Journal of AI and Data Mining
Vol 8, No 3, 2020, 343-356.
DOI: 10.22044/JADM.2020.7858.1923

Development of a Unique Biometric-based Cryptographic Key Generation with Repeatability using Brain Signals

M. Zeynali, H. Seyedarabi* and B. Mozaffari Tazehkand

Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran.

Received 18 December 2018; Revised 02 December 2019; Accepted 27 January 2020
**Corresponding author: seyedarabi@tabrizu.ac.ir (H. Seyedarabi).*

Abstract
Network security is very important when confidential data is sent through a network. Cryptography is the science of hiding information, and a combination of cryptography solutions and cognitive science starts a new branch called cognitive cryptography that guarantees the confidentiality and integrity of the data. Brain signals, as a biometric indicator, can be converted to a binary code, which can be used as a cryptographic key. In this paper, we propose a new method for decreasing the error of the electroencephalogram-based key generation process. Discrete Fourier transform, discrete wavelet transform, autoregressive modeling, energy entropy, and sample entropy are used to extract the features. All features are used as the input of the new method based on the window segmentation protocol, and then are converted to the binary mode. We obtained the 0.76% and 0.48% mean half total error rate (HTER) for the 18-channel and single-channel cryptographic key generation systems, respectively.

Keywords: *Security, Cryptography, Electroencephalogram, Biometric cryptosystem.*

1. Introduction

The traditional cryptography is a science that uses symmetric or asymmetric techniques to hide information, and by executing various protocols, ensures the confidentiality and integrity of the data [1]. Almost any algorithm uses a sequence of bits (keys) with a specific length to guarantee the computational security of the algorithm or encryption method used. In the traditional Shannon information theory, the best cryptographic keys are random keys. Such algorithms are very secure but do not allow the cryptographic process to be related to the biometric information of individuals [2]. It is really difficult to remember long and random keys, and also storing them in a database will cause security problems [3].

A secure storage of keys is an important responsibility, and a key management is often the weakest part of many systems. Private keys must be kept secret, and here, biometric technologies can help [4]. The biometric methods have solved the problem of remembering the old keys, and because they are not required to be kept or written, it is hard to fake, copy, and share these keys in comparison with the old passwords and pin codes [3]. The biometric indicators are the physiological properties of the human body or behavioral characteristics [5]. These indicators should be measurable, unique, and unreplictable, and should remain constant for a reasonable period of time [6, 7].

In the recent years, there have been a few research works in the fields of cognitive informatics and computer security. The analysis of progress in many cognitive informatics departments shows that these sections contribute to the development of contemporary cryptography, and can even be used to create the fields that combine the algorithms that guarantee the confidentiality and integrity of the data with the biometric information of people. Such a combination has created a branch of computer science called cognitive cryptography [2].

One of the cognitive cryptographic applications available to prevent data leakage is the use of personal cryptography and the application of

biological models or biometric information for various security tasks. The most important example is the generation of personalized cryptographic keys for the symmetric or asymmetric encryption known as biometric encryption [8]. Encryption is a process that securely attaches a digital key to a biometric or generates a biometric key.

In principle, the key is "encrypted" with a biometric and stored. If a correct biometric representation is provided, the digital key will be "decrypted" when it is checked. This encryption/decryption process is obscure because the biometric sample is different from the encryption key in normal cryptography at any time. An important technological challenge is that despite the natural change in the biometric input, a digital key will be re-created [9].

The traditional biometric indicators are based on iris patterns [10] facial features [11], fingerprints, and audio features. However, using spoof attacks, these attributes can easily be falsified [12]. Recently, attention has been drawn to the use of electrical medical signals for biometric applications. An example of these signals is the electroencephalographic (EEG) signal [13].

An EEG signal is an electrical record of brain activity that is known as voltage fluctuation due to ionic flow within the brain neurons [14]. The EEG signals can be recorded using electrodes placed on the scalp (non-invasive).

The EEG signals are divided into five standard sub-bands: the Delta (1-4 Hz), Theta (4-8 Hz), Alpha (8-12 Hz), Beta (12-30 Hz), and Gamma (30-44 Hz) frequencies [15]. Since the EEG signals are generated from the electrical field by pyramidal cells of the cortex, they belong to the physiological characteristics and can be classified as biometric behavioral characteristics based on the visual or emotional stimuli [13].

The traditional biometric indicators like iris pattern, fingerprint, sound, hand geometry, and facial recognition used in biometric cryptographic systems have a limited number of features (for example, each person only has ten fingerprints, two irises, and one face); with the loss of these features, there is no other alternative. This problem is solved by the cancelable systems [3]. Ratha *et al*. have first introduced the concept of "cancelable biometric". It consists of distortions on the biometric features based on a chosen transform to provide different versions of a biometric template [16].

Some of the practical reasons for using brain signals to generate encryption keys are as follow:

1. Physical unclonable function (PUF): Neurons in the brain have unique connections for each subject and end in a different pattern from EEG, even if they have the same mental activity.
2. Revocable: The EEG signals do not require a cancellable transformation of the biometric template to provide revocability. The key is generated using EEG derived from a particular mental activity, and if the key is at risk, by changing the mental activity, a new key can be generated using another mental activity.
3. Entropy: Biometric EEGs measured across the population have a high entropy and raise the level of uncertainty in the key from the enemy's perspective.
4. Coercion attack: Since the brain signals depend on a person's state such as stress, it is not possible to obtain a key by force and pressure [3].

Only a few research works have studied the possibility of generating cryptographic keys from brain signals. K.V.R Ravi *et al*. have used a method based on event-related brain signals for data encryption. The idea is to shuffle the Huffman tree using a cryptographic key generated by EEG signals recorded when the user perceives a common black and white line picture [17].

Palaniappan *et al*. have introduced one of the early ideas about the use of EEG for PIN generation. Their system was based on the P300-based BCI, which included an external visual stimulus. They considered the Cz electrodes to be suitable for a limited number of experiments [18].

Lokeshwai *et al*. have introduced a new approach to data security that combines the concept of EEG, genetic algorithm, and pseudo-random binary sequences. For the key generation step, the extracted features of EEG are compressed using SPIH (Set Partitioning in Hierarchical Trees) for an efficient bandwidth usage, and are given as inputs to the pseudo-random generators. This system has been proposed as a theoretical idea with less analysis for implementation [19].

Akhila *et al*. have proposed a set of independent components that combine the characteristics of several regions of the brain. In this work, the Principal Component Analysis (PCA) was used as the feature extraction algorithm. They also introduced the key generating techniques using the EEG signals. The system is heavily influenced by emotions [20].

Garima Bajwa *et al*. have introduced the cryptographic key generation system, which in the first step, uses the EEG signals for authentication, and in the second step, key generation involves feature selection using normalized thresholds and segmentation window protocol. In this system, the discrete Fourier transform and discrete wavelet

transform were used for the feature extraction process. Finally, the mean Half Total Error Rate (HTER) for generating cryptographic keys from 18 electrodes was 4.53% [3].

The recent published papers propose robust features to emotion and epilepsy based on the EEG signals. Dang Nguyen *et al*. have studied the influence of emotions on EEG- based key generation systems. The experimental results showed that emotion had impacts on the accuracy of EEG-based cryptographic key generation. The accuracy of the system was at a maximum of 97.88% for 16 channels selected from the DEAP dataset [21].

Dang Nguyen *et al* also studied the influence of epilepsy on the EEG-based key generation systems and showed that epilepsy had impacts on the generated keys. They could achieve a minimum equal error rate of 2.10% for epileptic and 8.27% for the normal people using the EEG signal and Gama band, respectively [22].

1.1. System overview

EEG-based cryptographic key generation consists of the following steps, as shown in figure 1.

Enrolment: Before the key can be successfully generated by the system, the biometric indicators must be collected, processed, and stored. The quality of the stored biometric data is important for the next steps; usually, several biometric examples are used for registration, and the main template is created for the user, and is located in the template storage or database system. This process is called enrolment in the biometric systems [23].

Key generation: The key generation step does not require to store the original biometric data, and it receives the EEG signals generated from mental activity, and then extracts the appropriate features and produces appropriate feature vectors. Feature vectors are converted to the binary mode in order to generate valid keys by using the templates in the template storage. After applying the hash functions, the generated key is compared with the generated key at the enrolment step to accept or reject.

For the first time, Bajwa and Dantu proposed a new method for generating the cryptographic keys from an individual's EEG signals, while a subject performed certain mental tasks to provide portable cognitive keys with a possibility of regeneration even on mobile devices. In order to achieve this goal, the system must have the least error.

In this paper, we introduce a new method based on the window segmentation protocol for cryptographic key generation and add a new parameter to this protocol for decreasing the error rate of the system. The software used for implementation in this paper is Matlab R2018a.

2. Methods

2.1. Experimental data

The dataset used in this work was taken from UC Irvine Machine Learning Repository. In this experiment, there were two groups of subjects: alcoholic and control. Each subject was exposed to either a single visual stimulus (S1) or to two stimuli (S1 and S2). In the case of the second stimulus (S2), it was presented in either a matched condition, where S1 was identical to S2 or in a non-matched condition where S2 differed from S1.

The duration of each picture stimulus in each test trial was 300 ms. The interval among each trial was fixed to 3.2 s. The occurrence of matching and non-matching stimuli were randomized. The dataset

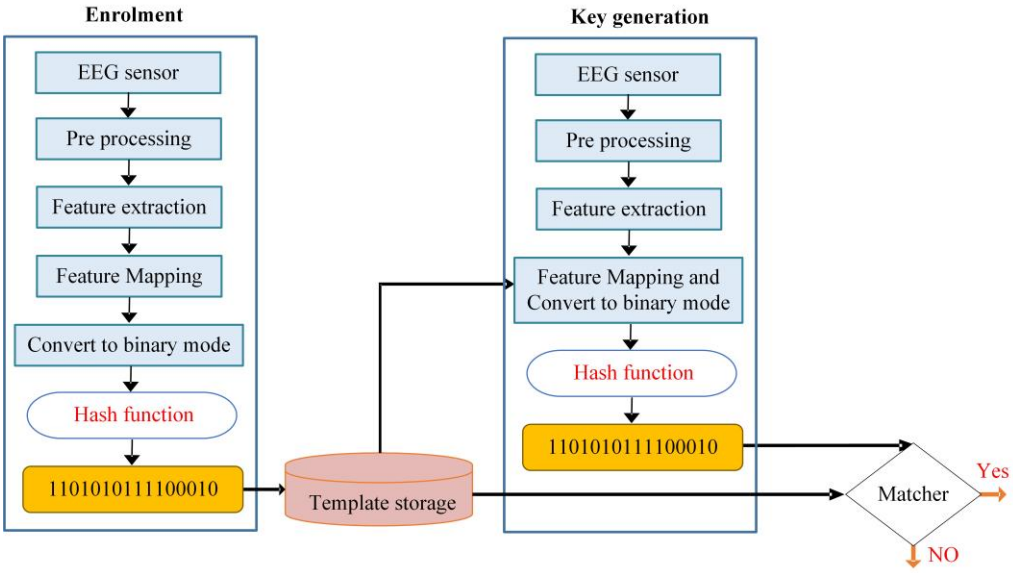


Figure 1. Flow of key generation from EEG of the subjects.

contained EEG measurements from 64 electrodes placed on a subject's scalp at a sampling rate of 256 Hz for a 1-second duration. There were 122 subjects, and each subject completed 120 trials of the three visually evoked stimuli presented in a random fashion. The data was recorded in a sound-attenuated RF shielded room with the subject seated in a reclining chair.
The signals were amplified with a gain of 10,000 by EpA2 amplifiers with a bandpass between 0.02 and 50 Hz. Data readings involving eye and body movements (> 73.3 μV) were rejected as noise [3, 24]. We removed the data of two subjects as the EEG signals were noisy and contained many error trials.

2.2. Feature extraction process

Feature extraction can be considered as a mapping from the original space to the space of features in which new samples of different classes can be distinguished better.

2.2.1. Fourier transform and power spectrum density

Fourier transform is one of the non-parametric feature extraction techniques for EEG signals. The discrete Fourier transform of the EEG signal can be obtained according to (1).

$$S(\mathrm{k}) = \sum_{n=0}^{N-1} S(\mathrm{n})\, \mathrm{e}^{-j\frac{2\pi}{N}nk} \quad \mathrm{k} = 0,1,2,..,\mathrm{N}\text{-}1 \qquad (1)$$

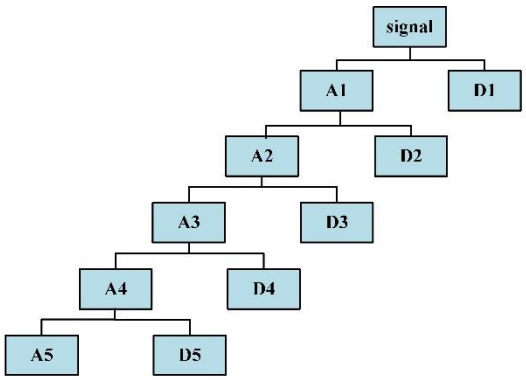
where, S(k) represents the k-factor of the discrete Fourier transform [5] and N represents the number of signal samples.
One of the most common signal representations in the frequency domain is the analysis of the signal power spectrum, so the spectrum estimation discussion is one of the most commonly discussed issues in defining and extracting the features of the signal.
Previous researches have shown that there is a clear difference in the shape of the EEG signal power spectrum of different individuals, which have led the power spectrum to be one of the most important features used in most studies in the biometric field of the EEG signal [13].
The power spectral density of EEG signals can be estimated directly from (2) [5].

$$P_s(k) = \frac{1}{N}\left|S(k)\right|^2 \qquad (2)$$

The EEG signals are divided into five standard sub-bands frequencies. In this paper, the time-domain signals were converted to the frequency domain using Fast Fourier transform (FFT), which is an efficient algorithm for calculating DFT.
FFT was applied to all channels, and the frequency spectrum was obtained. Then by averaging this value on the EEG standard bands, five features were obtained for each channel. The power of each frequency band from 1 to 44 Hz was also calculated.

2.2.2. Wavelet transform

In this work, Discrete Wavelet Transforms (DWT) from the Daubechies family of wavelets were used to extract the features. The general decomposition of the signal into its detailed and approximate coefficients was achieved by applying a series of high and low-pass filters to the signal.
Unlike FFT, DWT displays a time-frequency representation of the signal and helps in analyzing the signals with discontinuity or severe changes. Daubechies's versions of "db4", "db6", and "db8" were compared, and "db8" was found to be more suitable for recording the significant changes in the EEG signals [3].
Relationship between the EEG signal bands and wavelet decomposition tree are shown in figure 2.



Energy Bands	Frequency range(Hz)	Decomposition level
Delta	(0 - 4)	A5
Theta	(4 - 8)	D5
Alpha	(8 - 16)	D4
Beta	(16 - 32)	D3
Low gamma	(32 - 64)	D2
High gamma	(64 - 128)	D1

Figure 2. Relationship between the EEG band and wavelet decomposition tree [25].

In order to derive the feature by the DWT method, instead of using all the coefficients at each decomposition level, the following statistical information was extracted from the wavelet coefficients at each level.

- Mean of the absolute value of the coefficients at each level.

- Average power of wavelet coefficients in each sub-band.
- Standard deviation of coefficients in each sub-band.

2.2.3. Autoregressive modeling

In autoregressive modeling, the value of a signal in each moment is defined as a linear combination of the signal amount in a previous moment with the effect of white noise. The mathematical expression x [k] is modeled as (3).

$$x[k]=\sum_{i=1}^{p}\alpha_i x[k-i]+e[k] \quad (3)$$

In (3), e[k] is the gaussian white noise. Parameters of the model are the coefficients of this linear combination (α_i). These coefficients are directly considered as the features [26]. In this paper, using the search method, p = 10 was selected.

2.2.4. Log energy entropy

This feature can clearly illustrate the complexity of the signal in time, and shows the spectral feature of the signal. That is why it can be used as a feature.
If $E(0)\ E(1),\dots,E(N-1)$ represent the distribution of energy in N samples of the spectrum in each frequency band, the probability distribution function denoted by $P(E)$ can be defined as:

$$P_i(E)=\frac{E(i)}{\sum_{m=0}^{N-1}E(m)} \quad (4)$$

The Log energy entropy of *E* can be obtained from [27]:

$$logEn=-\sum_{i=0}^{N-1}\left(log_2\left(P_i(E)\right)\right)^2 \quad (5)$$

2.2.5. Sample entropy

Sample entropy is a revised version of the approximate entropy, and is less sensitive to noise; it can be applied for the short-length time series data. This entropy can be expressed as the negative logarithm of the probability of two sequences that are similar in m points, with the condition that they remain similar at the next point, where self-matches are not included in calculating the probability.
This similarity is calculated by considering the tolerance $\pm r$. In order to calculate the sample entropy, the time series $\{u(j)\ 1\le j\le N\}$ is expressed in an m-dimensional space with vectors of length m, as follows:

$$\left\{x_m(\mathrm{i})=\left[u(\mathrm{i}+\mathrm{k})\right]_{k=0}^{m-1},\ \mathrm{i}=1,..\mathrm{N}-\mathrm{m}+1\right\} \quad (6)$$

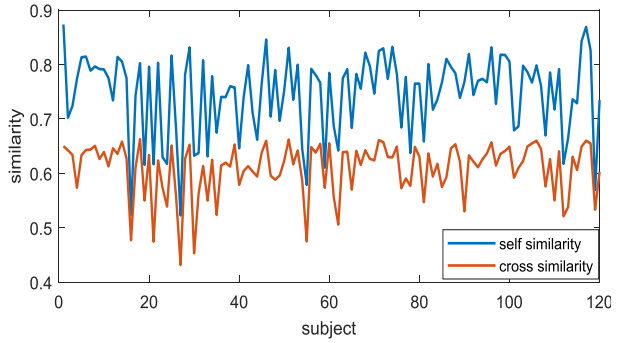
For vectors with length m, $-B^m(r)$ is the probability of sharing two sequences in m points, and is obtained by counting the average number of vectors with Euclidean distance less than $\pm r$. (In this paper, the value of r is 0.1.)
The same procedure was repeated by adding a unit to the vector $m \leftarrow m+1$, and similar to the probability $B^m(r)$ at this stage, calculating the probability of $-A^n(r)$ for $n \leftarrow m+1$ [28].

$$SampEn(\mathrm{m},\mathrm{r},\mathrm{N})=-\ln\left(\frac{A^n(\mathrm{r})}{B^m(\mathrm{r})}\right) \quad (7)$$

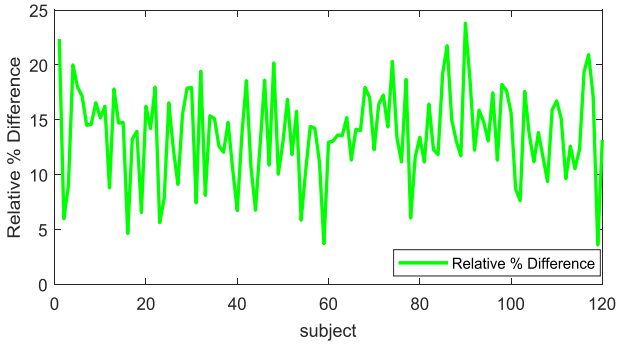
2.3. Feature analysis

In order to assess the effectiveness of signals in the generation of cryptographic keys, it is necessary to detect signals from one subject among other people.
The similarity between the two signals is used as a criterion for illustrating this issue. Similarity gives a value between 0 and 1; when the similarity is 1, it represents a complete match.
Self-similarity shows the similarity between the signals registered from one subject, while cross-similarity shows the similarity between the signals of different people. The hypothesis is that self-similarity in all tasks should always be more than a cross-similarity for all individuals. If this hypothesis is correct, the authentication system will be able to confirm the identities of the individuals. The key generation system will be able to generate unique keys for each person [29].
The difference between self-similarity and cross-similarity is used as a criterion with the name of the relative percentage difference to measure the degree of differentiation.
The more distinguished signals have a higher relative percentage difference. Equation (8) represents a general mode for determining the similarity between the two feature vectors A and B based on the cosine distance [3].

$$\text{similarity}=\frac{\mathbf{A}.\mathbf{B}}{\|\mathbf{A}\|.\|\mathbf{B}\|}=\frac{\sum_{i=1}^{n}\mathbf{A}_i\times\mathbf{B}_i}{\sqrt{\sum_{i=1}^{n}\mathbf{A}_i^2}\times\sqrt{\sum_{i=1}^{n}\mathbf{B}_i^2}} \quad (8)$$



(A)



(B)

Figure 3. Self-similarity and cross-similarity (A) relative percentage differences (B) scores obtained across each subject.

In figure 3.A, the highness of self-similarity compared to cross-similarity indicates that the similarity between the extracted features of one subject's signals is greater than the similarity between the extracted features of different person's signals. The higher the relative percentage difference, the more distinguishability of the extracted features of the signal. A high distinguishability means that the extracted features are suitable for the cryptography key generation (figure 3.B).

3. Key Generation

In this work, a method was used for the biometric-based key generation process, which is an extended version of the method used by G. Bajwa *et al*. [3]. This work also expands the methods used by Y.-J. Chang *et al*. [30] and F. Monrose *et al*. [31].

3.1. Feature mapping

Initially, feature vectors are extracted for all electrodes, tasks, and subjects, and then feature vectors for generating keys are calculated as (9) for each electrode.

$$feature\,vector = \frac{(\delta^3 + \theta^3 + \alpha^3 + \beta^3 + \gamma^3)}{(\delta + \theta + \alpha + \beta + \gamma)} \qquad (9)$$

Here, α, β, γ, δ, and θ represent the values for the features of the standard frequency bands of EEG.

The distribution of feature vectors for each subject, activity, and electrode is computed using the training dataset, and the parameters such as the standard deviation $\sigma_{sub,feature}$ and mean $\mu_{sub,feature}$ are obtained using these distributions. Also for the feature vectors of an electrode of the training set for all subjects, the global standard deviation σ_{global}, the global mean μ_{global} and its global distribution is calculated.

The global distribution width is obtained using the global standard deviation and the global mean calculated for the distribution of the training datasets for each task and electrode using (10).

$$window\,start = \mu_{global} - k\_seg \times \sigma_{global}$$
$$window\,end = \mu_{global} + k\_seg \times \sigma_{global} \qquad (10)$$

k_seg is a criterion used for determining the width of global feature distribution, and with increase in this criterion, the distribution width is increased.

The interval bins for each subject's feature vectors (features of an electrode) were derived in the global distribution using the authentication region of each subject's feature vector.

$$Auth_{reg\_interval} = (\mu_{sub,\,feature} - k_{sub,\,feature} \times \sigma_{sub,\,feature}, \mu_{sub,\,feature} + k_{sub,\,feature} \times \sigma_{sub,\,feature}) \qquad (11)$$

The maximum value for $k_{sub,feature}$ is obtained using the distinguishability criterion calculated in (12).

$$k_{sub,\,feature} = \left(\frac{\mu_{global,\,feature} - \mu_{sub,\,feature}}{\sigma_{sub,\,feature}} \right) \qquad (12)$$

The number of bins can be obtained from (13).

$$number\,of\,segment = \left[\frac{window\,end - window\,start}{Auth_{reg\_interval}} \right] + 1 \qquad (13)$$

Each feature vector (feature vectors of a single electrode) is mapped from the training set to a bin of global distribution.

$$if\left(FV \geq \left(window\,start + index \times Auth_{reg\_interval}\right)\right)\&$$
$$\left(FV \leq \left(window\,start + (index+1) \times Auth_{reg\_interval}\right)\right) \qquad (14)$$

The *index* in (14) is the index of the mapped bin. For each subject and electrode, the most frequent *index* is selected as Ar.

For each subject and electrode, the extracted patterns from the above steps are stored in the template storage. The templates are the *number of*

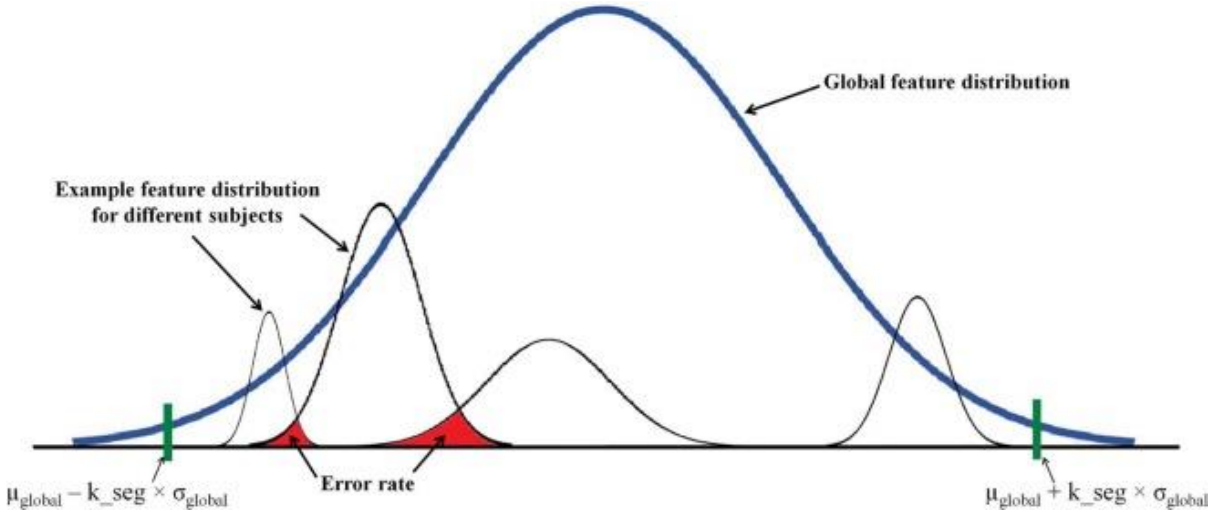


Figure 4. An example of key generation process from the global feature distribution of an electrode for a subject[3,26].

segment, Ar, Authreg- interval, window start and do not require the original biometric data to be stored. An example of a key generation process from the global feature distribution of an electrode for each subject is shown in figure 4.

3.2. Proposed method

The proposed method for improving the key generation algorithm is as follows.

The index of bins for each electrode in (14) that is generated from a different trial of one subject is stored in vector ***V*** in accordance with (15).

$$\boldsymbol{V} = (v_1, v_2, v_3, ...) \tag{15}$$

After generating ***V***, the distribution of this vector is calculated by the mean (μ) and standard deviations (σ). The distribution is defined as (16).

$$[l\_start, l\_end] = [\mu - k\sigma, \mu + k\sigma] \tag{16}$$

In (16), *k* is a criterion for determining the width of distribution and is a parameter that has been added as the proposed method to the feature mapping algorithm.

The start and end of the distribution width are stored as one of the templates in the template store. For the proposed method, *Ar* is defined as the mean of ***V*** and is different from *Ar* generated from (14). Because the size of $Auth_{reg-interval}$ for each electrode of a subject is different, the number of global distribution bins for each subject and the electrode will be different.

The templates for the proposed method are the *number of segments, Ar, Authreg-interval, window star l_start, l_end*, and do not require the original biometric data to be stored.

3.3. Conversion to binary mode

In order to use the key in the cryptographic systems, the generated key is used for the biometric features of individuals such as the number of segments, and *Ar* is converted to the binary mode using the algorithm in Appendix from [3].

Processing of the binary key generation involves two hash functions called SHA-1 and MD5 that are shown in figure 5, which results in a 640-bit-length key. The result of applying two duplicate functions creates more disturbance of the generated key.

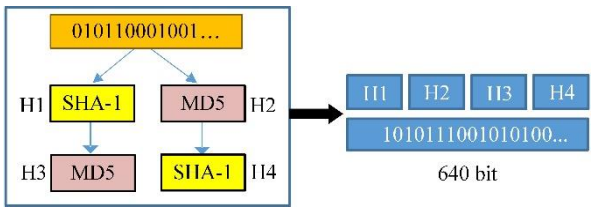


Figure 5. Flow of applying hash functions.

3.4. Key evaluation

For each subject, the features of the EEG signals are extracted, and then using (9) for each electrode, new feature vectors whose dimensions are equal to the number of electrodes are produced. Then the feature vector of each electrode is mapped to the corresponding bin using the stored template for each subject and the electrode in the template storage according to (14). If the index of bin belongs to the interval defined in (14), then *Ar* (mean of ***V***) is chosen as a new feature vector.

If the bin index does not belong to this distribution, the new feature will be the same as the bin index.

Then using the algorithm presented in the Appendix for converting to the binary mode, the features are converted to the desired keys.

This process is repeated for all electrodes. If 18 electrodes are used to generate the keys, the keys

from each electrode are connected to each other, and after applying the hash function, the generated key is compared for rejection or acceptance with the key in the template storage.
This system is named as an 18-channel system but if the generated key of each electrode is used separately, it is called a single-channel system.

3.5. Parameter selection

To reduce the key generation error, the appropriate values for both the k and k_seg values that are introduced in the key generation section and the proposed method must be selected.
According to (16), as the value of k increases, the amount of l_start decreases and the amount of l_end increases, so the width of the distribution and the probability of the belonging index of the bin to this interval increases. As a result, the value of FRR decreases.
In figure 6.A, the FRR diagram for the 18-channel system is shown in terms of different k_seg values for different k values. As shown, the amount of FRR decreases with an increase in the k value.
By increasing the value of k_seg, the distance between the distributions in (16) increases, so the overlap with FAR is decreased. In figure 6.B, the FAR diagram for the 18-channel system is shown in terms of different values of k_{seg}; as shown, increasing k_seg decreases FAR. However, the FRR changes are not significant with increasing the k value, except in certain cases, and the diagrams are on each other.
In figure 7.A, the HTER diagram for the 18-channel system is obtained in terms of different values of k_seg for various k values. As it is known, increasing k results in decreasing HTER but the amount of these changes decreases too, and

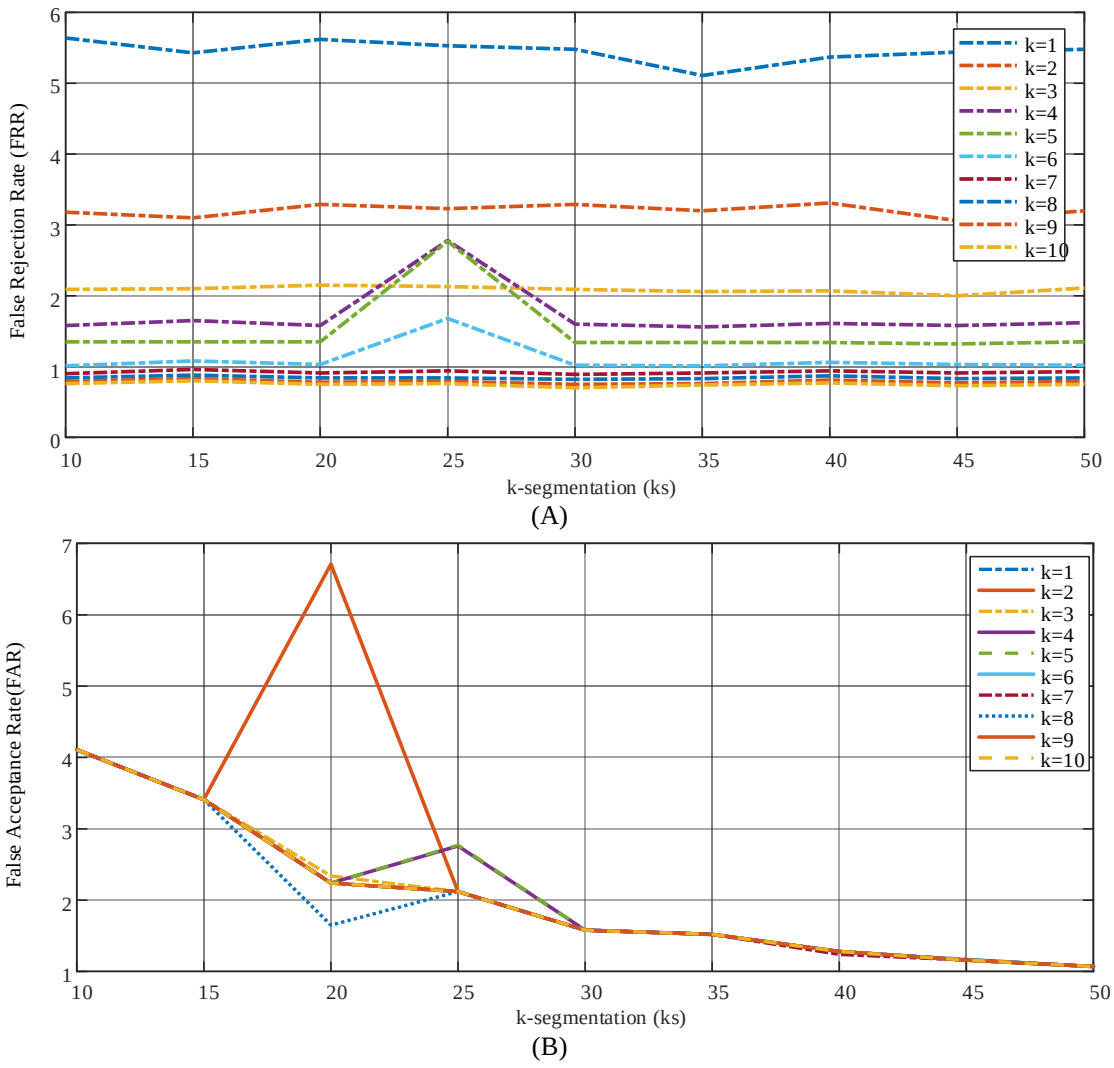


Figure 6. FRR (A) and FAR (B) diagrams in terms of different values of *k_seg* for different *k values* for the 18-channel system.

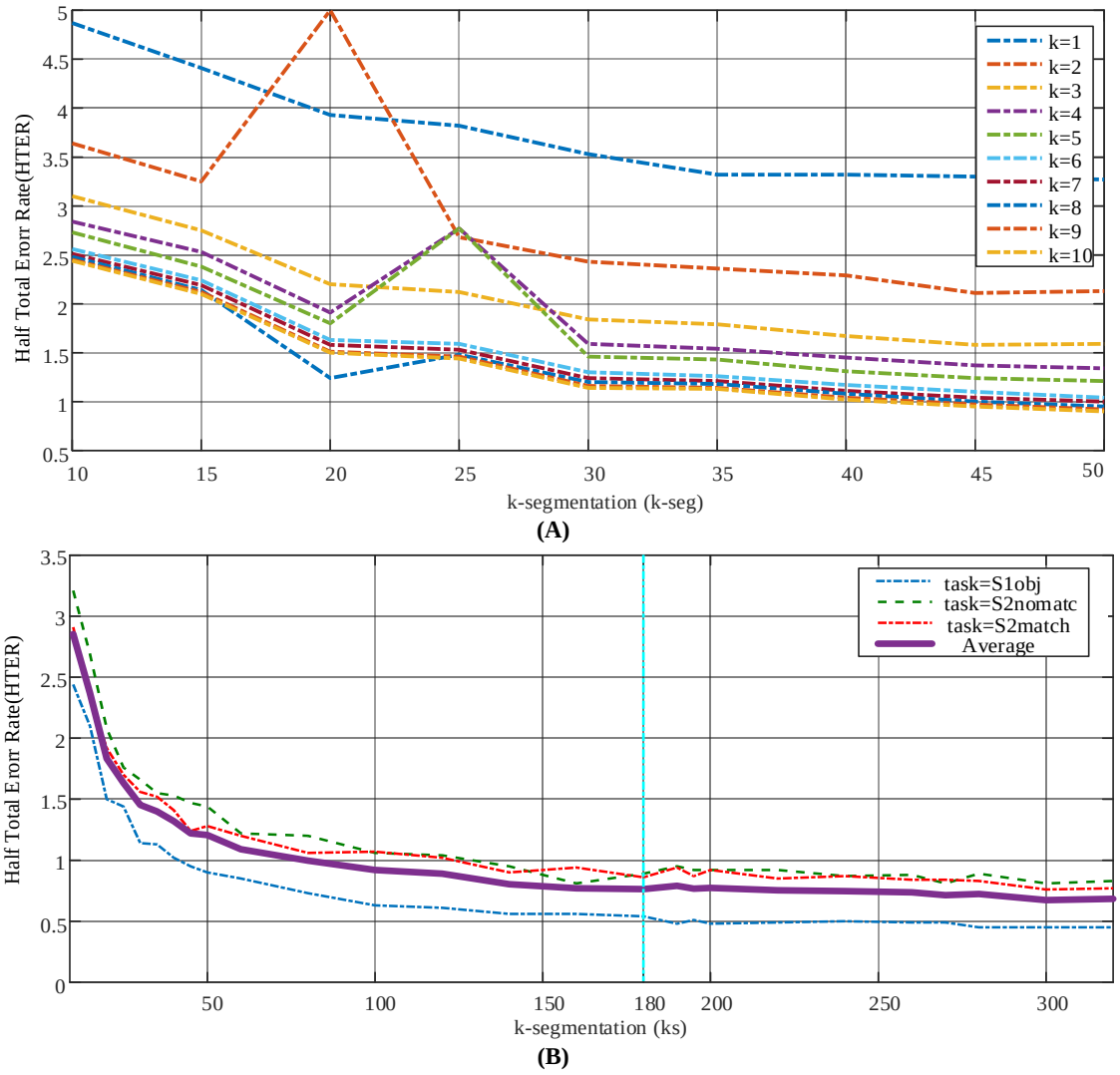


Figure 7. HTER diagram in terms of different *k_seg* values for different k values, 18-channel system (A) The HTER diagram in terms *k_seg* for the 18-channel system and *k = 10* (B).

eventually, in $k = 8, 9, 10$. The amount of these changes is negligible and can be ignored, so $k = 10$ is chosen.

In figure 7.B, the HTER diagram is shown in terms of k_seg for the 18-channel system, which is obtained for $k = 10$. As shown in the diagram, increasing k_seg decreases HTER, and finally, it becomes almost constant, and there are no significant changes, so $k\_seg = 180$ is selected.

4. Experimental results

For the database used in this paper, the tasks were the visual images. Considering the occipital and parietal areas of the human brain are related to vision and the activities of the occipital and parietal areas will be noticeable when performing these tasks. 18 electrodes are selected among the 64 electrodes in these areas (T7, T8, O1, O2, PO7, PO8, TP8, TP7, P3, P4, P5, P6, C3, C4, P8, P7, P1, and P2). The position of the selected electrodes is shown in figure 8 on the international system 10-10.

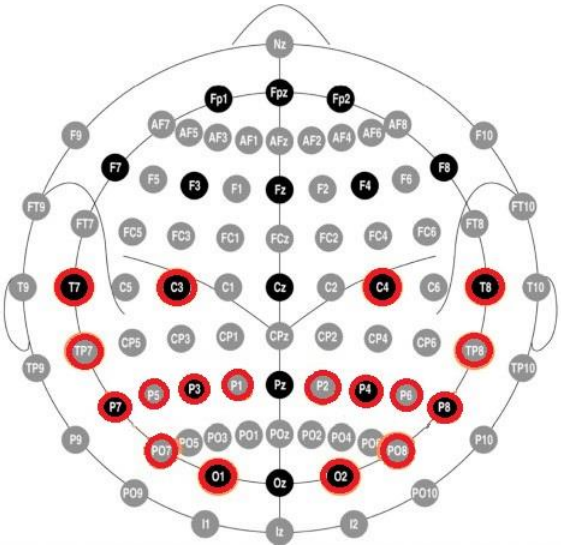


Figure 8. Position of selected electrodes on the international system 10-10.

Different feature extraction methods, for example, frequency features, time-frequency features, statistical features, and entropy-based features are used in this paper. Among the entropy-based features, the extracted features of sample entropy, Log energy entropy had a higher relative percentage difference.

The combined feature vector for a subject from 18 selected channels has 79 features per electrode containing (44+5) FFT features, 18 DWT features, one energy entropy feature, one sample entropy feature, and 10 autoregressive coefficients features. The justification that has in the literature, splitting a dataset into 60% to 80% for training to better model the underlying distribution and then test the results with the remaining 20-40% is a good choice.

In this paper, 70% of the database was randomly selected and used for the training system, and 30% of the database was used for key evaluation. The evaluation of the keys will be based on the FAR and FRR criteria. The system may create two types of errors: a false acceptance (FA) error when the system accepts an imposter and a false rejection (FR) error when the system rejects a client.

$$FAR = \frac{number\ of\ FRs}{number\ of\ client\ \ accesses} \tag{17}$$

$$FRR = \frac{number\ of\ FAs}{number\ of\ impostor\ accesses} \tag{18}$$

$$HTER = \frac{FAR + FRR}{2} \tag{19}$$

FRR is the ratio of the number of times the key generation system will incorrectly reject the derived key of a genuine user to the total attempts. FAR is the measure of the likelihood that the key generation system will incorrectly accept the derived key from an unauthorized user [3]. In most cases, the system can be measured using a decision threshold for obtaining a compromise between a small FAR or a small FRR [32]. Therefore, a trade-off depends on the system policies. If systems try to reduce FAR to the lowest possible level, FRR will rise. In other words, the more secure your access control, the less convenient it will be, as users are falsely rejected by the system. The same also applies the other way round.

The mean FAR and FRR values for all individuals in the database and 18 selected electrodes are shown in figure 9.A, and the mean HTER values for all individuals in the database and 18 selected electrodes are shown in figure 9.B.

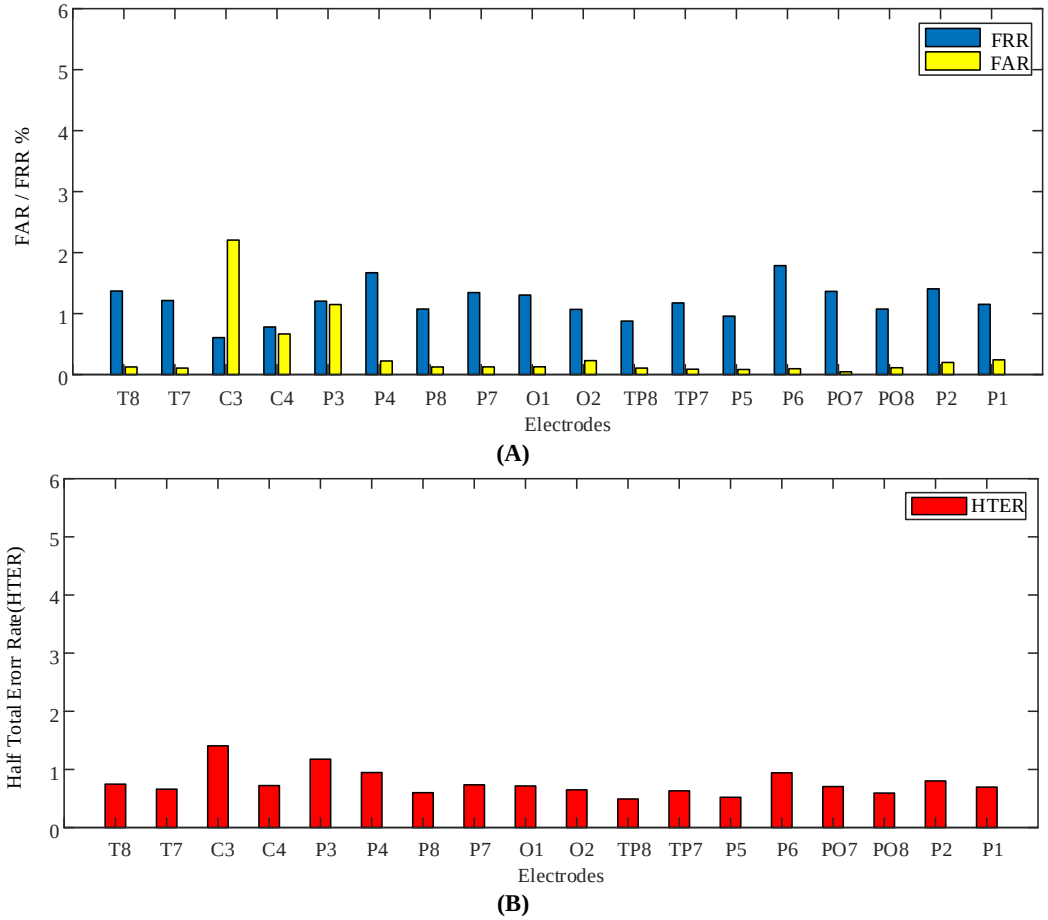


Figure 9.The mean FAR and FRR (A), HTER (B) values for all individuals on 18 electrodes for all tasks.

Table 1 shows the mean HTER, FAR, and FRR of the 18-channel system for all electrodes and subjects. The total error shows the average of HTER, FAR, and FRR for three tasks.

Table 1. Mean error for tasks for all individuals of the 18-channel system.

	S1-task	S2-Match	S2-NoMatch	Total Error
HTER (%)	0.54	0.86	0.89	0.76
FAR (%)	0.30	0.27	0.43	0.33
FRR (%)	0.78	1.44	1.34	1.18

For evaluation of the probability of success, the generated keys at the key evaluation step are compared with the generated key at the feature mapping step, which is stored in the template storage for all subjects and tasks. Table 2 shows the probability of success in the key generation for three tasks and subjects of the 18-channel system. Total probability shows the average value of the probability of success for three tasks.

Table 2. Mean probability of success in the key generation for tasks for all individuals of the 18-channel system.

	S1-task	S2-Match	S2-NoMatch	Total probability
Probability of success (%)	96	95.4	94.1	95.1

HTER for the single-channel system is shown in table 3. In this table, among the 18 available electrodes, 6 electrodes are selected with the lowest HTER.

Table 3. Mean HTER for tasks for all individuals of the single-channel system.

	S1-task (%)	S2-Match (%)	S2-NoMatch (%)	Total Error (%)
P8	0.49	0.73	0.57	0.59
O2	0.39	0.68	0.86	0.64
TP8	0.23	0.48	0.74	0.48
TP7	0.59	0.56	0.72	0.62
P5	0.49	0.58	0.55	0.54
PO8	0.44	0.61	0.72	0.59

5. Discussion

Network security is very important when confidential data is sent within organizations or between organizations through the network. Biometric cryptography is an emerging methodology in communication networks. From the brain signals, we can generate a binary code that can be used as a cryptographic key. The security of the key can be improved because brain waves will be one of the most powerful biometrics compared to others. For practical applications, error of the generating keys must be decreased. The goal of the proposed method in this paper is to decrease HTER.

Table 4. Comparison of results obtained with those of previous works.

Methods	Results (%)
Dang Nguyen *et al*. [22]	2.1 EER
Garima Bajwa *et al*. [3]	4.78 HTER
This paper	0.76 HTER

Table 4 shows a comparison of the results obtained with those of some previous works in the field of cryptographic key generation using EEG signals. For 18-channel cryptographic systems, according to the results presented by the G. Bajwa and R. Dantu's method, HTER for the three S1-task, S2-Match, and S2-NoMatch tasks was 4.28%, 4.80%, and 4.78%, respectively, and the total HTER of the system was 4.62%.

Dang Nguyen et al. achieved 2.1% EER (Equal Error Rate) for their systems. According to the results tabulated in table 1, HTER for the proposed algorithm is 0.76%, which is significantly reduced. In table 1, the mean FAR and FRR for each one of the three tasks were 0.33 and 1.18, respectively. Comparing to the G. Bajwa and R. Dantu's method, FAR has increased slightly and FRR has decreased.

The low amount of FAR indicates that the generated keys are unique for each subject and people (with a small error) cannot generate other people's keys.

Table 2 shows the 95.1% total probability access for three tasks. The high amount of probability of success and a low amount of FRR (Table 1) indicate that the generated keys are repeatable for one subject during different trails. This means that using the same task at different times and records, the key generation systems can produce the same keys.

The proposed algorithm was applied to three different activities, for which there was an acceptable error rate, thus the generated key had the property of revocability. If the generated key from one visually evoked task is at risk, changing the task produces another key.

Considering that the HTER value varies for different electrodes, it can be concluded that the system error rate is sensitive to the selection of the electrode. According to the type of task or mental

activity, a better combination of electrodes with high relative percentage difference can be selected. A key space is one of the important security factors in a cryptographic system, and is referred to as all possible states for key generation. If the binary key has n bits, the key space is 2^n. The key length in this system is 200-230 bits before applying the hash function. In comparison to other biometric indicators, we can say [33]:

Token (1012) > Password (1014–106) > Iris (106) > Fingerprint, PIN (104) > EEG-based cryptographic key (1/0.0027 ~ 370) > Face (6.25)

The key space of the generated key by this system is only higher than the face. Increasing key space to prevent search attacks is one of the most important priorities of this system. In this database, with the combination of different assignments, the key length can be increased up to three times.

The key generated from the proposed algorithms for hash function has 640 bits, and can be increased up to 1920 bits with combining different activities. One of the problems with EEG-based cryptographic keys is the difficulty of collecting signals. The solution proposed is to use single-channel and portable signal recording devices. In this paper, based on the results obtained and the acceptable error rate for each electrode, single-channel EEG-based systems could be generated. Table 3 shows the results for the six electrodes P8, O2, TP8, TP7, P5, and PO8, among which the TP8 electrode has the lowest mean HTER for all three activities and is equal to 0.48. Also the mean FAR and FRR for all three activities were achieved to be 0.1 and 0.87, respectively.

Before applying hash functions, the generated key by the single-channel system is weak in terms of key space and is, on average, 10-15 bits, which are not usable in cryptographic systems.

6. Conclusions and future works

In this paper, unique and cancelable cryptographic keys with repeatability were studied using the EEG signals for 120 subjects. The purpose of the biometric cryptographic key generation systems in this paper was to reduce the error of generating keys in order to increase the efficiency of the system for practical applications; the proposed method and different extracted features from the signal significantly reduced this error.

Also a single-channel EEG-based cryptographic key generation system was introduced in this paper. Given that the EEG signal and its application in BCI systems is an active area, it is expected that with portable devices and dry electrodes, this biometric index enters practical applications in the daily lives of individuals.

The proposed system has some limitations such as sensitivity social engineering attacks, dictionary attacks, and phishing attacks that have not been studied in this work. The key space of the generated keys by the proposed system is weak, so one of the most important goals of future works should be to increase the key space of these keys, especially in the single-channel mode. The generated keys in this system are outputs of the hash functions, so the length of the generated keys from the single-channel systems with 18-channel systems will be the same, and considering the nature of the hash functions, these two keys must be checked for security.

7. Appendix

Pseudo-code for converting feature vector to binary mode.

```
Algorithm 1: Binary Feature Vector Quantization
Input: Biometric feature vector Fv, number of segmentation N,
Authentication region Ar
For i : 1 to  Number of subjects
    For j : 1 to Number of electrodes.
        temp_key[0] :dec to bin (Fv[i][j])      %Binary quantization
        Seed : Fv[i][j] mod Ar[i][j]
 % Determine seed for temporary key
      temp_key[k]: XOR(temp_key[k-1], seed)
        key[i]: circularshift(temp_key[k],N[i][j])
        % Use the number of segments to perform the circular shift
        N_key[i]: (N_key[i] || key[k])
        % Concatenate the bits from each round to form the key
    End for
End for
Return N_key
```

8. Acknowledgment

The authors are grateful to the late Prof. Henri Begleiter at the Neurodynamics Laboratory at the State University of New York Health Centre at Brooklyn, USA, who generated the data and UCI Machine Repository for making it available online.

References

[1] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

[2] Ogiela, L. & Ogiela, M. R. (2014). Towards Cognitive Cryptography. Journal of Internet Services and Information Security, vol. 4, no. 1, pp. 58–63.

[3] Bajwa, G. & Dantu, R. (2016). Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Computers & security, vol. 62, pp. 95–113.

[4] Katz, J. & Lindell, Y. (2014). Introduction to Modern Cryptography, Second Edition. CRC press.

[5] Hema, C. R., Paulraj, M. P. & Kaur, H. (2008). Brain signatures: a modality for biometric authentication.

In 2008 International Conference on Electronic Design, Penang, Malaysia, 2008.

[6] Jain, A. K., Ross, A. & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, pp. 4–20.

[7] Delac, K. & Grgic, M. (2004). A survey of biometric recognition methods. In 46th International Symposium Electronics in Marine, vol. 46, pp. 184–193.

[8] Ogiela, M. R. & Ogiela, U. (2012). DNA-like linguistic secret sharing for strategic information systems. International Journal of Information Management, vol. 32, no. 2, pp. 175–181.

[9] Naccache, D., et al. (2011). Biometric Encryption, in Encyclopedia of Cryptography and Security. Boston, MA: Springer US, pp. 90–98.

[10] Mavaddati, A. (2019). A Novel Face Detection Method Based on Over-complete Incoherent Dictionary Learning. Journal of AI and Data Mining, vol. 7, no. 2, pp. 263–278.

[11] Noruzi, A., Mahlouji, M. & Shahidinejad, A. (2019). Robust Iris Recognition in Unconstrained Environments. Journal of AI and Data Mining., vol. 7, no. 4, pp. 495–506.

[12] Nixon, K. A., Aimale, V. & Rowe, R. K. (2008). Spoof Detection Schemes," in Handbook of Biometrics, Boston, MA: Springer US, pp. 403–423.

[13] Abbas, S. N., Abo-Zahhad, M., & Ahmed, S. M. (2015). State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. IET Biometrics, vol. 4, no. 3, pp. 179–190.

[14] Schomer, D. L. & Da Silva, F. L. (2012). Niedermeyer's electroencephalography: basic principles, clinical applications, and related fields. Lippincott Williams & Wilkins.

[15] Campisi, P. & La Rocca, D. (2014). Brain waves for automatic biometric-based user recognition. IEEE transactions on information forensics and security, vol. 9, no. 5, pp. 782–800.

[16] Ratha, N. K., Connell, J. H. & Bolle R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems, IBM systems Journal, vol. 40, no. 3, pp. 614–634.

[17] Ravi, K. V. R., Palaniappan, R., Eswaran, C. & Phon-Amnuaisuk, S. (2007). Data Encryption Using Event-related Brain Signals, in International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), vol. 2, pp. 540–544.

[18] Palaniappan, R., Gosalia, J., Revett, K., & Samraj, A. (2011). PIN generation using single channel EEG biometric. International Conference on Advances in Computing and Communications, Springer, Berlin, Heidelberg, 2011.

[19] Lokeshwari, G., Udaya, S. & Aparna, G. (2013). A novel approach for data encryption using EEG, SPIHT and genetic algorithm for secured applications, International Journal of Power Control Signal and Computation (IJPCSCS), vol. 5, pp. 23–27.

[20] Akhila, V. A., Arunvinodh, C., Reshmi, K. C. & Sakthiprasad K. M. (2016). A New Cryptographic Key Generation Scheme Using Psychological Signals, Procedia technology, vol. 25, no. Raerest, pp. 286–292.

[21] Nguyen, D., Tran, D., Sharma, D., & Ma, W. (2018). Emotional Influences on Cryptographic Key Generation Systems using EEG signals, Procedia computer science, vol. 126, pp. 703–712.

[22] Nguyen, D., Tran, D., Sharma, D., & Ma, W.(2017). Investigating The Impact Of Epilepsy On EEG-based Cryptographic Key Generation Systems, Procedia computer science, vol. 112, pp. 177–185.

[23] Matyáš, V. & R\iha, Z. (2000). Biometric authentication systems, in verfügbar über: http://grover. informatik. uni-augsburg. de/lit/MM-Seminar/Privacy/riha00biometric. pdf.

[24] Ingber, L. (1997). EEG database, UCI machine learning repository,University of California, Irvine, School of Information and Computer Sciences, Available: http://archive.ics.uci.edu/ml/datasets/ EEG+Database.

[25] Zeynali, M. & and Seyedarabi, H. (2019). EEG-based single-channel authentication systems with optimum electrode placement for different mental activities, biomedical journal, vol. 42, no. 4, pp. 261–267.

[26] Bao, X., Wang, J. & Hu, J. (2009). Method of individual identification based on electroencephalogram analysis, in New Trends in Information and Service Science, 2009. NISS'09. International Conference on, pp 390–393.

[27] Aydin, S., Saraouglu, H. M. & Kara S. (2009). Log energy entropy-based EEG classification with multilayer neural networks in seizure, Annals of biomedical engineering, vol. 37, no. 12, pp. 2626.

[28] Song, Y. & Liò, P. (2010). A new approach for epileptic seizure detection: sample entropy based feature extraction and extreme learning machine, Journal of Biomedical Science and Engineering, vol. 03, no. 06, pp. 556–567.

[29] Chuang, J., Nguyen, H., Wang, C. & Johnson, B. (2013). I think, therefore i am: Usability and security of authentication using brainwaves, in International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, pp. 1–16.

[30] Chang, Y. J., Zhang, W. & Chen, T. (2004). Biometrics-based cryptographic key generation, in 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763), vol. 3, pp. 2203–2206.

[31] Monrose, F., Reiter, M. K., Qi Li, & Wetzel, S. (2001). Cryptographic key generation from voice, in

Proceedings 2001 IEEE Symposium on Security and Privacy. S & P 2001, pp. 202–213.

[32] Bengio, S. & Mariéthoz, J. (2004). The expected performance curve: a new assessment measure for person authentication, in Proceedings of Odyssey 2004: The Speaker and Language Recognition Workshop, No. EPFL-CONF-83047.

[33] O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication, Proceedings of the IEEE, vol. 91, no. 12, pp. 2021–2040.