Chapter

EEG Authentication System Using Fuzzy Vault Scheme

Fatima M. Baqer and Salah Albermany

Abstract

Authentication is the process of recognizing a user's identity by determining claimed user identity by checking user-provided evidence, combining cryptographic with biometric can solve many of security issues, including authentication. Our goal is to try to combine cryptography and biometrics to achieve authentication using fuzzy vault scheme. Electroencephalography (EEG) signals will be used as they are unique and also difficult to expose and copy; also they are difficult to be hack, using nine healthy persons' EEGs from the BCI Competition and extracting power features from signals spectrum of beta and alpha band of EEG signal, the extracted features are from three channels (C3, Cz, and C4), then support vector Machine (SVM) is used for classification. In this chapter, two tasks (left hand and right hand) are used from a four tasks in the dataset, and the system achieves 96.98% validation accuracy, using 10-fold cross-validation on the training set and the model is saved, after extract features, these features will used to be evaluated on a polynomial generated from the secret key using reed Solomon code and chaff points generated using tent map are added to hide the data, which create the final result that is the vault, for decoding the system using Lagrange interpolation for polynomial reconstruction and returning the key.

Keywords: fuzzy vault, EEG, brain wave, cognitive biometric, authentication, electroencephalogram

1. Introduction

User authentication is an important phase in security systems. Authentication is the determining process of a person is really, who claimed to be. Authentication technology affords the access to the systems after checking/verifying if a user's certification matches the authorized certification in a database, usually provided with an ID of a user, and authentication is achieved when the user provides a certification. Generally, authentications can be according to their use: password-based, token-based, and biometrics-based. Each of has its advantages and disadvantages [1].

Biometrics systems based on human being's measurements analyze statistic aspects of unique physical and behavioral characteristics, which can be consumed to identify or verify a human [2].

The term biometric is a Greek word, referring to bio means "life" and metric means "measurement." Biometrics is used to achieve reliable authentication and identification that can be expressed as face fingerprints, iris, retina, signatures, gait,

voice, etc. Recently, a new biometric field has gained its popularity because of its less drawbacks over other biometrics; it is the brain wave biometric or electroencephalography (EEG) [3].

However, without the drawbacks of both passwords-based and biometric-based, the EEG-based biometric authentication system combines their advantages [1]. EEG signals are dynamic, sensitive, and inexpensive and used to observe mental state that can be used to distinguish persons.

These signals can be bound with a cryptography to empower the security, a scheme that can be used with brain wave signals is called fuzzy vault scheme, key-based cryptographic scheme uses error correction codes to generate polynomials to secure the key.

1.1 Biometric concept

Biometric structure helps to find out the person with the physical-behavioral mechanism using statistics from person. [4], there are two types of biometrics: conventional and cognitive, conventional refers to physical and behavioral characteristics, such as fingerprint, voice, oder, DNA, face, iris, retina. Etc., cognitive refers to mental state signals as electroencephalography (EEG), these biometrics are unique for every individual. Physical biometrics is distinguished by "what the individual is" while behavioral is distinguished by "how individual do," cognitive is "what individual think" [5]. **Figure 1** illustrates biometric types.

1.1.1 Electroencephalogram (EEG)

Electroencephalogram, EEG for short, is the human brain's electrical activity. Nerve system of human, including the brain, consists of neurons, which are nerve cells. The electrical current transmitted signals by neurons to other neurons [6]. The changes in voltage resulting from the electrical current are then measured by electrodes. Patterns form waves used by EEG and are sinusoidal. Based on the frequency bandwidth can be classified into several bands. Each band of waves corresponds to different activities. Most common bands classification [6]: Delta (0.5–4) HZ, Theta (5–7) HZ, Alpha (8–15) HZ, Beta (16–31) HZ, Gamma(32-higher) HZ, the correspondence for each band, **Table 1** describes each band and its activity.

It is the measurement of electrical activity of the brain, sensor used to obtain these signals. Brain consists of millions of neurons, and these neurons express emotions and thoughts as signals [7].

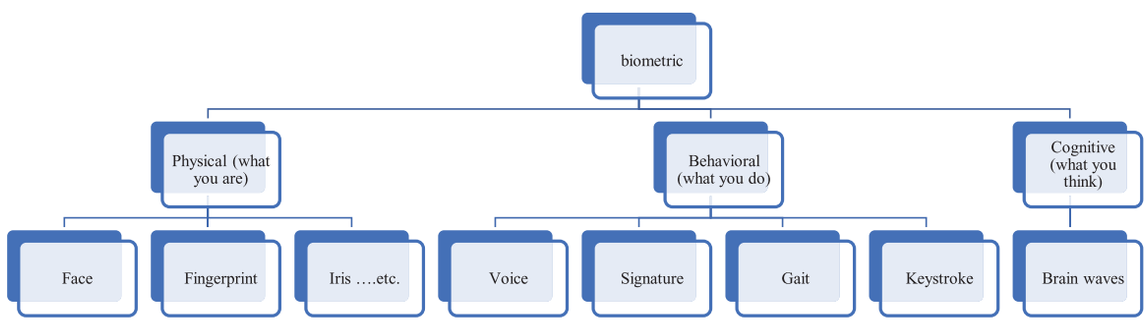


Figure 1.
Biometric types.

Band name	Range in HZ	Activity
Gamma	32–higher	Consciousness, higher processing tasks
Beta	16–31	Awake, active thinking, concentration and arousal states, eyes opened
Alpha	8–15	Relaxation, eyes closed
Theta	5–7	Drowsy, meditating and sleeping
Delta	0.5–4	Deep sleeping

Table 1.
EEG bands description.

"EEG measures the currents that flow during synaptic excitations of the dendrites of many pyramidal neurons in the cerebral cortex. Differences of electrical potentials are caused by summed postsynaptic graded potentials from pyramidal cells that create electrical dipoles between soma (body of neuron) and apical dendrites (neural branches) [5]."

The potentials are measured between two or more points called electrodes or sensors, which are placed on the scalp at different locations. EEG resembles waves, which is why the term brain waves is used when referring EEG signals. Padfield et al. [8], these EEG signals are unique for every individual and less exposed because it is under the scalp, which is hard to obtain and cannot be copied or manipulated [2].

Universality, uniqueness, permanency, performance, collectability, acceptability, and robustness satisfy the requirements of EEG-based biometric authentication method [7].

1.1.2 Motor imagery (MI)

MI is imagining a motor action without any efferent information to neuromuscular system. Thoughts and actions are intimately linked. A confirmation of this prediction is found in the spatial patterning of activated cortical areas seen with functional brain imaging techniques such as PET and fMRI [9]. MI is widespread in BCI systems because it has naturally occurred discriminative properties and also because signal acquisition is not expensive [8]. It is widely used in sport training as mental practice of action, neurological rehabilitation, and has also been employed as a research paradigm in cognitive neuroscience and cognitive psychology to investigate the content and the structure of covert processes (i.e., unconscious) that precede the execution of action. The effectiveness of motor imagery has been demonstrated in musicians. There have also been conducted multiple studies on its uses in neurological rehabilitation in patients after stroke [10].

1.2 Literature survey

1.2.1 EEG person authentication

Marcel and Millan [11] investigate the use of brain activity for person authentication, using a statistical framework based on Gaussian Mixture Models and Maximum a posteriori model adaptation. Intensive experimental simulations are performed using strict train/test protocols to show the potential of method [11].

Fladby [12] performs an experiment with 12 participants for eight different tasks in three sessions. They extract features from time and frequency domain by analyzing EEG and then the proposed algorithm is applied as dynamic time warping as well as a feature-based distance metric [12].

He [7] proposes an EEG feature hashing approach for person authentication, by extracting the coefficients of the autoregression model from multiple EEG channels, Fast Johnson-Lindenstrauss transform that is based dimension reduction algorithm to hash vectors. For person authentication, a Naive Bayes probabilistic model is applied [7].

Nguyen et al. [13] investigated the person verification based on brain wave features extracted from EEG signals of motor imagery tasks. For each subject, left, right, and best motor imagery tasks were used. As for modeling, the Gaussian mixture model (GMM) and support vector data description (SVDD) methods were used [13].

Nieves and Manian [14] proposed a system use an effective time-frequency-based feature extraction method using the short-time Fourier transform (STFT) or spectrogram. Computed features on the spectrogram were energy, variance, and skewness. These features were used to train a SVM and neural network classifier. Using cross-validation for testing data for person authentication the classifiers are tested. Results using a different number of channels with optimum features presented [14].

Soni et al. [2] "design a system and implement it, so that users set patterns as an unlock pattern to obtain the access's permission. This pattern can be any combination of eye blink, attention and various brain rhythms like Alpha, Beta, Theta and Delta. Provided two-level authentication. First level of which is brain waves. Once the correct pattern of brain signal is provided the system will ask for a pass key as a second level of authentication [2]."

Sjamsudin [15] "investigates the aspects of performance and time-invariance of EEG-based authentication. Two sets of experiments are done to record EEG of different individuals. The system implemented the use of machine learning such as SVM and deep neural network to classify EEG of subjects [16]."

1.2.2 Fuzzy vault

Juels and Sudan [16] propose a novel cryptographic construction scheme defined as a fuzzy vault. Alice is a player lock a secret value in a fuzzy vault and "lock" it, using a set of element A. using set B of the same length Bob will try to "unlock" the vault, he gets the secret only, if A and B overlap substantially [16].

Uludag et al. [17] explore the combination of fuzzy vault with the fingerprint minutiae data, which try to secure the important data using the fingerprint data, such that only the authorized user can access the secret by providing the valid fingerprint [17].

Nandakumar and Jain [18] use the fuzzy vault to secure a multi-biometric template derived from a person's templates. Exhibiting that a multi-biometric vault provides better recognition performance and higher security compared with a uni-biometric vault [18].

Khalil-Hani et al. [19] "propose a new chaff generation algorithm which is computationally fast and viable for hardware acceleration by employing simple arithmetic operations."[19].

You et al. [20] proposed cancelable fuzzy vault algorithm based on the user's transformed fingerprint features, which are used to generate a fuzzy vault [20].

1.2.3 Combining cryptography with EEG signals

Damaševilius et al. [21] "combine an EEG based biometric with the fuzzy commitment scheme and BCH error correcting for person. Evaluating features that are covariance matrix of EEG data using EEG recorded from 42 subjects. The experimental results present that the system can generate up to 400 bits of cryptographic key from the EEG codes, while tolerating up to 87 bits of error [21]."

2. The proposed system

2.1 Problem statement

With the rapid development of technology, large institutions and government institutions, which have sensitive information and also applications, need systems with high security and reliable authentication way that is hard to/or possible to copy or manipulate brain wave biometric has these proprieties, in authentication it is very important that people accept the system (acceptability). With this in mind it is safe to say that a noninvasive method of capturing brain wave signals is the best way for biometric acquisition as for securing these biometrics.

2.2 EEG dataset

In this chapter, the winning BCI competition Graz IV2a Dataset (2008) by burner is used [22], which is consists of nine subjects each performing four MI tasks randomly (this process called trial), each task is a class (left hand, right hand, foot, and tongue) corresponding to (1,2,3,4) respectively, the experiment is done by experts, with no feedback. For our system we use only left and right classes [22].

Each subject sat on comfortable armed chair in front of a computer screen at time (t = 0) a fixation cross appeared on the screen and a beep tone to alarm the subject, at (t = 2) a cue appear for 1.25 s in form of arrow that refers to one of classes (left, right, down, up) to inform the subject of the beginning of MI tasks this last until t = 6 the cue disappears and a break is followed [22].

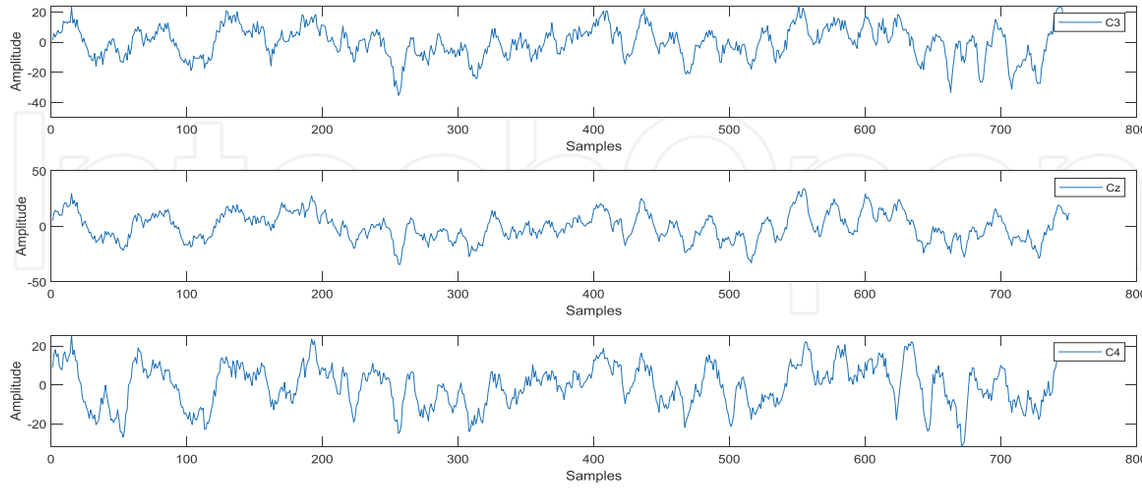
The dataset is divided into two sessions each in separate day, one for training and other for evaluation, each subject performs 48 trial (each class 12 trial) for 6 runs, yielding in total 288 trial [22]. The sampling rate of the signal is 250 Hz, a bandpass filter was applied between 0.5 Hz and 100 Hz. The sensitivity of the amplifier set to 100 μV, to suppress line noise, a 50 HZ notch filter was applied, and artifact trials were marked. The signals were recorded from 25 channels, 22 EEG, 3EOG [22].

2.3 Extraction of EEG trials

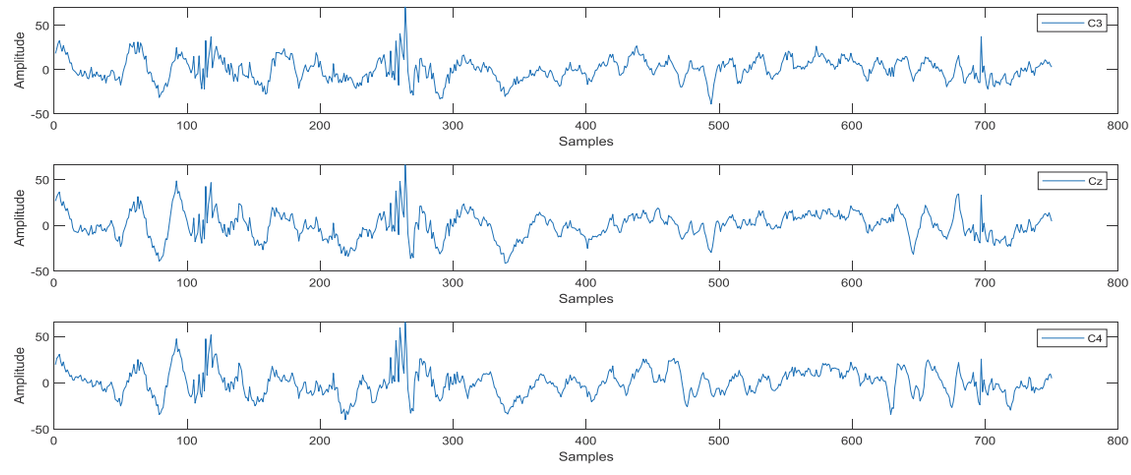
Extraction of EEG trials means the process of finding trial of interest of EEG signals by segment the signal according to the event associated with the dataset.

Events gives the time that the MI trail starts and ends to facilitate extraction of the task and the segment number, also the dataset that gives the artifact in each trial to eliminate it if need, in our case we need a clear signal so we eliminate these artifacts for the subjects. The proposed system segments the signals of each channel (C3, C4, Cz), these channels are the most effected by MI tasks. Also, because we use two classes only

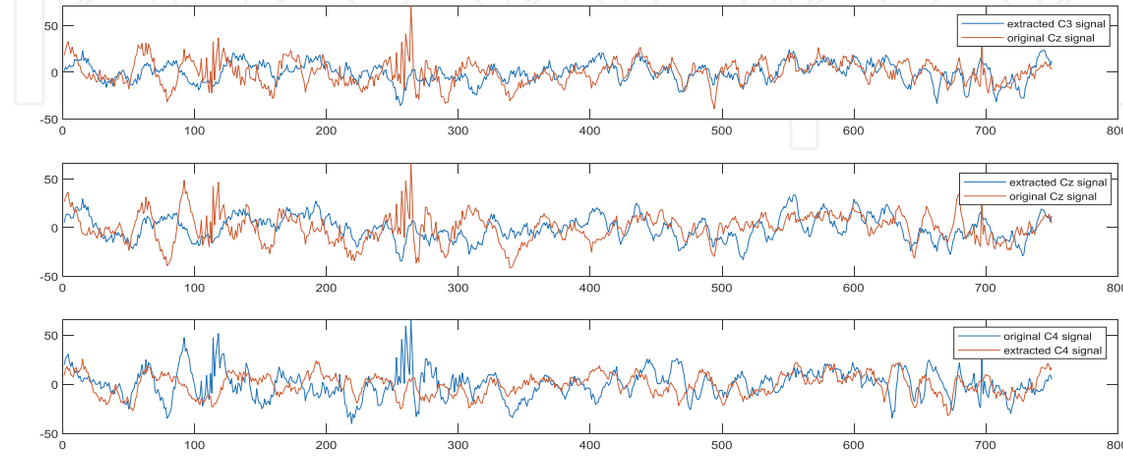
(left and right hand) the other two classes (feet and tongue) eliminated and their corresponding trials also eliminated. **Figure 2** shows the signal of C3 channel before and after segmentation for three trials.



(a)



(b)



(c)

Figure 2.
(a) Signal three channels before trials extraction; (b) signal after trials extraction (c) show the deference between original signal and extracted signal for three trial.

2.4 Artifact's reduction

Artifacts can be defining as the unwanted signals that appear in EEG signals, they can be caused from various origins including body or eye movement, heart beating blinking, or frequency from utility, which is (50 Hz in Europe or 60 Hz in the United States) [23]. The utility frequency was removed already by applying notch filter while eye artifacts are left due to possibility of artifacts removal algorithms testing [22].

To handle eye artifact, there are three main approaches: avoidance, rejection, and removal [23].

For artifacts avoidance can be by asking the user to avoid movement during the recording that causes EEG artifact, which decreases the artifact's number, but eye movement and blinks cannot be avoided.

Another way is to reject all corrupted trials by artifacts, which can automatically have done or manually. Manually can be done through visual examination, as the corrupted trials marked if they are corrupted or not by an expert. An algorithm is implemented in automatic artifact rejection, that can determine if artifacts corrupt a trial or not, and artifact rejection reduces the size of the training set. Last, is artifact removal, in order to remove the EEG signal artifact, some algorithms are used that leave the desired brain-originated signal intact.

2.5 Bandpass filtering

After applying segmentation algorithm to segment signals of each channel into 3 s sub signal according to the event associated with the data set then remove all marked artifact trials, **Figure 3** shows EEG signal for three trials after applying bandpass filter, the signal is filtered using a bandpass filter designed for a given frequency band. Using, for each channel, a 4th order Butterworth infinite impulse response (IIR) filter, IIRs are used to change the frequency component of a time signal by reducing or amplifying a particular frequency. This filter is used to pass only the band-limited portion of frequency content.

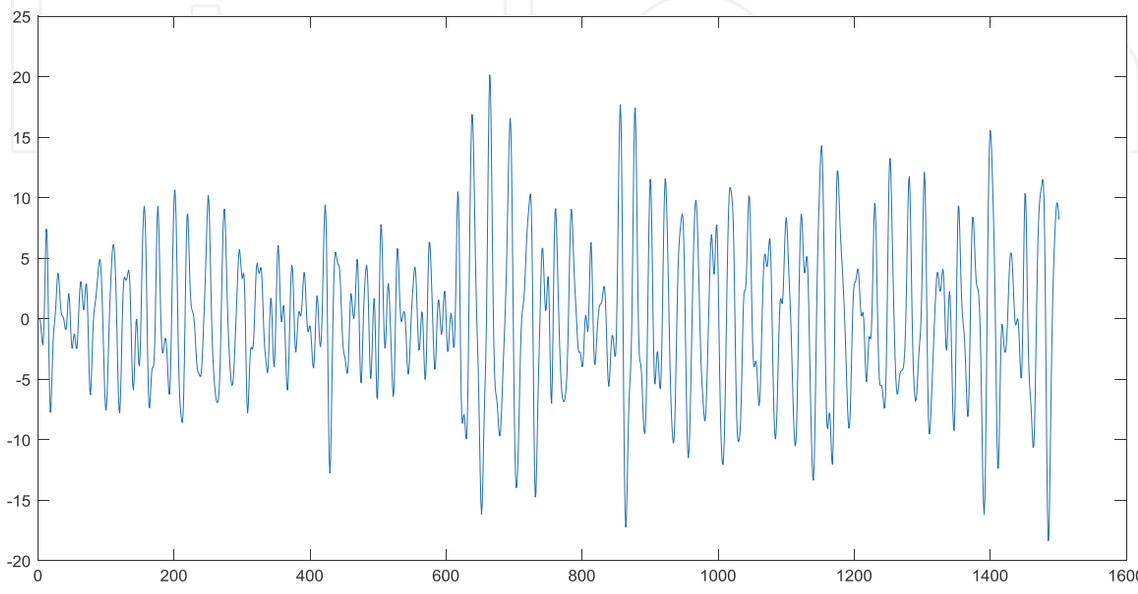


Figure 3.
Signal of C3 channel after applying bandpass filter between (8–30 HZ).

2.6 Feature extraction

The filtered signals are used to calculate spectrum PSD, in detail, estimate the PSD in the band between 8 and 30 Hz, this is based on the fact that the beta rhythm has distinct topographies and responses to the limb movements, compared with the alpha rhythm, the oscillatory power of the mu rhythm in the sensorimotor cortex ipsilateral to the tasks increased, while that of the beta rhythm in the contralateral sensorimotor cortex decreased simultaneously. The Welch's averaged used for spectral estimation that is a modified periodogram method. With 1 s Hamming window and 50% overlap, Welch's method can reduce noise. Each trial is divided into five bands and then the power and variance of each band are calculated, and energy of the whole trial is calculated.

2.7 Model building

The SVM method was used to train person EEG models using 10-fold cross-validation training and was used to train models on the whole training set and test on a separate test set.

SVM developed by Cortes and Vapnik [24] is a practical implementation of statistical learning theory capable of processing difficult problems of supervised learning, SVM is nonprobabilistic classifier; the two limitations of SVM are linear and binary features [25].

A decision boundary (plane) in SVM is used to separate the feature vectors. SVM classifier finds during training into two classes. The problem is to find the decision boundary (a linear hyperplane) that has the maximum separation (margin) between the two classes. The margin of a hyperplane is the distance between parallel equidistant hyperplanes on either side of the hyperplane such that the gap is void of data objects. The optimization during training finds a hyperplane that has the maximum margin. The SVM then uses that hyperplane to predict the class of a new data object once presented with its feature vector. See **Figure 4** [26].

2.8 Fuzzy vault

It is an updated version of the ideas of the fuzzy commitment scheme [27]. In this scheme, a message M is encoded as coefficients of a k-degree polynomial (p) using Reed Solomon code RS, in x (data points evaluated on polynomial(p)) over a finite

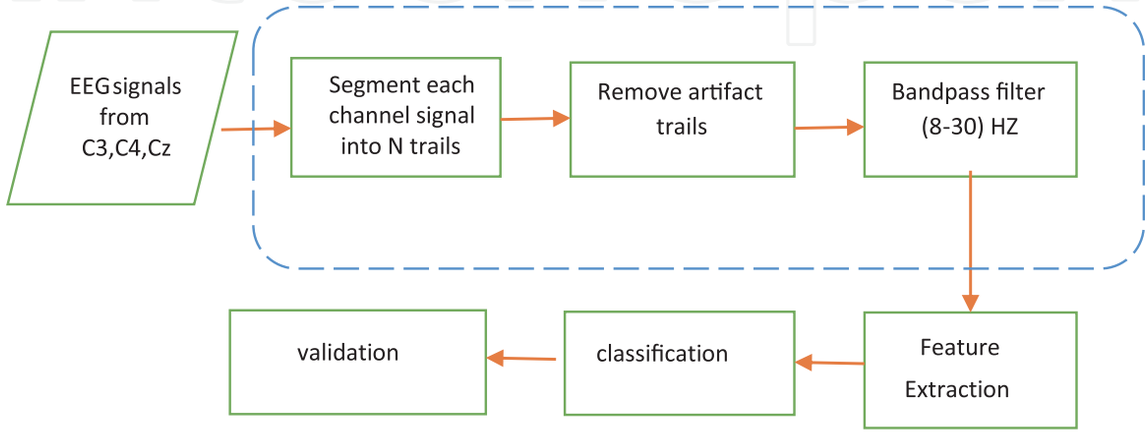


Figure 4.
Model building.

field *F_q*. Then the polynomial p is evaluated at the input data points (*X*) to calculate *p* (*X*) = *Y*. These (*X*, *Y*) pairs, known as genuine points, constructing the locking set, which become the vault later. False points (called chaff) are used to hide the identity of the genuine points, and then, they are added to the genuine points set. This is called vault, which is then stored. The difficulty of the fuzzy vault scheme is shown in polynomial reconstruction problem, which is to make it secure [28].

2.9 Lock the vault

Polynomial is generated by using the code results from encoding a polynomial coefficient called secret that is a secret value using RS. Every EEG feature is projected onto the polynomial. Then it creates the chaff points using the proposed tent chaff points. Then shuffling the two point sets, to produce the vault. As the following algorithm:

Input: Parameters k, t, and r where $k \le n \le r \le q$. A Pre-select Secret $S \in \mathcal{F}$. A locking set A=$\{a_i\}_{i=1}^{n}$ where $a_i \ \mathcal{F}$.
Output: A set R of points $\{(x_i, y_i)\}_{i=1}^{r}$ such that $x_i, y_i \in \mathcal{F}$
Variables :CH chaff points

$X, R \leftarrow \phi$
poly $(x) \leftarrow$ **RSENCODE**(S,k)
for i=1 to n do
$(\mathbf{x}_i; \mathbf{y}_i) \leftarrow (\mathbf{a}_i; \boldsymbol{poly}\ (\mathbf{a}_i))$;
CH $(\mathbf{x}_i; \mathbf{y}_i) \leftarrow$ chaff $(\mathbf{x}_i; \mathbf{y}_i)$;
$X \leftarrow sort\boldsymbol{x}_i$
$\boldsymbol{R} \leftarrow \mathrm{CH}(\mathbf{x}_i; \mathbf{y}_i) \bigcup (x_i, y_i)$
output $\boldsymbol{R}$

S: a secret key intended to protect.
poly (x): a polynomial of degree less than k.
$A = \{a_i\}_{i=1}^{n}$: a locking set containing n elements.
$\mathcal{F}$: finite field.
q: the number of finite field *F elements*.
n: the number of real points.
r: the total number of real points and chaff points.
Figure 5 illustrates feature projection on polynomial produced by encoding the secret s using RS, x_i is the featurea_i, and y_i is the projection on polynomial poly(a_i).

2.10 Tent-chaff points

After projection of the feature onto the polynomial p using features as:

$$p\left(f_q\right) = c_{d+1} \cdot {f_q}^{d+1} + c_d \cdot {f_q}^{d} + \ldots + c_1 \cdot f_q. \tag{1}$$

The genuine point list is comprised of:

$$\text{Genuine Points} = \begin{bmatrix} f_{q_1} & p\left(f_{q_1}\right) \\ \vdots & \vdots \\ f_{q_m} & p\left(f_{q_m}\right) \end{bmatrix} \tag{2}$$

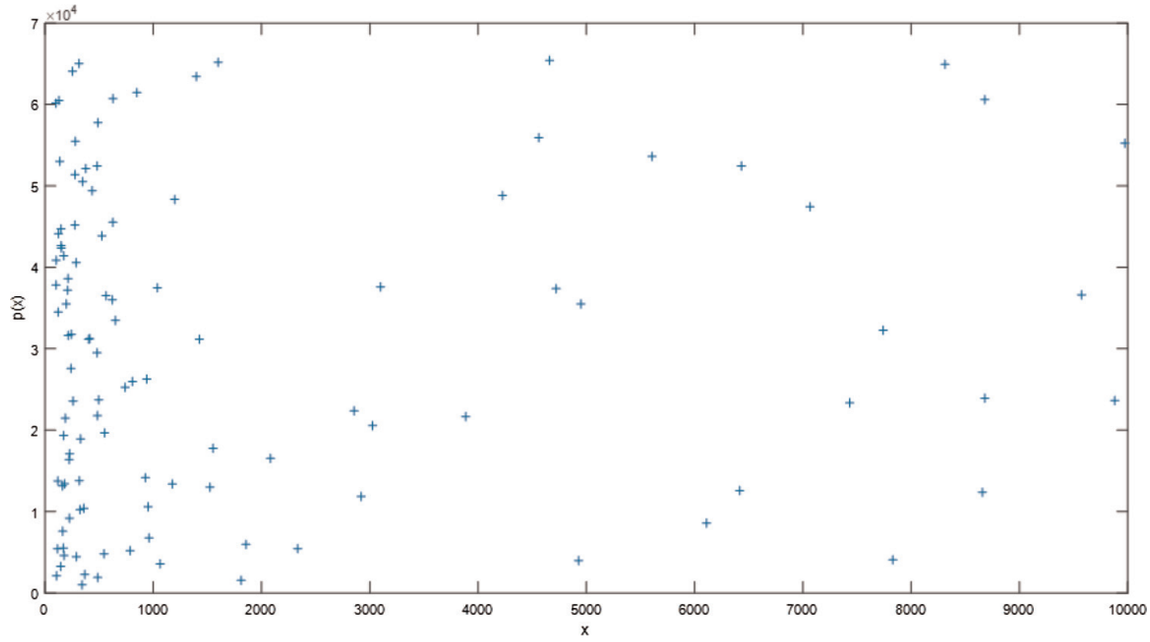


Figure 5.
Features projection on polynomial poly.

To mask the identity of true points, chaff points are added using chaotic tent map. Let μ be the seed, X_n = initial

$$x_{n+1} = \begin{cases} \mu x_n x_n \in [0, 0.5) \\ \mu(1 - x_n), x_n \in [0.5, 1] \end{cases} \tag{3}$$

Each chaff point and other genuine points do not need to put distance between them. The reason is that the chaff points are known for the two sides.

$$\text{Chaff Points} = \begin{bmatrix} Ch_{x_1} & Ch_{y_1} \\ \vdots & \vdots \\ Ch_{x_n} & pCh_{x_n} \end{bmatrix} \tag{4}$$

Finally, genuine Points and Chaff Points are combined, and the new matrix is shuffled. That represents fuzzy vault final matrix.

Figure 6 shows how chaff points hide genuine points; red circles in (a) are chaff points, (b) showing how attacker sees the final points projection.

2.11 Unlock the vault

The message vault is received and is attempted to decrypted it using input features produced from evaluation dataset. (X') are evaluated in the model build to identify the person in the vault pairs. If predicted person is the same as the original, then regenerate the chaff point set using the agreed seed and initial state for both parties and then remove the chaff points, after that from (x_i, y_i) pairs recover the message through polynomial reconstruction; otherwise reject;

Input: A fuzzy vault R,
Output: A value $S' \in \mathcal{F}^k$ $\{null\}$.
Variables : CH :chaff points,R :the vault ,Q:is the reconstructed polynomial
$Q \leftarrow \phi$
regenerate chaff points CH
for i = 1 to n do
Temp= CH(x_i, y_i)==R(x_i, y_i)
R(Temp)= []
Q=R
$Q \leftarrow Q\ (x_i, y_i)$
$S' \leftarrow$ **RSDECODE**(Q, k)
Output S' or null

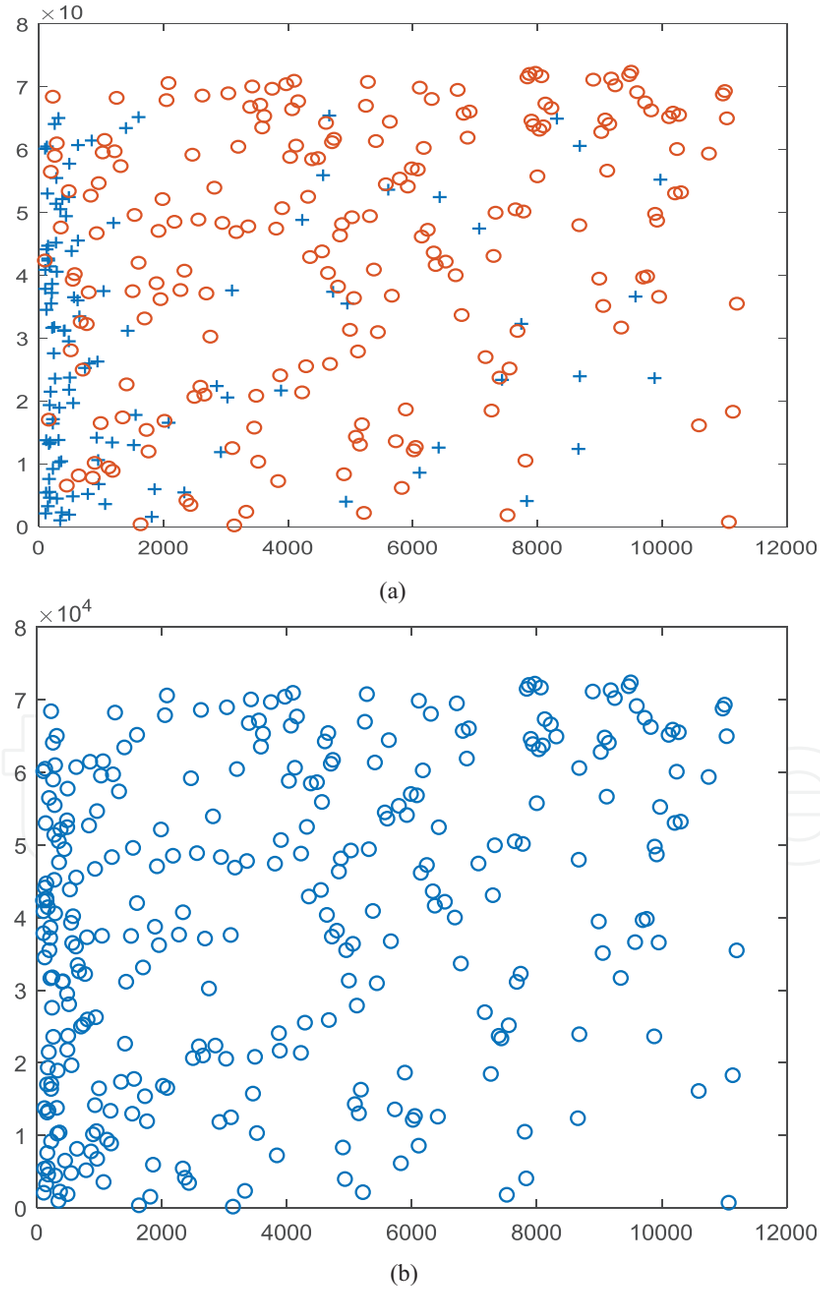


Figure 6.
How chaff points hide the polynomial.

2.12 Lagrange interpolation

It is a method used to reconstruct polynomials; it is a method that computes the interpolation polynomial to form the system:

$$Ax = b_i, \text{ where } bi = y, \ i = 0, \ldots, n, \tag{5}$$

"The A entries can be defined by $a_{ij} = p_j(xi)$, where $i, j = 0, \ldots, n$, and $x_i = x_0, x_1, \ldots, x_n$ are the points at which the data $y_0, y_1, \ldots, y_n$ are obtained, and $p_j(x) = x^j, j = 0, 1, \ldots, n$. The basis $\{1, x, \ldots, x^n\}$ of the polynomials' space of degree $n + 1$ is called the monomial basis, and the corresponding matrix A is called the Vandermonde matrix for the points $x_0, x_1, \ldots, x_n$, In Lagrange interpolation, the matrix A is simply the identity matrix, by virtue of the fact that the interpolating polynomial is written in the form:

$$p_n(x) = \sum_{j=0}^{n} y_i \mathcal{L}_{n,j}(x) \tag{6}$$

where the polynomials $\{\mathcal{L}_{n,j}\}, {}^{n}_{j=0}=0$ have the property that

$$\mathcal{L}_{n,j}(x_i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \tag{7}$$

The Lagrange polynomials for interpolation is: $\{\mathcal{L}_{n,j}\}$ where $j = 0, \ldots, n, x_0, x_1 \ldots, x_n$. are the interpolation points, they are defined by:

$$\mathcal{L}_{n,j}(x) = \prod_{k=0, k\neq j}^{n} \frac{x - x_k}{x_j - x_k} \tag{8}$$

3. Conclusion

After testing the system, it gives a good accuracy of classifying, which is 96%, but the run time of fuzzy vault authentication algorithm is kind of slow regarding that authentication must be fast to be practical for using it in real life; the reason of its slowness is because of the high number of EEG features, which result of many of multiple operations to compute Lagrange's interpolation that slow the work of the algorithm that make the algorithm impractical, on the other hand, using the tent chaff points gives the system an advantage because it reduces the error occurrence when separating chaff points from the genuine points, which are the EEG signal features because the initial seeds are known by both sender and receiver so, the system can regenerate the chaff points again and rise them without or less effecting the genuine points, and in the traditional chaff point generation, it needs to keep distance from the genuine point, which requires more calculation, which this method does not. Also we have difficulties in converting the features that are float numbers into integers so they can be used in Galois field, which needs integers to deal with, another problem is the repeated numbers produced from the conversion into integers because the features' values are close so they result in a repetition. The repeated values cannot use when reconstructing the polynomial because it results in division on zero, which is not acceptable because we need a unique number.

The system used nine healthy persons' EEGs from the BCI Competition and extracted features from signals spectrum of beta and alpha band of EEG signal, then extracted features from three channels and used support vector Machine (SVM) to classify two tasks left hand and right hand that achieve 96.98% validation accuracy, using 10-fold cross-validation on the training set and then saved the model, these features are evaluated on a polynomial generated from the secret key, then chaff points using tent map are added, which reduce the error; for decoding, we use Lagrange interpolation for polynomial reconstruction and returning the key.

To measure performance, a confusion matrix was calculated from which its precision and recall are calculated, a part from using the confusion matric to find precision and recall, it is important to analyze the result by the help of the confusion matrix to analyze the results as it also gives a very strong, it gives the evidence where your

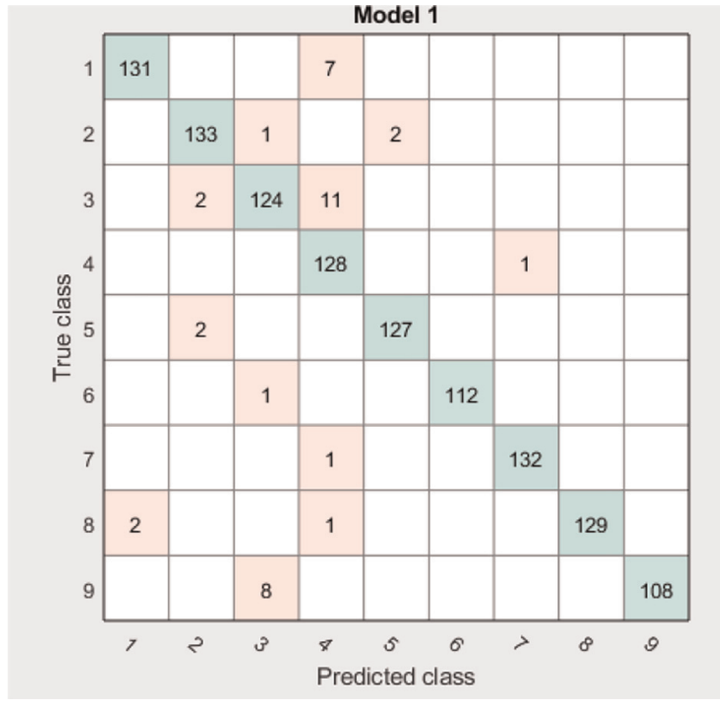


Figure 7.
Confusion matrix for the classification model.

Subject	TPR (%)	FNR (%)
1	95	5
2	98	2
3	91	9
4	99	1
5	98	2
6	99	1
7	99	1
8	98	2
9	93	7

Table 2.
TPR and FNR.

classifier is going wrong. So for our model, we can see that our classifier goes in the right direction, which means the classifier can distinguish between subjects' labels; **Figure 7** illustrates confusion matrix for nine subjects.

The total validation accuracy is 96.98%, from confusion matrix; also, one can calculate the true positive rate (TPR) and the false negative rate (FNR) as shown below, by observing the table; TPR is high and FNR is low, which means the performance at its best. See **Table 2**.

Author details

Fatima M. Baqer* and Salah Albermany
University of Kufa, Najaf, Iraq

*Address all correspondence to: fatimam.alkhersan@student.uokufa.edu.iq

References

[1] Pham T Ma W, Tran D, Tran DS, Phung DQ. A study on the stability of EEG signals for user authentication. In: 2015 7th International IEEE/EMBS Conference on Neural Engineering (NER). New Jersey: IEEE; 2015. pp. 122–125

[2] Soni YS, Somani SB, Shete VV. Biometric user authentication using brain waves. In: 2016 International Conference on Inventive Computation Technologies (ICICT). New Jersey: IEEE; 2016. pp. 1–6

[3] Story R. Using machine learning to improve motor imagery neurofeedback [master thesis[. Halifax, Canada: Dalhousie University; 2015

[4] Sujitha V, Chitra DR. A novel technique for multi biometric cryptosystem using fuzzy vault. Journal of Medical Systems. 2019;**43**:1-9

[5] Reshmi K, Muhammed PI, Priya VV, Akhila V. A novel approach to brain biometric user recognition. Procedia Technology. 2016;**25**:240-247

[6] Sharma M, Atri ES. A review on cryptography mechanisms. International Journal of Computer Technology and Applications. 2011;**2**(4):1048-1050

[7] He C. Person authentication using EEG brainwave signals [unpublished master's thesis]. 2009

[8] Padfield N, Zabalza J, Zhao H, Masero V, Ren J. EEG-based brain-computer interfaces using motor-imagery: Techniques and challenges. Sensors. 2019;**19**(6):1423

[9] Yüksel A. Classification Methods for Motor Imagery Based Brain Computer Interfaces [thesis]. Istanbul Technical University; 2016. p. 21

[10] Hlinka M. Motor Imagery Based Brain-Computer Interface Used in a Simple Computer Game. Brno, Czechia: Masaryk University Faculty of Informatics; 2017

[11] Marcel S, Millán JDR. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2012;**29**(4):743–752. DOI: 10.1109/TPAMI.2007.1012

[12] Fladby K. Brain wave based authentication [master thesis]. Gjøvik, Norway: Gjøvik University College; 2008

[13] Nguyen P, Tran D, Le T, Huang X, Ma W. EEG-based person verification using multi-sphere SVDD and UBM. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin, Heidelberg: Springer; 2013. pp. 289-300

[14] Nieves O, Manian V. Automatic person authentication using fewer channel EEG motor imagery. In: 2016 World Automation Congress (WAC). New Jersey: IEEE; 2016. pp. 1-6

[15] Sjamsudin FP. EEG-based authentication with machine learning. 2017

[16] Juels A, Sudan M. A fuzzy vault scheme. Designs, Codes and Cryptography. 2006;**38**:237-257. DOI: 10.1007/s10623-005-6343-z

[17] Uludag U, Pankanti S, Jain AK. Fuzzy vault for fingerprints. In: International Conference on Audio-and Video-Based Biometric Person

Authentication. Berlin, Heidelberg: Springer; 2005. pp. 310-319

[18] Nagar A, Nandakumar K, Jain AK. Securing fingerprint template: Fuzzy vault with minutiae descriptors. In: 2008 19th International Conference on Pattern Recognition. New Jersey: IEEE; 2008. pp. 1-4

[19] Khalil-Hani M, Marsono MN, Bakhteri R. Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. Future Generation Computer Systems. 2013;**29**(3):800-810

[20] You L, Wang Y, Chen Y, Deng Q, Zhang H. A novel key sharing fuzzy vault scheme. KSII Transactions on Internet and Information Systems. 2016; **10**:4585-4602

[21] Damaševičius R, Maskeliūnas R, Kazanavičius E, Woźniak M. Combining cryptography with EEG biometrics. Computational Intelligence and Neuroscience. 2018;**2018**:1-11

[22] Brunner C, Leeb R, Müller-Putz G, Schlögl A, Pfurtscheller G. BCI Competition 2008–Graz data set A. Institute for Knowledge Discovery (Laboratory of Brain-Computer Interfaces), Graz University of Technology. 2008;**16**:1-6. Available from: http://www.bbci.de/competition/iv/desc_2a.pdf

[23] Fatourechi M, Bashashati A, Ward RK, Birch GE. EMG and EOG artifacts in brain computer interface systems: A survey. Clinical Neurophysiology. 2007;**118**(3):480-494

[24] Cortes C, Vapnik V. Support-vector networks. Machine Learning. 1995; **20**(3):273-297

[25] Hetal B, Ganatra AMIT. Variations of support vector machine classification technique: A survey. International Journal of Advanced Computer Research. 2012;**2**(6):230-236

[26] Bridgelall RPHD. Introduction to Support Vector Machines. Lecture. 2017. p. 1

[27] Jain AK, Ross AA, Nandakumar K. Introduction to Biometrics. Berlin: Springer Science & Business Media; 2008. pp. 1–22

[28] Gui Q, Jin Z, Xu W. Exploring EEG-based biometrics for user identification and authentication. In: 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB). Philadelphia, PA, USA: IEEE; 2014. pp. 1–6