Journal of King Saud University – Computer and Information Sciences 35 (2023) 101541

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Personal authentication and cryptographic key generation based on electroencephalographic signals

Eman A. Abdel-Ghaffar [a,*], Mohamed Daoudi [b,c]

[a] Electrical Engineering Department, Faculty of Engineering Shoubra, Benha Univ., Cairo, Egypt
[b] IMT Nord Europe, Institut Mines-Télécom, Centre for Digital Systems, F-59000 Lille, France
[c] Univ. Lille, CNRS, Centrale Lille, Institut Mines-Télécom, UMR 9189 CRIStAL, F-59000 Lille, France

ARTICLE INFO

Article history:
Received 16 December 2022
Revised 23 March 2023
Accepted 24 March 2023
Available online 5 April 2023

Keywords:
Electroencephalogram (EEG)
Biometric
Brain computer interface (BCI)
Riemannian manifold
Cryptographic key generation

ABSTRACT

Brain signals have recently been proposed as a strong biometric due to their characteristics such as, uniqueness, permanence, universality, and confidentiality. There are many factors that affect the stability of EEG signals as a biometric for example, using different recording devices, variation in participant emotional states, performing different mental tasks and recording in temporally spaced sessions. Due to the non-stationary nature of EEG signals, there are still speculations about the stability of using them for generating a unique and repeatable cryptographic key. The challenge that faces all biometric based crypto-systems is to overcome the variation in biometric itself over time and to generate multiple unique keys from the same observation. In this work, we investigate the stability of using EEG signals as a biometric for both personal authentication and cryptographic key generation. The authentication process was tested using three datasets AMIGOS, DEAP, and SEED. Achieving accuracy of 96.23%, 98.85%, and 99.89% respectively. The key generation process generates a set of different keys with different lengths from the same observation. Each key is unique and repeatable. The generated keys were examined using NIST test suite, scale index test, and autocorrelation test. Time complexity analysis of the key generation process was performed.
© 2023 The Author(s). Published by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In the last few decades brain computer interface (BCI) became a fast-growing and promising technology, which aims to allow human brain to communicate with and control external devices. BCI applications spreads across multiple and diverse fields including e-healthcare (Ke et al., 2020; Vishwanath et al., 2021; Dahmani et al., 2022; Kaushik et al., 2019), e-learning (Lin and Kao, 2018; Abu-gellban et al., 2022), marketing (Kaheh et al., 2021; Amin et al., 2020; Khurana et al., 2021), gaming (Giannakos et al., 2019; Wan et al., 2021), human emotion analysis (Du et al., 2022; Abdel-Ghaffar et al., 2022; Abdel-Ghaffar and Daoudi, 2020) and security (Zhang et al., 2021; Biradar et al., 2022). Conventional biometrics such as face (Agrawal et al., 2021), iris (Sonkar and Rani, 2021), fingerprint (Yin et al., 2021), voice (Shofiyah et al., 2022), and DNA (Zahid et al., 2019) contain unique and repeatable identity information for each individual, but each of them have it's own limitation (Sudar et al., 2019).

EEG signals have recently been proposed as a promising biometric approach. Thomas and Vinod in (Thomas and Vinod, 2016) studied person authentication from EEG signals during the rest state with both eye open (EO) and eye close (EC) using sample entropy and power spectral density, their system reached a genuine accept rate (GAR) of 99.7% for EO, and 98.6% for EC in the beta frequency band. Monsy in (Monsy, 2020) used frequency-weighted power (FWP) which is an equivalent representation of the power in a specific frequency band. The system was examined using two EEG datasets recorder during the rest-state and achieved an equal error rate (EER) of 0.0039 from EC resting state EEG signals. Biradar et al. and Gui et al. in (Biradar et al., 2022; Gui et al., 2019) offered an extensive survey on the use of brain signals for building biometric security systems. In crypto-systems, participants use secret keys to protect their confidential data. Keys should be long, unique and repeatable which make them very hard to generate and memorize. Biometrics have been widely used in cryptographic key generation (Wang et al., 2020; Knutson et al., 2021).

Recently, generating cryptographic keys from brain waves was introduced. Bajwa and Dantu in (Bajwa and Dantu, 2016)

* Corresponding author.
E-mail address: eman.mohamed@feng.bu.edu.eg (E.A. Abdel-Ghaffar).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.03.019
1319-1578/© 2023 The Author(s). Published by Elsevier B.V. on behalf of King Saud University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

performed user authentication based on EEG signals, they used energy bands obtained from discrete Fourier transform and discrete wavelet transform. Their system was tested using two datasets achieving mean accuracy of 98.46% and 91.05%. For performing neurokey generation, feature selection task was performed using normalized thresholds and segmentation window protocol. They generated a 230 bit key, and evaluated the strength of their generated key using nine NIST tests. They concluded that, different keys could be generated from different mental tasks. Nguyen et a. in (Nguyen et al., 2017) used power spectral density from different frequency bands as features. They used a random initialization vector (IV) with a password for better protection for users' templates and to add more randomness for their generated keys. They evaluated their method using the EEG Alcoholism and GrazIIIa datasets, and found that their generated key has 99% regeneration success rate. Their generated key was 192 bits and they evaluated its strength using six NIST tests.

A common limitation that faces all biometric based cryptosystems is that; biometrics are noisy in nature, as they are sensitive to acquisition equipment's, environmental conditions and variation in biometric itself over time. As, cryptographic keys needs to be exact, any change in the biometric will cause variation in the generated key. The challenge in all biometric based cryptosystems is to overcome the variation in biometric itself over time and to generate multiple unique keys from the same biometric (Sudar et al., 2019).

The objective of this work is to design a stable EEG-based personal authentication and cryptographic key generation system that overcomes the previous limitations and offers the following security aspects;

- Prevents Biometric data leakage; The EEG data in its original form is not stored in the system database. Information stored in the user's template if stolen, will neither allow an imposter to be falsely accepted by the system nor it will help him in regenerating the correct cryptographic key.
- Provides stable authentication and key generation processes; Individual's EEG samples taken in different times are almost never identical. The system accuracy was found to be stable when tested using different datasets having variation in data collection procedure, number of participants, number of electrodes, and number of recording sessions. System accuracy was also stable when training and testing data are from the same session or from different sessions that are temporally spaced.
- Generate a set of unique keys that could be used in different applications; From the same EEG observation the proposed system generates a set of different keys with different lengths without the need to perform any change in the system internal structure. Each generated key is unique and repeatable.
- Generated keys are suitable to be used for cryptographic applications; The statistical properties of each generated Key were tested using NIST test suite, its degree of non-periodicity were examined using scale index text, and the correlation of the key and a shifted version of itself was checked using autocorrelation test. The generated keys passed all the tests and are suitable to be used as cryptographic keys.
- Time complexity analysis of the key generation process is performed showing that the key generation has linear complexity and is fast enough for practical applications.

The rest of the paper is organized as follows; in Section 2 we introduce the basic techniques used in building our system. Section 3 gives an overview on the three datasets used for testing our proposed system. In Section 4 we present our personal authentication and cryptographic key generation methodology. In Section 5 we summarize our results and analyze the security aspects offered by our proposed system. In Section 6 we conclude our work.

2. Related techniques

In this section we introduce some of the basic techniques used as building blocks in our proposed system.

2.1. Riemannian Geometry and the Manifold of SPD matrices

Recently, a series of techniques based on Riemannian geometry has been used to build different BCI applications (Corsi et al., 2021; Abdel-Ghaffar et al., 2022; Gupta et al., 2022). In this subsection we introduce some basic properties regarding the space of symmetric positive definite (SPD) matrices.

2.1.1. Manifold of SPD matrices: basic concepts

Let $M(N) = \{\mathbf{M} \in \mathbb{R}^{N\times N}\}$ be the space of $N \times N$ square matrices, while $S(N) = \{\mathbf{S} \in M(N), \mathbf{S}^T = \mathbf{S}\}$ be the space in $M(N)$ of symmetric $N \times N$ square matrices. $\mathscr{P}(N)$ is an open subset of $S(N)$ where, $\mathscr{P}(N) = \{\mathbf{P} \in S(N), \mathbf{u}^T\mathbf{P}\mathbf{u} > 0, \forall \mathbf{u} \in \mathbb{R}^N\}$. The space of $P(N)$ is the space of SPD matrices.

2.1.2. Covariance matrix Estimation

In this work, we generate the covariance matrices which represent the relations between the EEG signals recorded from N electrodes. Those covariance matrices are SPD matrices that forms a smooth Riemannian manifold with a non-positive curvature in the $N(N+1)/2$ dimensional Euclidean space.

Let $\mathbf{x}_k(t)$ be the time series recorded from each electrode, $k = 1, \ldots, N$. $\mathbf{x}_k(t)$ is divided into m small windows. Let $\mathbf{W}_{ik}$ refers to each window separately, where $i = 1, \ldots, m$ and $k = 1, \ldots, N$. $\mathbf{W}_{ik}$ is a vector containing n samples. Convolution is performed between each window and the corresponding windows from the N electrodes to generate m covariance matrices $\mathbf{C}_i, i = 1, .., m$.

Let $\mathbf{X} \in \mathbb{R}^{N\times n}$ be the set of EEG signals recorded from N electrodes and each having n samples. The covariance matrix $\mathbf{C} \in \mathbb{R}^{N\times N}$ is a square matrix that can be calculated from $\mathbf{X}$:

$$\mathbf{C} = \frac{1}{N-1}\sum_{i=1}^{N}(\mathbf{x}_i - \overline{\mathbf{x}})(\mathbf{x}_i - \overline{\mathbf{x}})^T \tag{1}$$

where $\overline{\mathbf{x}} = \frac{1}{N}\sum_{i=1}^{N}\mathbf{x}_i$

2.1.3. Riemannian distance

To measure the distance between two points $\mathbf{A}, \mathbf{B} \in P(N)$, we measure the geodesic distance, which is the length of the unique shortest path connecting the two points (Bhatia, 2009; Nielsen and Bhatia, 2013):

$$d(\mathbf{A}, \mathbf{B}) = \| \log\left(\mathbf{A}^{\frac{-1}{2}}\mathbf{B}\mathbf{A}^{\frac{-1}{2}}\right)\|_F = \left(\sum_{i=1}^{n}\log^2\lambda_i\right)^{1/2} \tag{2}$$

where $\|\cdot\|_F$ is the *Frobenius* norm, and $\lambda_i, \ldots, \lambda_n$ are the eigenvalues of $\left(\mathbf{A}^{\frac{-1}{2}}\mathbf{B}\mathbf{A}^{\frac{-1}{2}}\right)$.

2.1.4. Center of mass for a set of SPD Matrices

To describe the center of mass for a set of m points $(\mathbf{A}_1, \ldots, \mathbf{A}_m)$ on the SPD manifold we use the geometric mean, which is called Karcher mean (Bini and Iannazzo, 2011; Nielsen and Bhatia, 2013) and it is defined as:

$$\mathbf{G}(\mathbf{A_1}, \ldots, \mathbf{A_m}) = \underset{\mathbf{A}\in\mathscr{P}(n)}{\operatorname{argmin}}\sum_{i=1}^{m} d^2(X, \mathbf{A}_i) \tag{3}$$

where $d(\cdot,\cdot)$ is the Riemannian distance defined in Eq. (2). The unique point (X) that represent the minimum in Eq. (3) is the geometric mean and forms the solution for the matrix equation:

$$\sum_{i=1}^{m} \log\left(\mathbf{A}_i^{\frac{-1}{2}} X \mathbf{A}_i^{\frac{-1}{2}}\right) = 0 \tag{4}$$

for $m > 2$ Eq. (4) does not have a closed-form solution, iterative algorithms should be used (Rodrigues and Jutten, 2019; Congedo et al., 2017).

2.1.5. Vectorization

The element $c_{i,j}$ in an $N \times N$ covariance matrix $C \in P(N)$ indicates the covariance value between the i^{th} channel and the j^{th} channel.

$$\mathbf{C} = \begin{bmatrix} \mathbf{c_{1,1}} & \cdots & \mathbf{c_{1,N}} \\ \vdots & \ddots & \vdots \\ \mathbf{c_{N,1}} & \cdots & \mathbf{c_{N,N}} \end{bmatrix} \tag{5}$$

Due to symmetry, the upper triangular part of C can be flattened into an $\left[\frac{N(N+1)}{2} \times 1\right]$ column vector (Barachant et al., 2013):

$$\mathbf{V_C} = \left[\mathbf{c_{1,1}}; \sqrt{2}\mathbf{c_{1,2}}; \mathbf{c_{2,2}}; \sqrt{2}\mathbf{c_{1,3}}; \sqrt{2}\mathbf{c_{2,3}}; \mathbf{c_{3,3}}; \ldots; \mathbf{c_{N,N}}\right] \tag{6}$$

where, $\|\mathbf{C}\|_F = \|\mathbf{V_C}\|_2$. The equality of norm is preserved using the $\sqrt{2}$ coefficient applied on the non-diagonal elements.

2.2. Error correction code

In our proposed key generation algorithm the error correction process is performed using Reed-Solomon (RS) coder. RS coder is a systematic block coder that have the following properties (Shrestha and Xu, 2011; Singh, 2013):

- RS coder works with multi-bit symbols, each symbol consists of m bits.
- The message is divided into separate blocks of data (k symbols each).
- It is described as $RS(n,k)$, where $n \leqslant 2^m - 1$.
- Parity protection information ($2t$ symbols) is added to each block to form a self-contained code word of n symbols. Fig. 1 shown RS code configurations.
- The code adds $2t$ parity symbols and is capable of correcting t symbol errors where;

$$t = \begin{cases} \frac{n-k}{2}, & \text{for } (n-k) \text{ even} \\ \frac{n-k-1}{2}, & \text{for } (n-k) \text{ odd} \end{cases} \tag{7}$$

- In RS code both the message and parity symbols are elements of Galois field (GF), for coding m bit symbols, the GF has 2^m elements (Shrestha and Xu, 2011).

One of the advantages of RS coder is that, it works with symbols of m bits which makes RS particularly good when dealing with bursts of errors because even if all the m bits in a symbols is wrong, this counts only as one error.

3. Data sets

Our proposed system is examined using three publicly available datasets, AMIGOS, DEAP and SEED. Table 1, gives an overview for the three datasets, and Fig. 2 shows the electrode positioning in each.

In AMIGOS dataset (Miranda-Correa et al., 2021) EEG and other physiological signals were recorded. The dataset contains two experiments one for individuals and the other for groups. In this work we are using the individuals experiment in which EEG signals were recorded from 40 participants watching 16 short emotional videos. EEG signals were recorded using 14 electrodes placed according to the 10–20 international positioning system (Jurcak and Tsuzuki, 2007) at a sampling rate of 128 Hz. Each observation (trial) is from 51 to 150 s according to the length of the stimuli video used. In this work we limit each trial time to 51s, and we excluded 6 participants (ID number 12, 21, 22, 23, 24, 33) with invalid and corrupted data.

In the DEAP dataset (Koelstra et al., 2012) EEG and other physiological signals of 32 participants were recorded while each of them watching 40 one-minute musical videos. EEG signals were recorded using 32 electrodes placed according to the 10–20 international positioning system at a sampling rate of 512 Hz. The DEAP dataset is recorded in two sessions in the same day separated by a lunch break (20 trials per session). DEAP has a pre-processed version in which, the Electrooculography (EOG) artifacts were removed, signals were down-sampled to 128 Hz, and filtered from 4 to 45 Hz. Each observation (trial) is 63s in which the first 3s are baseline signals. In this work we use the pre-processed version of DEAP and the first 3s were removed.

In the SEED dataset (Duan et al., 2013; Zheng and Lu, 2015) EEG signals of 15 participants were recorded while each of them watching 15 videos excerpts from Chinese movies. EEG signals were recorded using 62 electrodes placed according to the 10–20 international positioning system (Jurcak and Tsuzuki, 2007) at a sampling rate of 1000 Hz. The dataset was recorded during 3 sessions with an interval of approximately one week between sessions (15 trials per session for each participant). In the pre-processed version of SEED, signals were down-sampled to 200 Hz, and filtered from filter 0–75 Hz. Each observation (trial) is from 185 to 265 s according to the length of the stimuli video used. In this work we used the pre-processed version of SEED and limit each trial time to 185s.

4. Methodology

In this section, we present our proposed personal authentication and cryptographic Key generation mechanism.

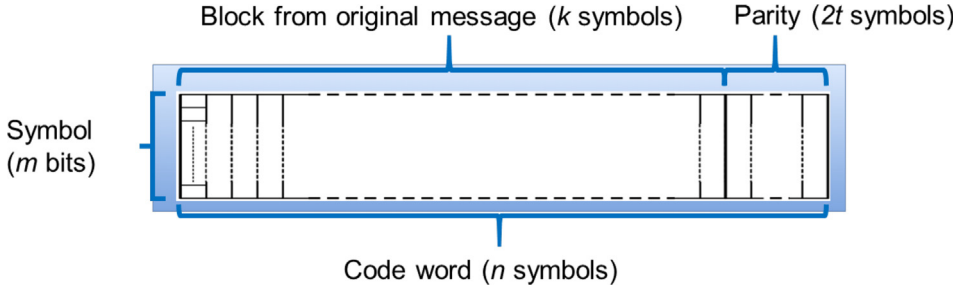


Fig. 1. Reed-solomon code configuration.

Table 1
An overview on the AMIGOS, DEAP and SEED datasets.

Item	AMIGOS	DEAP	SEED
Recording Device	Emotiv Neuroheadset3	Biosemi ActiveII	ESI NeuroScan
# of subjects	40	32	15
Subjects Description	27 males, 13 females	16 males, 16 females	7 males, 8 females
# of Electrodes	14	32	62
Sampling Rate	128 Hz	Originally 512 Hz, down-sampled to 128 Hz	Originally 1000 Hz, down-sampled to 200 Hz
Affective Stimuli	Music Videos	Music Videos	Excerpts from movies
# of Recording Sessions	One	Two-sessions in the same day.	Three sessions (approximately one week apart).
# of Trials per session	16	40	15
Trial Duration	From 51s to 150s	63 s	From 185s to 265s

4.1. Personal authentication

Personal authentication task is divided into two stages; the enrollment stage and the verification stage.

4.1.1. The enrolment stage

During the enrolment stage, each user offers his claimed ID, required cryptographic key length (in bits) and M trials (each trial consists of N-channel EEG signals used for training the system). The enrolment stage is illustrated in Fig. 3 and summarized in the following steps:

1. In each training trial (observation) the EEG signals are recorded from N electrodes. The signal from each electrode is divided into m small windows. Covariance matrices are generated from each set of windows, as explained in Section 2.1.2. Since, the three datasets AMIGOS, DEAP and SEED used to examine our system are mainly created to analyze human emotions, and as the emotion hold time is from 1 to 8 s (Mohammadi et al., 2017; Thammasan et al., 2016). We decided to work with a window size of 10s to avoid the influence of participant affective state on the authentication and key generation processes.
2. As each participant offers M trials in the enrollment stage. The geometric mean $\mathbf{R}_i$ for the set of covariance matrices in each training trial $\mathbf{T}_i$ (where $i = 1, \ldots, M$), is calculated as explained in Section 2.1.4.
3. We use the set of geometric means $R_1, \ldots, R_M$, calculated in the previous stage to generate a common center point for each participant G, using Eq. 3.
4. To simplify key generation process, point $G \in \mathbb{R}^{N \times N}$ is converted into an $\left[\frac{N(N+1)}{2} \times 1\right]$ column vector V_G as explained in section (2.1.5).
5. The vector V_G is quantized using a scalar quantizer in which the quantization levels (threshold values) are determined using multi-Otsu thresholding method (Liao et al., 2001). The output from the quantizer consists of two parts; the first part QV_G which is the quantized values of V_G that forms the input to the RS encoder. The second part is the quantization thresholds which is a $L \times 1$ vector (where L is the number of quantization levels). The quantization threshold is stored in the system database as the first part of user's template.
6. The quantized vector QV_G forms the input to Reed-Solomon encoder. The number of bits per symbol in QV_G is 8 bits. The Reed-Solomon encoder we used is RS(255,239) the parameters of the RS coder is; $m = 8; n = 255, k = 239, 2t = 16$. This coder is capable of correcting 8 symbols. The Reed-Solomon error correction coder is explained in in Section 2.2 and the generated code configuration is shown in Fig. 1. The symbols in QV_G is divided into blocks k symbols each. Let the number of symbols in QV_G be H symbols. if H/k is not integer, zeros are added at the end of the last block to make all the blocks complete with k symbols each. The output of the Reed-Solomon encoder is divided into two parts; the first part is an $[H * k]$ matrix represents the coded symbols of QV_G, this part is used to generate the key. The second part is $[H \times 2t]$ symbols which represents the parity symbols, those parity symbols are flattened into a $[H * 2t \times 1]$ vector which is stored as the second part in the user's template.

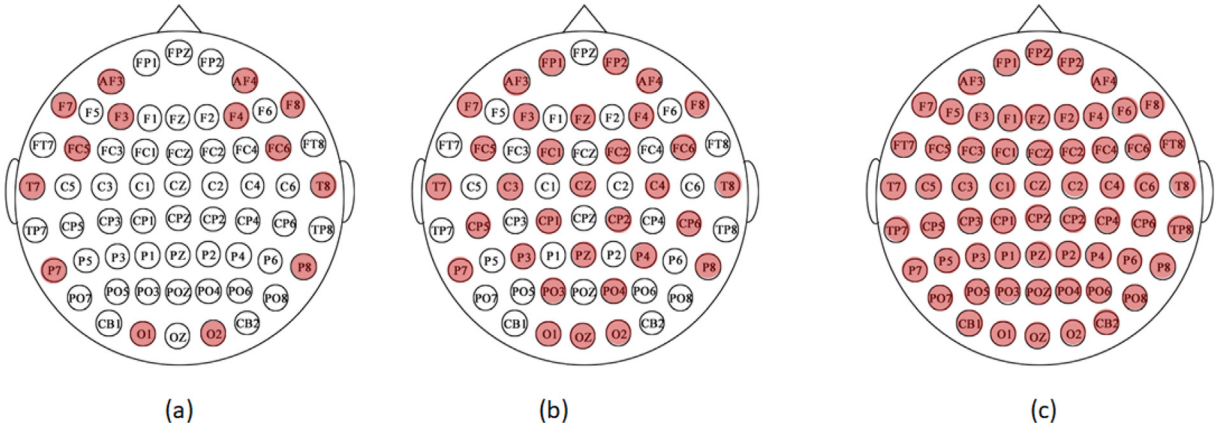


Fig. 2. Electrode positioning (a) AMIGOS dataset 14 electrodes. (b) DEAP dataset 32 electrodes (c) SEED dataset 62 electrodes. Electrodes placed according to the 10–20 international positioning system.

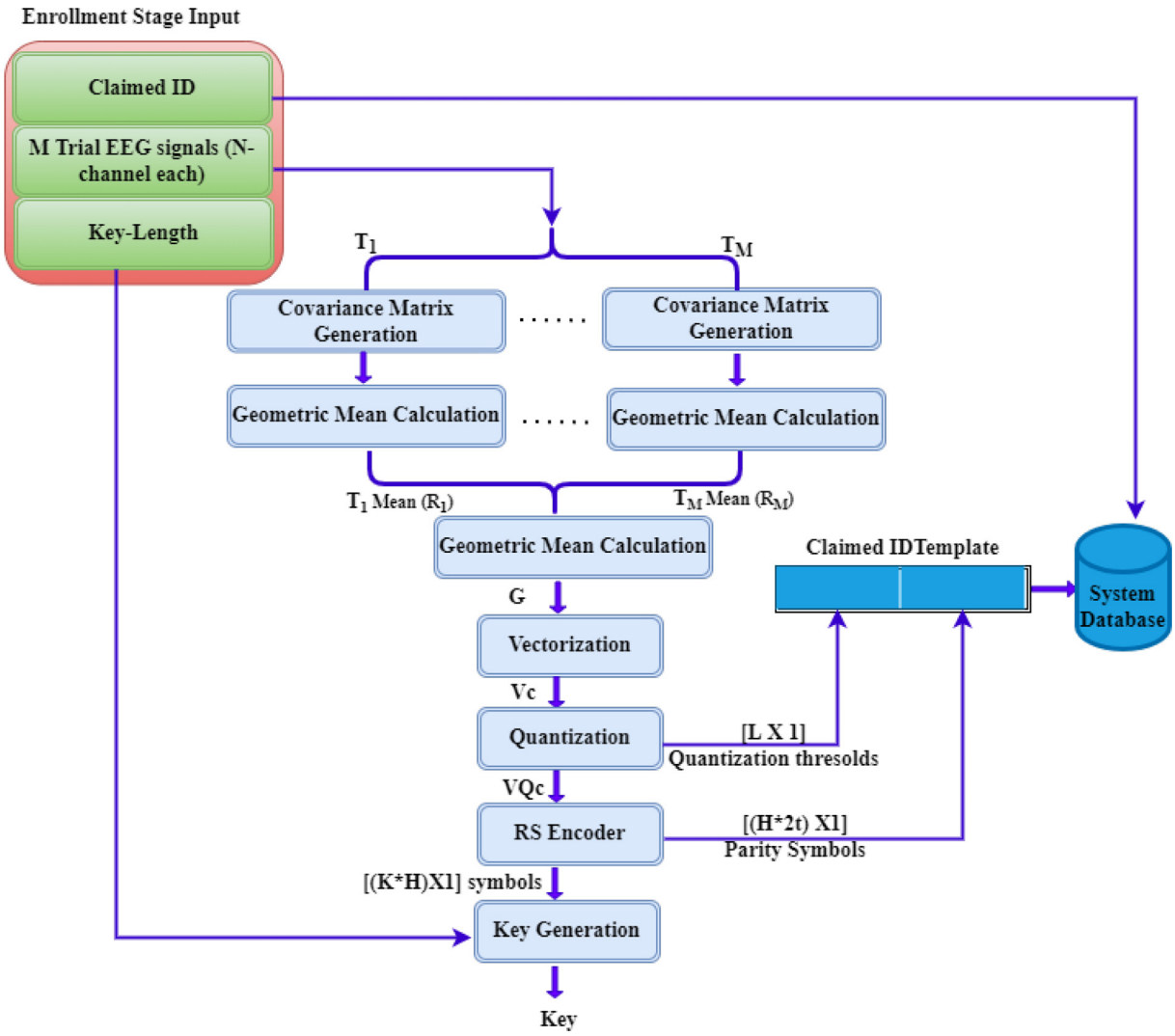


Fig. 3. Enrolment Stage. During the enrolment stage, each user offers his claimed ID, required cryptographic key length (in bits) and M trials (each trial consists of N-channel EEG signals used for training the system). The quantization thresholds and the parity symbols are stored in user template in the system database. The generated key is used for encryption.

7. The $H \times k$ matrix represents the coded symbols output from the RS encoder is flattened into $[(H * k) \times 1]$ vector, and forms one of the inputs to the key generation process (4.2).

4.1.2. The verification stage

During the verification stage, each user claims an identity and offers an observation (N-channels EEG signals). Each user should also determine the length of the required cryptographic key. The verification stage is illustrated in Fig. 4 and summarized in the following steps.

1. The EEG signals are recorded from N electrodes. The signal from each electrode is divided into 10s windows. Then, covariance matrices are generated from each set of windows using Eq. 1.
2. The geometric mean **R** for the set of covariance matrices **G** is calculated using Eq. 3.
3. Point **G** is converted into an $\left[\frac{N(N+1)}{2} \times 1\right]$ column vector V_G using Eq. 6.
4. The vector V_G is quantized using a scalar quantizer in which the quantization levels (threshold values) are taken from the $[L \times 1]$ vector stored in the user's claimed ID template.
5. The output from the quantizer QV_G is reshaped to form an $[H \times K]$ matrix if H/k is not integer, zeros are added at the end of the last block to make all the blocks complete with k symbols each. The $[H * 2t \times 1]$ parity vector stored in the user's template is also reshaped into $[H \times 2t]$ matrix, the two matrices are horizontally concatenated. Each raw is n symbols (n = 255) forms the input to the RS decoder. The RS decoder is capable of correcting t symbols in each raw. If the error result from RS decoder is zero the verification process is completed and the user is genuine, other wise he is an imposter.
6. If the user is genuine, the key generation process (explained in Section 4.2) is performed.

4.2. Key generation

The key generation process is performed using SHAKE-265 cryptographic hash function that requires two inputs;

- The $[H \times k]$ matrix representing the coded symbols output from the RS encoder after flattening it into $[(H * k) \times 1]$ vector.
- The required key length in bits which is provided by the user during both the enrollment and the verification stages.

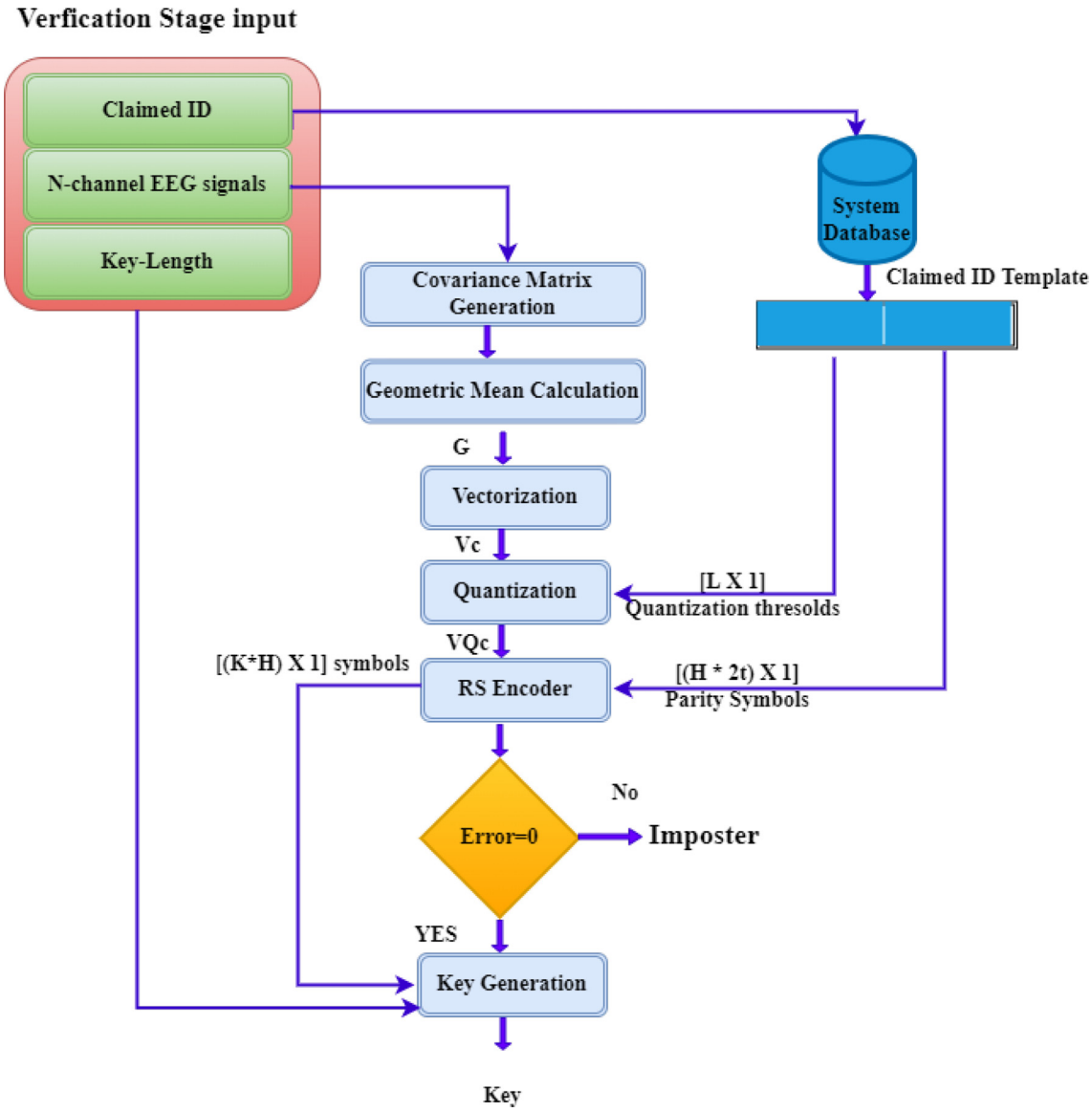


Fig. 4. Verification Stage. During the verification stage, each user claims an identity and offers an observation (*N*-channels EEG signals), and determine the length of the required cryptographic key. Quantization thresholds and parity symbols stored in the user template is used during the verification process. If the error result from RS encoder is zero the verification process is completed and the user is genuine, other wise he is an imposter. If the user is genuine, the key generation process is performed and the result key is used for decryption.

SHAKE-265 is an extendable-output function (XOF) [(Dworkin, 2015; Sarker et al., 2020). The XOF share the same sponge construction with SHA-3 hash functions (Bertoni et al., 2014). The advantage of using XOF as key derivative function is that, the length of the output can be chosen to meet the requirements of individual applications. So, the user can generate different keys with different lengths for each of his applications. Each of those keys is unique and repeatable.

5. Results and discussion

To evaluate the stability of our proposed technique we performed two experiments; in the first experiment training and testing data are from the same session. In the second experiment training and testing data are from different sessions. The first experiment generates the following outcomes; AMIGOS, DEAP-Case1, DEAP-Case2, SEED-Case1, and SEED-Case2. In AMIGOS, DEAP-Case1, and SEED-Case1 we use the data from the same session for both training and testing. In DEAP-case2 we collect the data from each user two sessions and use it in both training and testing processes. In SEED-Case2 we collect the data from each user three sessions and use it in both training and testing processes. The cross validation in this first experiment is performed by dividing the data into 70% training and 30% testing and performing 5-fold cross validation.

The second experiment is applied only on DEAP and SEED datasets, as they contain more than one session (Dataset description section III). The second experiment generates the following outcomes; DEAP-Case3, SEED-Case3, and SEED-Case4. In DEAP-Case3 we use the data from one session for training and the other session for testing. In SEED-Case3 when we use data from two sessions for training and data from the third sessions for testing. SEED-Case4 when we use data from one session for training and data from the other two sessions for testing. The accuracy of our proposed system is evaluated using; Genuine accept rate (GAR), false reject rate (FRR), and false accept rate (FAR). The result from both the two experiments is shown in Table 2. From which we can see that

Table 2
Results from the two experiments. Results from experiment 1 (Amigos, DEAP-Case1, DEAP-Case2, SEED-Case1, SEED-Case2. Results from experiment 2 (DEAP-Case3, SEED-Case3, SEED-Case4.

	AMIGOS	DEAP			SEED			
		Case1	Case2	Case3	Case1	Case2	Case3	Case4
GAR	96.23 ± 0.628	98.85 ± 0.588	98.63 ± 0.034	98.34 ± 0.043	99.89 ± 0.034	99.55 ± 0.056	99.31 ± 0.133	99.25 ± 0.083
FRR	3.772 ± 0.628	1.154 ± 0.588	1.37 ± 0.034	1.63 ± 0.043	0.114 ± 0.034	0.446 ± 0.066	0.694 ± 0.133	0.746 ± 0.083
FAR	0.039 ± 0.015	0.092 ± 0.042	0.063 ± 0.023	0.047 ± 0.021	0.104 ± 0.019	0.379 ± 0.026	0.229 ± 0.017	0.115 ± 0.047

Table 3
Comparison of the proposed system accuracy with other techniques in the literature.

Study	Dataset	Neuro-key	Accuracy
(Monsy, 2020)	**PhysioNET** - (109 subject, 64 electrodes, 4 tasks, 14 runs in 1 day).	No	Using 20-electrodes HTER(0.0065), 64-electrodes HTER(0.00345)
	BMIS Lab - (16 subjects, 64 electrodes, rest state, 1 session).	No	20-electrode HTER(0.00915), 64-electrodes HTER(0.003)
(Thomas and Vinod, 2016)	**PhysioNET**	No	EO-GAR(99.7%), EC-GAR(98.6%) in the beta band.
(Ashenaei et al., 2022)	**PhysioNET**	No	Using 21- electrodes Same session GAR(99.48%). Different sessions (EO-GAR(93.98%), EC-GAR(86.19%)).
	Self-collected dataset- (21 subjects, 21 electrodes, rest state-EC, 4 sessions in 1 day).	No	Same session GAR(99.84%). Different sessions GAR(93.76%).
(Bajwa and Dantu, 2016)	**Keirn and Aunon dataset**- (7 subjects, 6 electrodes, 5 mental tasks, 1 session).	230 bit	GAR(98.46%).
	Alcoholism- (120 subject, 64 electrode, 1 session).	230 bit	Using 18 electrodes GAR(91.05%).
(Damaševicius et al., 2018)	**Self-collected database**- (42 subjects, 17 electrodes, rest state, 1 session).	Up to 400 bit.	EER(0.024), and TPR(99.74%)
(Nguyen et al., 2017)	**Alcoholism**.	192 bit	EER(0.079) in Gamma band.
	GrazIIIa - (3 subjects, 60 electrodes, six sessions).	192 bit	EER(0.0018) in Gamma band.
(Nguyen et al., 2019)	**GrazIIIa**	256 bit	Using 32 electrodes EER(0.4%) in Gamma band.
	DEAP	256 bit	EER(2.83%) in the Gamma band.
(Yang et al., 2017)	**Self-collected database** - (10 subjects, 4 electrodes, different tasks, 4 session in 1 week).	21 bits	FAR(1.83%), ERR(1.875%).
Our System	**AMIGOS**	128, 265, 512,...	GAR(96.23%), FAR(0.039%).
	DEAP	128, 265, 512,...	Same session GAR(98.845%), FAR(0.092%). Different sessions GAR (98.34%), FAR(0.043%).
	SEED	128, 265, 512,...	Same session GAR(99.89%), FAR(0.104%). Different sessions GAR (99.25%), FAR(0.115%).

using different sessions for training and testing results in slight reduction in GAR around (1%) while in (Ashenaei et al., 2022) the reduction in GAR caused by using different sessions was around 5% to 6%. The result of our proposed system is comparable with other techniques that exist in literature. Table 3 shows a comparison between our result and others.

5.1. Key testing

For analysing the randomness of the generated keys and determine whether or not they are suitable to be used as cryptographic keys. The generated keys were examined using NIST test suite, scale index test, and autocorrelation test.

We used the NIST statistical test suite for the validation of random numbers for cryptographic applications (AndrewRukhin et al., 2010) to test the randomness of the generated cryptographic keys. The p-value is the most important parameter in each NIST test as it represents the measure of randomness for the tested sequence. If $p > 0.01$, then the test is successful and the tested sequence is considered random. For performing NIST tests keys with length 1100000 bits were generated. Table 4 shows the the percentage of keys successfully passed each of the fifteen NIST tests.

The scale index test is used to investigate the degree of non-periodicity of the generated keys. Scale index test was first introduced by (Benítez et al., 2010), several studies in the literature used it to examine the periodicity of their generated cryptographic keys (Kaya, 2020a; Kaya et al., 2021). The scale index value is between zero and one, if the scale index of tested sequence is one or near one it is considered non-periodic (Kaya, 2020b; Kaya and Tuncer, 2019). To perform the scale index test we used R package wavScalogram (Bolós and Benítez, 2022). The average scale index value for keys with different lengths is illustrated in Table 5. All average scale index values are between 0.7168 and 0.8988 which indicates that the generated keys are non-periodic.

The autocorrelation test is concerned with the dependency between numbers in a sequence, it is used to measure the relation between current values and past values of the tested sequence, it determines if their are any repetitive pattern of bits (Menezes et al., 1996, Ch. 5). Eq. 8 shows the mathematical definition for testing a sequence s having n bits (Tuncer and Kaya, 2018):

$$A(m) = \sum_{i=0}^{n-m-1} s_i \oplus s_{i+m} \tag{8}$$

where $\oplus$ is the XOR operation, m is the lag ($1 \leqslant m \leqslant \lfloor n/2 \rfloor$). Eq. 9 shows the relationship between 0 and 1s in a sequence.

$$X5 = \frac{2[A(m) - (n-m)/2]}{\sqrt{n-m}} \tag{9}$$

for $\alpha = 0.05$, the tested sequence passes the autocorrelation test if $|X5| < 1.6449$. The autocorrelation test is performed on all the

Table 4
NIST Test Results. The percentage of keys successfully passed the NIST tests.

Test type	AMIGOS	DEAP	SEED
Frequency (Monobit) test	100	100	100
Frequency within a Block	100	100	100
Runs Test	100	100	100
Longest-Run-of-Ones in a Block	100	100	100
Binary Matrix Rank	100	100	100
Discrete Fourier Transform (Spectral) test	91.17	93.8	93.3
Non-overlapping Template Matching	100	100	100
Overlapping Template Matching	100	100	100
Maurer's "Universal Statistical"	85.3	84.32	80
Linear Complexity	97.05	96.8	93.3
Serial	82.35/ 85.23	84.4/ 87.5	86.6/ 88.8
Approximate Entropy	97.05	100	93.3
Cumulative Sums (Cusums)	100	100	100
Random Excursions	82.35	84.4	86.6
Random Excursions Variant	100	100	100

Table 5
Scale index Test Results. Average scale index values for keys with different lengths.

Key length	AMIGOS	DEAP	SEED
128	0.82582	0.80684	0.8988
256	0.74245	0.74055	0.8239
512	0.77641	0.77489	0.7989
1024	0.72582	0.71684	0.8518

Table 6
Autocorrelation Test Results. The percentage of keys successfully passed the Autocorrelation test (for different m values).

m	AMIGOS	DEAP	SEED
16	91.18	93.55	90.32
32	97.05	96.8	93.55
64	97.06	87.5	95.55
128	87.35	86.375	91.12
256	97.06	90.63	92.12

generated keys for different m values and the average success rate is shown in Table 6.

5.2. Time complexity analysis

In this section we perform time complexity analysis for the key generation process. The time cost is measured in the running environment: Intel(R) Core(TM) i7-6500U CPU, 16 GB RAM and MATLAB 2021a software framework. Time cost is measured using the CPU time. We generate the keys 100 times for each user in each database and average the result time. Keys with 10 different length from 128 bits to 65563 bits (2^7 to 2^{16}) where generated. Fig. 5 shows the time cost for key generation process. From which we can see that the key generation is a linear process, which is justified as the key generation is performed using SHAKE-265 cryptographic hash function which is linear with complexity $O(n+m)$ where n and m are the sizes of input and output respectively. The hash function input is the reshaped QV_G vector output from the quantizer with size $[N*(N+1)/2]$ where N is the number of electrodes (Section 4.2). Since, AMIGOS dataset recorded from 14 electrodes, DEAP from 32 electrodes and SEED from 62 electrodes, the input vector size for AMIGOS, DEAP, and SEED dataset are 105, 528, and 1953 samples respectively. Difference in input vector size justifies the difference in time required for key generation that appears clearly in Fig. 5b. The key generation time from AMIGOS dataset is between 0.84 to 10.3 ms, for DEAP dataset between 1.8 to 11.6 ms, and for SEED dataset between 8 and 18.5 ms. For reasonable key length the proposed key generation process is suitable for practical applications.

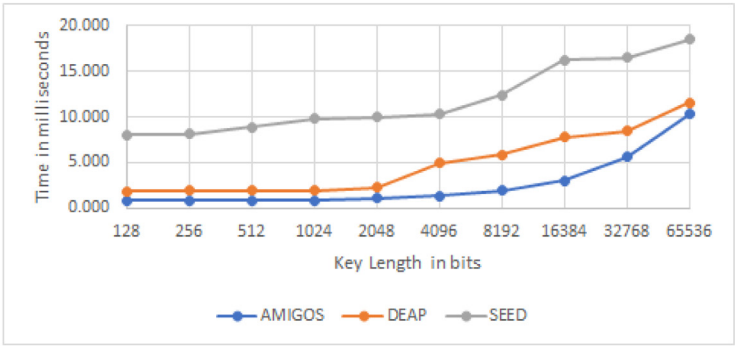
5.3. Security analysis

Our proposed system offers several security aspects summarized in the following points;

- The original user data is not stored in the system database, so even if an imposter steal a genuine user template he will neither be able to pass the authentication process nor regenerate the cryptographic key.
- The quantization thresholds for each participant is stored in his template in the system database. Since we used a scalar quantizer in which the quantization levels are determined using multi-Otsu thresholding method, each participant will have his own quantization thresholds. This results in reducing the FAR in our system.
- Also in the user template we stored the $[H \times 2t]$ symbols which represents the parity symbols results from the RS encoder. Storing user specific parity symbols gave us two benefits. First, it increased the GAR as during the verification process the RS error correction will focus all its t symbol correction capability on the errors exist in the user's new offered observation, which will increase the GAR. Second, if an imposter offered his own observation concatenating the genuine user $[H \times 2t]$ parity symbols

key Length	AMIGOS	DEAP	SEED
128	0.840	1.875	8.069
256	0.842	1.901	8.141
512	0.845	1.917	8.908
1024	0.848	1.925	9.752
2048	1.087	2.304	9.914
4096	1.380	4.951	10.276
8192	1.902	5.858	12.338
16384	3.010	7.818	16.198
32768	5.573	8.444	16.509
65563	10.296	11.556	18.494

(a)



(b)

Fig. 5. Time Complexity Analysis results. (a) A table contains key length in bits and key generation time in milliseconds. (b) A figure illustrating the linear relationship between increasing key length and the time required for the key generation process.

to the imposter quantizer output ($[H * K]$ matrix) will reduce the capability of the RS error corrector to recover the genuine user's vector which consequently results in reducing the FAR of our proposed system.

- One of the major problems in generating cryptographic key from biometrics is the limited capability of generating multiple keys from the same users' biometric template. In our proposed system we used SHAKE-265 which shares the sponge construction with SHA-3 hash functions. This gave us the advantage of generating different keys with different lengths from the same users' template without the need for performing any changes inside the system.
- The statistical properties of each generated Key were tested using NIST test suite, its degree of non-periodicity were examined using scale index text, and the correlation of the key and a shifted version of itself was checked using autocorrelation test. The generated keys passed all the tests and are suitable to be used as cryptographic keys.

5.4. Limitations of the study

Although it has been validated that the proposed system offers a stable personal authentication and cryptographic key generation mechanism, there are some limitations that need to be addressed in future work. First, the proposed method was examined using only three datasets with maximum three sessions one week apart. These results are limited, if the time separation between sessions are wider (months or years), the system performance is unknown. More experiments needs to be performed using datasets with larger number of sessions that are temporal separated over longer periods of time. Second, in this work we used a window size of 10s to avoid the influence of participant affective state on the authentication and key generation processes. Several studies (Nguyen et al., 2018; Pham et al., 2015; Arnau-González et al., 2021) concluded that emotions have significant impact on the performance of EEG based authentication systems. Investigating the influence of human emotional state on our proposed technique needs to be performed.

6. Conclusion

In this work, we present a system for personal authentication and cryptographic key generation based on EEG signals. The personal authentication process was performed using the raw EEG data without feature extraction by generating covariance matrices from the N-channel EEG signals and representing them as points (SPD matrices) on a Riemannian manifold. Then geometric mean was generated from each observation, followed by vectorization, quantization, and error correction processes (Section 4). The raw EEG data is not stored in the system database, even if an intruder steals a genuine user template, he will neither be capable of passing the authentication process nor regenerating the cryptographic key.

The personal authentication process was tested using three publicly available datasets AMIGOS, DEAP and SEED. Obtaining a GAR of 96.23%, 98.85% and 99.89% respectively if the training and testing data are from the same session, and 98.34% and 99.25% from the DEAP and SEED datasets when the training and testing data are from different sessions (Section 5). The achieved results are comparable to other techniques in the literature (Table (3).

A set of different cryptographic keys with different lengths is generated from each user sample, without the need for changing any internal system configuration. The user just needs to specify the required key length during both the enrollment and verification processes. For testing the statistical properties of the generated keys, were tested using NIST test suite, scale index text, and autocorrelation test. The generated keys passed all the tests and are suitable to be used as cryptographic keys (Section 5.1). Time complexity analysis of the key generation process is performed showing that the key generation has linear complexity and is fast enough for practical applications (Section 5.2).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abdel-Ghaffar, E.A., Daoudi, M., 2020. Emotion recognition from multidimensional electroencephalographic signals on the manifold of symmetric positive definite matrices. In: 2020 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp. 354–359. https://doi.org/10.1109/MIPR49039.2020.00078.

Abdel-Ghaffar, E.A., Wu, Y., Daoudi, M., 2022. Subject-dependent emotion recognition system based on multidimensional electroencephalographic signals: A riemannian geometry approach. IEEE Access 10, 14993–15006. https://doi.org/10.1109/ACCESS.2022.3147461.

Abu-gellban, H., Zhuang, Y., Nguyen, L., Zhang, Z., Imhmed, E., 2022. Csdleeg: Identifying confused students based on eeg using multi-view deep learning. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1217–1222. https://doi.org/10.1109/COMPSAC54236.2022.00192.

Agrawal, S.C., Sharma, V., Bhardwaj, P., 2021. Face recognition:a review of datasets and methods. In: 2021 5th International Conference on Information Systems and Computer Networks (ISCON), pp. 1–6. https://doi.org/10.1109/ISCON52037.2021.9702300.

Amin, C.R., Hasin, M.F., Leon, T.S., Aurko, A.B., Tamanna, T., Rahman, M.A., Parvez, M. Z., 2020. Consumer behavior analysis using eeg signals for neuromarketing application. In: 2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 2061–2066. https://doi.org/10.1109/SSCI47803.2020.9308358.

AndrewRukhin, JuanSoto, JamesNechvatal, Smid, M., ElaineBarker, Leigh, S., MarkLevenson, Vangel, M., DavidBanks, AlanHeckert, JamesDray, SanVo, 2010. NIST Special Publication 800–22: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications.

Arnau-González, P., Arevalillo-Herráez, M., Katsigiannis, S., Ramzan, N., 2021. On the influence of affect in eeg-based subject identification. IEEE Trans. Affective Comput. 12, 391–401. https://doi.org/10.1109/TAFFC.2018.2877986.

Ashenaei, R., Asghar Beheshti, A., Yousefi Rezaii, T., 2022. Stable eeg-based biometric system using functional connectivity based on time-frequency features with optimal channels. Biomed. Signal Process. Control 77, 103790. URL: https://www.sciencedirect.com/science/article/pii/S1746809422003123, https://doi.org/10.1016/j.bspc.2022.103790.

Bajwa, G., Dantu, R., 2016. Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Comput. Sec. 62, 95–113. URL: https://www.sciencedirect.com/science/article/pii/S0167404816300669, https://doi.org/10.1016/j.cose.2016.06.001.

Barachant, A., Bonnet, S., Congedo, M., Jutten, C., 2013. Classification of covariance matrices using a Riemannian-based kernel for BCI applications. Neurocomputing 112, 172–178. URL: https://hal.archives-ouvertes.fr/hal-00820475, https://doi.org/10.1016/j.neucom.2012.12.039.

Benítez, R., Bolós, V., Ramírez, M., 2010. A wavelet-based tool for studying non-periodicity. Comput. Mathe. Appl. 60, 634–641. URL: https://www.sciencedirect.com/science/article/pii/S0898122110003597, https://doi.org/10.1016/j.camwa.2010.05.010.

Bertoni, G., Daemen, J., Peeters, M., Assche, G.V., 2014. The making of KECCAK. Cryptologia 38, 26–60. https://doi.org/10.1080/01611194.2013.856818.

Bhatia, R., 2009. Positive Definite Matrices. Prinecton University Press.

Bini, D.A., Iannazzo, B., 2011. A note on computing matrix geometric means. Adv. Comput. Mathe. 35, 175–192.

Biradar, S.D., Nalbalwar, S.L., Deosarkar, S.B., 2022. Biometric security using eeg signal processing – acquisition, representation and classification approaches. In: 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1–6. https://doi.org/10.1109/ICDCECE53908.2022.9792639.

Bolós, V.J., Benítez, R., 2022. wavscalogram: an r package with scalogram wavelet tools for time series analysis. The R J. 14, 164–185. https://doi.org/10.32614/RJ-2022-031.

Congedo, M., Barachant, A., Koopaei, E.K., 2017. Fixed point algorithms for estimating power means of positive definite matrices. IEEE Trans. Signal Process. 65, 2211–2220. https://doi.org/10.1109/TSP.2017.2649483.

Corsi, M.C., Yger, F., Chevallier, S., Noûs, C., 2021. Riemannian geometry on connectivity for clinical bci. In: ICASSP 2021–2021 IEEE International

Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 980–984. https://doi.org/10.1109/ICASSP39728.2021.9414790.
Dahmani, A.A., Goncharenko, I., Gu, Y., 2022. E-worker mental fatigue detection through mindwave eeg data and deep neural networks. In: 2022 IEEE 4th Global Conference on Life Sciences and Technologies (LifeTech), pp. 501–502. https://doi.org/10.1109/LifeTech53646.2022.9754788.
Damaševicius, R., Maskeliunas, R., Kazanavicius, E., Wozniak, M., 2018. Combining cryptography with eeg biometrics. Comput. Intell. Neurosci. 2018, 1–11. https://doi.org/10.1155/2018/1867548.
Du, X., Ma, C., Zhang, G., Li, J., Lai, Y.K., Zhao, G., Deng, X., Liu, Y.J., Wang, H., 2022. An efficient lstm network for emotion recognition from multichannel eeg signals. IEEE Trans. Affective Comput. 13, 1528–1540. https://doi.org/10.1109/TAFFC.2020.3013711.
Duan, R.N., Zhu, J.Y., Lu, B.L., 2013. Differential entropy feature for EEG-based emotion classification, in. In: 6th International IEEE/EMBS Conference on Neural Engineering (NER), IEEE, pp. 81–84.
Dworkin, M., 2015. Sha-3 standard: Permutation-based hash and extendable-output functions. https://doi.org/10.6028/NIST.FIPS.202.
Giannakos, M.N., Sharma, K., Niforatos, E., 2019. Exploring EEG signals during the different phases of game-player interaction. In: 2019 11th Int. Conf. on Virtual Worlds and Games for Serious Applications (VS-Games), pp. 1–8. https://doi.org/10.1109/VS-Games.2019.8864519.
Gui, Q., Ruiz-Blondet, M.V., Laszlo, S., Jin, Z., 2019. A survey on brain biometrics. ACM Comput. Surv. 51. https://doi.org/10.1145/3230632.
Gupta, V., Meenakshinathan, J., Reddy, T.K., Behera, L., 2022. Performance study of neural structured learning using riemannian features for bci classification. In: 2022 National Conference on Communications (NCC), pp. 297–301. https://doi.org/10.1109/NCC55593.2022.9806736.
Jurcak, V., Tsuzuki, D., 2007. 10/20, 10/10, and 10/5 systems revisited: Their validity as relative head-surface-based positioning systems. Neuroimage 4, 1600–1611. https://doi.org/10.1016/j.neuroimage.2006.09.024.
Kaheh, S., Ramirez, M., Wong, J., George, K., 2021. Neuromarketing using eeg signals and eye-tracking. In: 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1–4. https://doi.org/10.1109/CONECCT52877.2021.9622539.
Kaushik, P., Gupta, A., Roy, P.P., Dogra, D.P., 2019. Eeg-based age and gender prediction using deep blstm-lstm network model. IEEE Sens. J. 19, 2634–2641. https://doi.org/10.1109/JSEN.2018.2885582.
Kaya, T., 2020a. Memristor and trivium-based true random number generator. Phys. A: Stat. Mech. Appl. 542, 124071. URL: https://www.sciencedirect.com/science/article/pii/S0378437119322502, https://doi.org/10.1016/j.physa.2019.124071.
Kaya, T., 2020b. A true random number generator based on a chua and ro-puf: design, implementation and statistical analysis. Analog Integr. Circ. Sig. Process 102, 415–426. https://doi.org/10.1007/s10470-019-01474-2.
Kaya, T., Tuncer, S.A., 2019. Generating random numbers from biological signals in labview environment and statistical analysis. Traitement du Signal 36, 303–310.
Kaya, T., Tuncer, T., Avaroğlu, E., 2021. True bit generation by using two different noise sources. J. Circ. Syst. Comput. 30, 2150261. https://doi.org/10.1142/S0218126621502613. arXiv:https://doi.org/10.1142/S0218126621502613.
Ke, H., Chen, D., Shi, B., Zhang, J., Liu, X., Zhang, X., Li, X., 2020. Improving brain e-health services via high-performance eeg classification with grouping bayesian optimization. IEEE Trans. Serv. Comput. 13, 696–708. https://doi.org/10.1109/TSC.2019.2962673.
Khurana, V., Gahalawat, M., Kumar, P., Roy, P.P., Dogra, D.P., Scheme, E., Soleymani, M., 2021. A survey on neuromarketing using eeg signals. IEEE Trans. Cognit. Develop. Syst. 13, 732–749. https://doi.org/10.1109/TCDS.2021.3065200.
Knutson, P., Raja, K., Larsson, D., Ramachandra, R., 2021. Finite field elliptic curve for key generation and biometric template protection. In: 2021 IEEE International Workshop on Biometrics and Forensics (IWBF), pp. 1–6. https://doi.org/10.1109/IWBF50991.2021.9465093.
Koelstra, S., Muhl, C., Soleymani, M., Lee, J., Yazdani, A., Ebrahimi, T., Pun, T., Nijholt, A., Patras, I., 2012. DEAP: A database for emotion analysis; using physiological signals. IEEE Trans. Affective Comput. 3, 18–31.
Liao, P.S., Chen, T.S., Chung, P.C., 2001. A fast algorithm for multilevel thresholding. J. Inf. Sci. Eng. 17, 713–727.
Lin, F., Kao, C., 2018. Mental effort detection using EEG data in E-learning contexts. Comput. Educ. 122, 63–79. URL: http://www.sciencedirect.com/science/article/pii/S0360131518300794, https://doi.org/10.1016/j.compedu.2018.03.020.
Menezes, A.J., van Oorschot, P.C., Vanstone, S.A., Rosen., K.H., 1996. Handboox of applied cryptography.
Miranda-Correa, J.A., Abadi, M.K., Sebe, N., Patras, I., 2021. Amigos: A dataset for affect, personality and mood research on individuals and groups. IEEE Trans. Affective Comput. 12, 479–493. https://doi.org/10.1109/TAFFC.2018.2884461.
Mohammadi, Z., Frounchi, J., Amiri, M., 2017. Wavelet-based emotion recognition system using EEG signal. Neural Comput. Appl. 28, 1985–1990. https://doi.org/10.1007/s00521-015-2149-8.
Monsy, J.C., 2020. Eeg-based biometric identification using frequency-weighted power feature. IET Biometrics 9, 251–258 (7). URL: https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2019.0158.
Nguyen, D., Tran, D., Sharma, D., Ma, W., 2017. On the study of eeg-based cryptographic key generation. Procedia Comput. Sci. 112, 936–945. URL: https://www.sciencedirect.com/science/article/pii/S1877050917314837, https://doi.org/10.1016/j.procs.2017.08.126. knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 21st International Conference, KES-20176-8 September 2017, Marseille, France.
Nguyen, D., Tran, D., Sharma, D., Ma, W., 2018. Emotional influences on cryptographic key generation systems using eeg signals. Proc. Comput. Sci. 126, 703–712. URL: https://www.sciencedirect.com/science/article/pii/S1877050918312821, https://doi.org/10.1016/j.procs.2018.08.004. knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 22nd International Conference, KES-2018, Belgrade, Serbia.
Nguyen, D., Tran, D.T., Ma, W., 2019. A study on combining eeg signals and crytography for bitcoin security. Aust. J. Intell. Inf. Process. Syst. 15, 34–42.
Nielsen, F., Bhatia, R., 2013. Matrix Information Geometry. Springer-Verlag, Berlin Heidelberg. https://doi.org/10.1007/978-3-642-30232-9. chapter 2.
Pham, T., Ma, W., Tran, D., Tran, D.S., Phung, D., 2015. A study on the stability of eeg signals for user authentication. In: 2015 7th International IEEE/EMBS Conference on Neural Engineering (NER), pp. 122–125. https://doi.org/10.1109/NER.2015.7146575.
Rodrigues, P., Jutten, C., 2019. Riemannian procrustes analysis: Transfer learning for brain-computer interfaces. IEEE Trans. Biomed. Eng. 66, 2390–2401. https://doi.org/10.1109/TBME.2018.2889705.
Sarker, V.K., Gia, T.N., Tenhunen, H., Westerlund, T., 2020. Lightweight security algorithms for resource-constrained iot-based sensor nodes. In: ICC 2020–2020 IEEE International Conference on Communications (ICC), pp. 1–7. https://doi.org/10.1109/ICC40277.2020.9149359.
Shofiyah, Z., Mahmudah, H., Santoso, T.B., Puspitorini, O., Wijayanti, A., Siswandari, N.A., 2022. Voice recognition system for home security keys with mel-frequency cepstral coefficient method and backpropagation artificial neural network. In: 2022 International Electronics Symposium (IES), pp. 497–501. https://doi.org/10.1109/IES55876.2022.9888507.
Shrestha, M., Xu, L., 2011. Efficient encoding for generalized reed solomon codes. In: 2011 IEEE 10th International Symposium on Network Computing and Applications, pp. 302–305. https://doi.org/10.1109/NCA.2011.52.
Singh, D.U., 2013. Error detection and correction using reed solomon codes. Error Detection and Correction Using Reed Solomon Codes 3.
Sonkar, K., Rani, R., 2021. Cancelable iris biometric: A review. In: 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), pp. 560–565. https://doi.org/10.1109/ICSCCC51823.2021.9478118.
Sudar, K.M., Deepalakshmi, P., Ponmozhi, K., Nagaraj, P., 2019. Analysis of security threats and countermeasures for various biometric techniques. In: 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES), pp. 1–6. https://doi.org/10.1109/INCCES47820.2019.9167745.
Thammasan, N., Fukui, K., Numao, M., 2016. Application of deep belief networks in EEG-based dynamic music-emotion recognition. In: 2016 Int. Joint Conf. on Neural Networks (IJCNN), pp. 881–888.
Thomas, K.P., Vinod, A.P., 2016. Biometric identification of persons using sample entropy features of eeg during rest state. In: 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 003487–003492. https://doi.org/10.1109/SMC.2016.7844773.
Tuncer, S.A., Kaya, T., 2018. True random number generation from bioelectrical and physical signals. https://doi.org/10.1155/2018/3579275.
Vishwanath, M., Jafarlou, S., Shin, I., Dutt, N., Rahmani, A.M., Jones, C.E., Lim, M.M., Cao, H., 2021. Investigation of machine learning and deep learning approaches for detection of mild traumatic brain injury from human sleep electroencephalogram. In: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), pp. 6134–6137. https://doi.org/10.1109/EMBC46164.2021.9630423.
Wan, B., Wang, Q., Su, K., Dong, C., Song, W., Pang, M., 2021. Measuring the impacts of virtual reality games on cognitive ability using eeg signals and game performance data. IEEE Access 9, 18326–18344. https://doi.org/10.1109/ACCESS.2021.3053621.
Wang, Y., Li, B., Zhang, Y., Wu, J., Yuan, P., Liu, G., 2020. A biometric key generation mechanism for authentication based on face image. In: 2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP), pp. 231–235. https://doi.org/10.1109/ICSIP49896.2020.9339252.
Yang, H., Mihajlovic, V., Ignatenko, T., 2017. Private authentication keys based on wearable device eeg recordings. In: 956–960In Proceedings of the 2017 25th European Signal Processing Conference (EUSIPCO).
Yin, X., Zhu, Y., Hu, J., 2021. A survey on 2d and 3d contactless fingerprint biometrics: A taxonomy, review, and future directions. IEEE Open J. Comput. Soc. 2, 370–381. https://doi.org/10.1109/OJCS.2021.3119572.
Zahid, A.Z., Mohammed Salih Al-Kharsan, I.H., Bakarman, H.A., Ghazi, M.F., Salman, H.A., Hasoon, F.N., 2019. Biometric authentication security system using human dna. In: 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), pp. 1–7. https://doi.org/10.1109/ICOICE48418.2019.9035151.
Zhang, S., Sun, L., Mao, X., Hu, C., Liu, P., 2021. Review on eeg-based authentication technology. Comput. Intell. Neurosci. https://doi.org/10.1155/2021/5229576.
Zheng, W.L., Lu, B.L., 2015. Investigating critical frequency bands and channels for EEG-based emotion recognition with deep neural networks. IEEE Trans. Auton. Ment. Dev. 7, 162–175. https://doi.org/10.1109/TAMD.2015.2431497.