochs with 70% training data and 30% test data. Binary cross entropy was chosen as the loss function as the output of the network is binary. Adam optimization was used as the optimizer since it is particularly effective with noisy inputs. The architecture of the network is illustrated below.

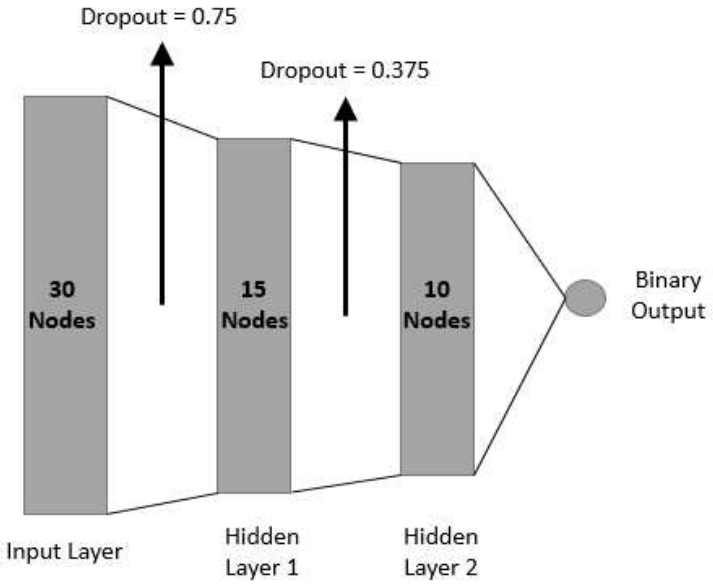

Figure 3 depicts the network architecture and each individual layer of the feed forward neural network.

RESULTS AND DISCUSSION

Training Data

The network achieved an accuracy of 99.5% on the training data which represented a random sample of 70% of the total experiment data. The loss in the model is calculated by the binary cross-entropy loss function as shown in Eq. 1 where "J" is the loss, "y" represents the target value, and "$\hat{y}$" is the model output.

$$J = -\frac{1}{N}\sum_{i=1}^{N} y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i) \quad (1)$$

The loss was reduced to 0.0168 after 30 epochs. A confusion matrix as shown in Figure 4 details the performance of the classification network on the training data.

	Correct User	Incorrect User
Network Authenticates User	1121	11
Network Denies Access to User	0	1094

Figure 4 displays the results of training the binary classification network in a confusion matrix.

Testing Results

The validation data made up 30% of the experimental data as this was used to test the performance of the network after optimization. The loss was approximately $2.63 \cdot 10^{-5}$ with an

accuracy of 100%. Figure 5 displays the results of the network on the validation dataset in a confusion matrix.

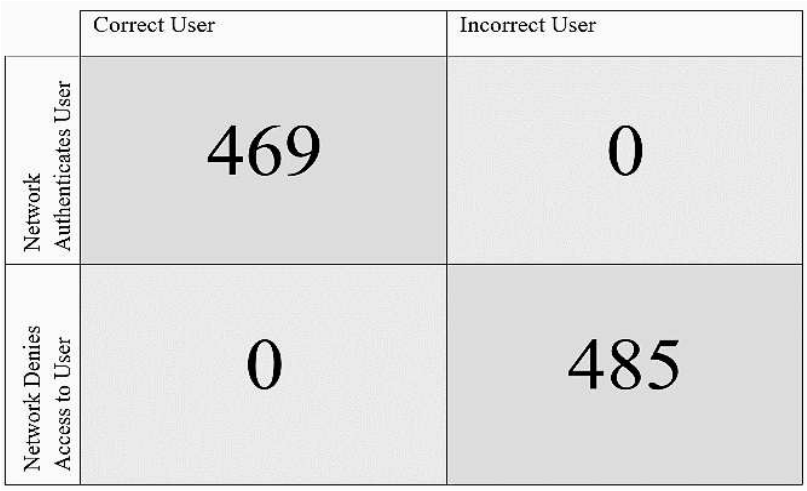

Figure 5 displays the results of testing the binary classification network in a confusion matrix.

Network Output

The classification network was able to achieve perfect accuracy on the validation test dataset with a relatively low quantity of nodes and layers due to the nature of the input data. Once the data was processed and shaped, the features in the input data are complex enough for the network to detect patterns in the correct user and separate them from the other users. A combination of the ICA processing and the three-movement passkey gives the machine learning algorithm more than enough data to separate the classes of authentic and inauthentic users. The results show that the act of moving one's feet and hands produce distinct enough brain patterns that an artificial neural network can distinguish unique users from the signals.

Security of the Algorithm

The results of the binary neural network testing show that machine learning based EEG encryption is a viable option for biometric security applications. The feasibility of EEG-based biometric authentication can only be realized when compared to other biometric encryption methods. Techniques such as fingerprint and facial recognition are widely accepted and trusted for high-security situations even though there is a risk of fallibility. The benefit of EEG-based user authentication goes beyond increased accuracy as there are other weaknesses in biometrics

that brain data help to avoid. The following table compares some of the currently used biometric encryption techniques.

Table 1 compares some of the widely accepted and used biometric encryption techniques.

Biometrics	Authors	Applied Scheme	Dataset Size	Bit
Signature	Vielhauer et al.	Quantization	10 subjects	24
Fingerprint	Nandakumar et al	Fuzzy vault	110 subjects	128
Face	Goh et al.	Biohashing	194 subjects	80
Iris	Hao et al.	Fuzzy commitment	70 subjects	140

Each technique has advantages and disadvantages, but EEG-based authentication is the most difficult to break using brute force methods due to the uniqueness of the data. Since EEG signals are incredibly complex relative to other biophysical signals, the computational cost of replicating a unique signal is extremely high. The ICA preprocessing method used in this experiment converts EEG recordings into 64 by 15 arrays containing the 64 electrodes and 15 independent components. Four separate recordings were used to authenticate a user making the resultant input a 64 by 15 by 4 array with values ranging from zero to one (3840 normalized values). Although the input EEG data does not need to be identical to the trained data for the user to be authenticated, it must be similar enough that it can be distinguished by the network as the correct user. Guessing 3840 unknown floating-point numbers within a narrow range of error is expected to be significantly more challenging than breaking the 80-bit encryption of facial recognition or the 128-bit fingerprint recognition key.

Brute force attacks are far from the only way that security systems can be compromised. Fingerprint authentication has been shown to be vulnerable to hackers that can acquire an image of the finger since a reproduction can easily be made [7]. Fingerprints can be obtained from surfaces that the user touch which can compromise the authentication process. Furthermore, simulations have been built to replicate voice and facial recognition once an attacker has enough data on the user's face or voice [8]. The key difference in brain data that protects EEG-based authentication from these types of attacks is that brain data is not easily accessible to attackers. The necessity for a full electrode EEG system to authenticate a user compounded with the

complexity of the brain signal itself makes it exceedingly difficult for an attacker to analyze and replicate a user's brain data.

Machine Learning and Encryption

The goal of the system proposed in this paper is to improve on the security, reliability, and scalability of EEG-based authentication. Most authentication systems are built upon some form of encryption standard to maximize security. The use of a neural network to authenticate users is a dynamic approach that can improve upon the traditional methods of encryption. One of the largest challenges in EEG encryption is the issue of change over time. The currently proposed EEG encryption systems have little consideration for the changes in a person's brain signal since the encryption key remains static. The neural network model is designed to update based on changes made to the training data which provides a dynamic solution to the problem of a user's brain signal change over time. The neural network authentication system proposed in this paper can work in harmony with asymmetric encryption in future applications to maintain the security and distributed nature of the system. The weights and biases can be encrypted so that the only way to gain access to the device or network is to produce the correct brain signal pattern. The experiment can be repeated with any user in the EEG BCI dataset chosen as the correct user since the neural network will automatically adjust to learn the uniqueness of that specific brain signal.

Feasibility in Live Applications

In the application of this system into a live cybersecurity platform, there are a few key aspects that might differ from the experiment. All of the input passkeys that the network gained and tested on had the same order and movements to train the system to distinguish users and not movements. However, in practical application, it is unlikely that incorrect users would know the exact motor movement order and would therefore perform the incorrect actions. This would make it much easier for the network to identify an inauthentic user input as this added layer of security would aid the success of the system. Furthermore, the experimental data was collected in a lab using a strict protocol and robust equipment. In practical applications, the data will likely be collected in various settings with different equipment which could lead to difficulties in the network's classification accuracy. The experiment provides a framework for how this would be

implemented but there will undoubtedly be adjustments made to accommodate for factors in live testing.

Use Cases

Based on the current state of the technology, EEG recording is an inconvenient task not well suited for modern consumers. Individuals looking to unlock a handheld device, or a personal email account would find the process described in this research to be unnecessarily cumbersome since biometrics such as fingerprint or facial recognition are adequate for most commonly used cybersecurity applications. EEG-based authentication is much better suited for high-security situations where the threats that undermine traditional biometric security pose a sizeable risk to the user. Industries such as banking, government, and military are just a few examples where the risk of compromised information warrants the need for higher levels of complexity in cybersecurity [9]. This is exactly where EEG-based authentication can be best implemented since the relatively costly and cumbersome task of recording motor movements with an EEG is worth the added security benefits.

CONCLUSIONS

In this paper, it is shown that machine learning techniques such as ICA and artificial neural networks work in tandem to create an authentication system based on EEG data that is both accurate and feasible. For cybersecurity applications where ease of use can be sacrificed for enhanced levels of protection, EEG-based authentication is optimal. The results of the experiment demonstrate a high degree of perception in the artificial neural network and the ability to differentiate between the motor movements of users. The benefits of resampling and preprocessing the data proved to be invaluable in enhancing the accuracy of the network. Based on the performance of the EEG authentication algorithm and the breadth of the dataset, commercial implementation of the system could lead to vast improvements in the field of biometric encryption.

REFERENCES

[1] D. Nguyen, D. Tran, D. Sharma, and W. Ma, "On The Study of EEG-based Cryptographic Key Generation," *Procedia Computer Science*, vol. 112, pp. 936–945, 2017, doi: 10.1016/j.procs.2017.08.126.

[2] Y. Liu, H. Huang, F. Xiao, R. Malekian, and W. Wang, "Classification and Recognition of Encrypted EEG Data Based on Neural Network," *Journal of Information Security and Applications*, vol. 54, p. 102567, Oct. 2020, doi: 10.1016/j.jisa.2020.102567.

[3] Schalk, G., McFarland, D.J., Hinterberger, T., Birbaumer, N., Wolpaw, J.R. BCI2000: A General-Purpose Brain-Computer Interface (BCI) System. IEEE Transactions on Biomedical Engineering 51(6):1034-1043, 2004.

[4] P. Comon, "Independent Component Analysis," in *Higher-Order Statistics*, J-L.Lacoume, Ed. Elsevier, 1992, pp. 29–38. Accessed: Dec. 14, 2021. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00346684

[5] Alexandre Gramfort, Martin Luessi, Eric Larson, Denis A. Engemann, Daniel Strohmeier, Christian Brodbeck, Roman Goj, Mainak Jas, Teon Brooks, Lauri Parkkonen, and Matti S. Hämäläinen. MEG and EEG data analysis with MNE-Python. *Frontiers in Neuroscience*, 7(267):1–13, 2013. doi:10.3389/fnins.2013.00267.

[6] A. Agrawal, H. L. Viktor, and E. Paquet, "SCUT: Multi-class imbalanced data classification using SMOTE and cluster-based undersampling," in *2015 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K)*, Nov. 2015, vol. 01, pp. 226–234.

[7] A. Adler, "Vulnerabilities in Biometric Encryption Systems," in *Audio- and Video-Based Biometric Person Authentication*, Berlin, Heidelberg, 2005, pp. 1100–1109. doi: 10.1007/11527923_114.

[8] V. L. Voydock and S. T. Kent, "Security Mechanisms in High-Level Network Protocols," *ACM Comput. Surv.*, vol. 15, no. 2, pp. 135–171, Jun. 1983, doi: 10.1145/356909.356913.

[9] C.-F. Lin and B.-S. Wang, "A 2D CHAOS-BASED VISUAL ENCRYPTION SCHEME FOR CLINICAL EEG SIGNALS," *Journal of Marine Science and Technology*, vol. 19, no. 6, Dec. 2011, doi: 10.51400/2709-6998.2209.

[10] M. N. Omar, M. Salleh, and M. Bakhtiari, "Biometric encryption to enhance confidentiality in Cloud computing," in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, Aug. 2014, pp. 45–50. doi: 10.1109/ISBAST.2014.7013092.

[11] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006, doi: 10.1109/TC.2006.138.

[12] A. Goh and D. C. L. Ngo, "Computation of Cryptographic Keys from Face Biometrics," p. 13.

[13] S. Liu, Y. Yao, C. Xing, and T. Gedeon, "Disguising Personal Identity Information in EEG Signals," *arXiv:2010.08915 [cs, eess]*, Oct. 2020, Accessed: Dec. 14, 2021. [Online]. Available: http://arxiv.org/abs/2010.08915

[14] S. Albermany and F. M. Baqer, "EEG authentication system using fuzzy vault scheme," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 0, no. 0, pp. 1–6, Mar. 2021, doi: 10.1080/09720529.2020.1859798.

[15] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007, doi: 10.1109/TIFS.2007.908165.

[16] C. Vielhauer and R. Steinmetz, “Handwriting: Feature Correlation Analysis for Biometric Hashes,” *EURASIP J. Adv. Signal Process.*, vol. 2004, no. 4, Art. no. 4, Dec. 2004, doi: 10.1155/S1110865704309248.
[17] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, “I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves,” in *Financial Cryptography and Data Security*, Berlin, Heidelberg, 2013, pp. 1–16. doi: 10.1007/978-3-642-41320-9_1.
[18] Goldberger, A., Amaral, L., Glass, L., Hausdorff, J., Ivanov, P. C., Mark, R., ... & Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. Circulation [Online]. 101 (23), pp. e215–e220.