Generating Random Number Sequences Using Electroencephalography (EEG) Signals

Dr. Boushra Maala*
Khadijeh Iskander**

(Received 3 / 10 / 2024. Accepted 4 / 3 / 2025)

□ ABSTRACT □

Random numbers play an important role in many applications, such as gaming, generating encryption keys, modeling and simulating complex phenomena, software testing, and more. There are many algorithms, procedures, and phenomena that serve as sources for generating true random numbers or pseudo-random numbers. However, these traditional methods have some drawbacks, such as computational complexity and time consumption. Recent studies have demonstrated the effectiveness of using biometric markers as generators of random numbers, such as fingerprints, facial recognition, voice, iris patterns, and handwriting. However, these traditional vital signs also have weaknesses; they are inherited and unchangeable, and they are exposed to the public, which makes them susceptible to theft. Recent research has focused on studying other biomarkers as generators of random numbers, such as electroencephalography (EEG). Electroencephalography (EEG) provides a recording of the brain's electrical activity through electrodes placed in specific areas on the scalp. This recording is displayed as a series of waves that contain special and unique features, which can be extracted and processed to generate random numbers.

In this research, we will present a scheme for generating random number sequences, each 512 bits long, based on the characteristics of brain signals related to imagined movement, using the EEG Motor Movement/Imagery Dataset. We examined the randomness of these sequences through statistical tests from the National Institute of Standards and Technology (NIST), and we studied the distinctiveness of these sequences through Hamming distance. Our findings indicate the potential use of these sequences as encryption keys in security applications.

Keywords: random number generation, biometric parameters, ElectroEncephaloGraphy (EGG), motor imagery, NIST.

* **Associate Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria. boushra.maala@gmail.com**

** **PhD Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Lattakia University, Lattakia, Syria. khadijeh.iskander@tishreen.edu.sy**

توليد سلاسل أرقام عشوائية باستخدام إشارات تخطيط الدماغ EEG

د. بشرى معلا•

خديجة اسكندر ••

(تاريخ الإيداع ٣ / ١٠ / ٢٠٢٤. قُبِل للنشر في ٤/ ٣ / ٢٠٢٥)

□ ملخّص □

تلعب الأرقام العشوائية دوراً هاماً في العديد من التطبيقات، مثل الألعاب، وتوليد مفاتيح التعمية، ونمذجة ومحاكاة الظواهر المعقدة، واختبار البرمجيات وغيرها. يوجد هناك العديد من الخوارزميات والإجرائيات والظواهر التي تُعدّ مصدراً لتوليد أرقام عشوائية صحيحة أو أرقام شبه عشوائية، ولكن هذه الطرائق التقليدية كان لها بعض السلبيات كالتعقيد الحسابي واستهلاك الزمن. بينت الدراسات الحديثة فعالية استخدام العلامات الحيوية كمولدات للأرقام العشوائية، مثل بصمة الإصبع، وبصمة الوجه، والصوت، وقزحية العين وخط اليد. ولكن كان لهذه العلامات الحيوية التقليدية نقاط ضعف أيضاً، فهي موروثة وغير قابلة للتغيير، كما أنها مكشوفة للعلن وهناك إمكانية لسرقتها. توجهت الأبحاث الحديثة إلى دراسة علامات حيوية أخرى كمولدات للأرقام العشوائية مثل تخطيط كهربائية الدماغ EEG. يقدّم تخطيط كهربائية الدماغ تسجيلاً للنشاط الكهربائي للدماغ من خلال أقطاب كهربائية تتوضع في مناطق محددة على فروة الرأس، ويعرض هذا التسجيل على شكل سلسلة من الموجات التي تحوي مميزات خاصة وفريدة، يمكن استخراجها ومعالجتها لتشكيل أرقام عشوائية.

سنقدم في بحثنا هذا مخططاً لتوليد سلاسل أرقام عشوائية طول كل منها ٥١٢ بت اعتماداً على مميزات إشارات تخطيط الدماغ الخاصة بتخيل الحركة مستخدمين قاعدة البيانات EEG Motor Movement/Imagery Dataset ودرسنا عشوائية هذه السلاسل من خلال الاختبارات الإحصائية للمعهد الوطني للمعايير والتكنولوجيا NIST، كما درسنا خاصية التميز (التفرد) لهذه السلاسل من خلال مسافة هامينغ، وتبين لنا إمكانية استخدام هذه السلاسل كمفاتيح تعمية في التطبيقات الأمنية.

الكلمات المفتاحية: توليد أرقام عشوائية، العلامات الحيوية، حساس تخطيط كهربائية الدماغ (EGG)، تخيل الحركة، NIST .

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سورية.
boushra.maala@gmail.com

•• طالبة دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية، اللاذقية، سورية.
khadijeh.iskander@tishreen.edu.sy

مقدّمة:

مولدات الأرقام العشوائية random number generators (RNGs) هي عبارة عن خوارزميات صممت من أجل إنتاج سلاسل من الأرقام التي يمكن اعتبارها عشوائية، والتي تلعب دوراً كبيراً في العديد من التطبيقات مثل الألعاب، وتوليد مفاتيح التعمية، ونمذجة ومحاكاة الظواهر المعقدة، وتحديد القرصنة في الدارات المتكاملة، واختبار البرمجيات وغيرها من التطبيقات.

تقسم الـ RNGs إلى نوعين أساسيين وهما: مولدات الأرقام شبه العشوائية pseudo random number generators (PRNGs) ، ومولدات الأرقام العشوائية التامة(true random number generators(TRNGs.

بالنسبة للصنف الأول PRNGs: يعتمد على خوارزميات رياضية لإنتاج سلاسل طويلة من الأرقام العشوائية خلال وقت قصير جداً، وتحتاج إلى بذرة (seed) كدخل لعملية إنتاج السلسلة العشوائية. يجب أن تكون البذرة (seed) سرية وآمنة، والخوارزميات الرياضية المستخدمة منتقاة بشكل جيد للحصول على خرج غير متوقع وبالنتيجة اعتباره عشوائياً. تُعرف PRNGs أيضاً بالنظريات الحتمية، حيث يمكن إعادة توليد نفس السلسلة العشوائية عند استخدام نفس الدخل seed. أما الصنف الثاني TRNGs: فهو يعتمد على مصدر غير حتمي لإنتاج سلاسل عشوائية تامة مثل: ضجيج المقاومة، وضجيج الأتموسفير، والنشاط الراديوي، وغيرها. عموماً تعد TRNGs أكثر فعالية من PRNGs ولكنها بطيئة، وصعبة التطبيق، وهي غير حتمية فلا يمكن إعادة توليد نفس السلاسل العشوائية، كما تتطلب بعض التطبيقات استخدام الصنف TRNGs مثل الألعاب، والأمن، وأخذ العينات العشوائي، واليانصيب[1,2].

تُعدّ العلامات الحيوية أو البيومترية مثل بصمة الإصبع أو الوجه أو الصوت أوخط اليد أو قزحية العين مصدراً جيداً للأرقام العشوائية، حيث يمكن اعتبار جسم الإنسان نفسه وصفاته البشرية مصدراً لتوليد أرقام عشوائية تامة TRNGs، أو يمكن اعتبارها دخل seed لمولدات الأرقام شبه العشوائية PRNGs. ساهم استخدام هذه العلامات الحيوية التقليدية في جعل مولدات الأرقام العشوائية TRNGs أكثر فعالية وأقل تكلفة، ولكن المعلومات التي تحملها هذه العلامات الحيوية موروثة وفريدة ولا يمكن تغييرها من أجل استخدامها مع تطبيقات مختلفة، وبالتالي في حال سُرقت العلامة الحيوية المستخدمة فإن جميع السلاسل العشوائية المولدة عن طريقها عرضة للكسر. كما يرافق العلامات الحيوية سابقة الذكر ضجيج بشكل طبيعي مما يفرض قيوداً فيما يتعلق بالتقنية المطلوبة لقراءة العلامة الحيوية. إضافة إلى أن بعض التطبيقات تتطلب تغيير الأرقام العشوائية المستخدمة كل فترة زمنية معينة، ولكن بما أن العلامات الحيوية التقليدية موروثة وغير قابلة للتغيير فإن السلاسل العشوائية المولدة من خلالها أيضاً ذات فضاء محدود وهذا يُعدّ مشكلة عند استخدامها في تأمين حساب بنكي أو بريد الكتروني، وهذا ما أشرنا إليه سابقاً في أن سرقة العلامة الحيوية تؤدي لتعريض جميع التطبيقات المؤمنة من خلالها لخطر الاختراق[3,4].

اعتُمِد في كثير من الأنظمة المتقدمة على بصمة الإصبع والقزحية والوجه معاً لزيادة السوية الأمنية لها، إلا أنها قد تكون مكشوفة للعلن وغير سرية، بمعنى أن التقاط صورة للوجه أو تسجيل صوت المستخدم أو سرقة بصمة الأصابع يُعدّ أمراً ممكناً.

طرائق البحث ومواده:

تم تحصيل إشارة تخطيط الدماغ الكهربائية من قاعدة البيانات EEG Motor Movement/Imagery Dataset V1.0.0، والتي تعدّ من أشهر قواعد البيانات المستخدمة لأغراض التصنيف ودراسة القضايا الأمنية المتعلقة بالعلامات الحيوية. اعتمدنا في دراستنا على المكتبة البرمجية (mne) والتي تتضمن العديد من النماذج التي تتعامل مع إشارة تخطيط الدماغ الكهربائية من خلال قراءتها وتحليل بارامتراتها [5].

وبرمجت جميع خطوات المخطط المقترح هنا باستخدام لغة البايثون Python الإصدار 3.10 [6].

ونفذت على جهاز حاسب ذو مواصفات مبينة في الجدول الآتي:

الجدول (١) : بعض مواصفات الجهاز الذي طبقت عليه الدراسة.

نظام التشغيل Operating system	المعالج Processor	نوع النظام System type	ذاكرة الوصول العشوائي RAM
Windows 7 Ultimate	Intel(R)Core(TM)i5-2410M CPU @2.30GHz	64-bit	4GB

قيمت النتائج التي حصلنا عليها من خلال اختبار NIST لاختبار العشوائية، ومن خلال مسافة هامينغ لاختبار التميز والتفرد.

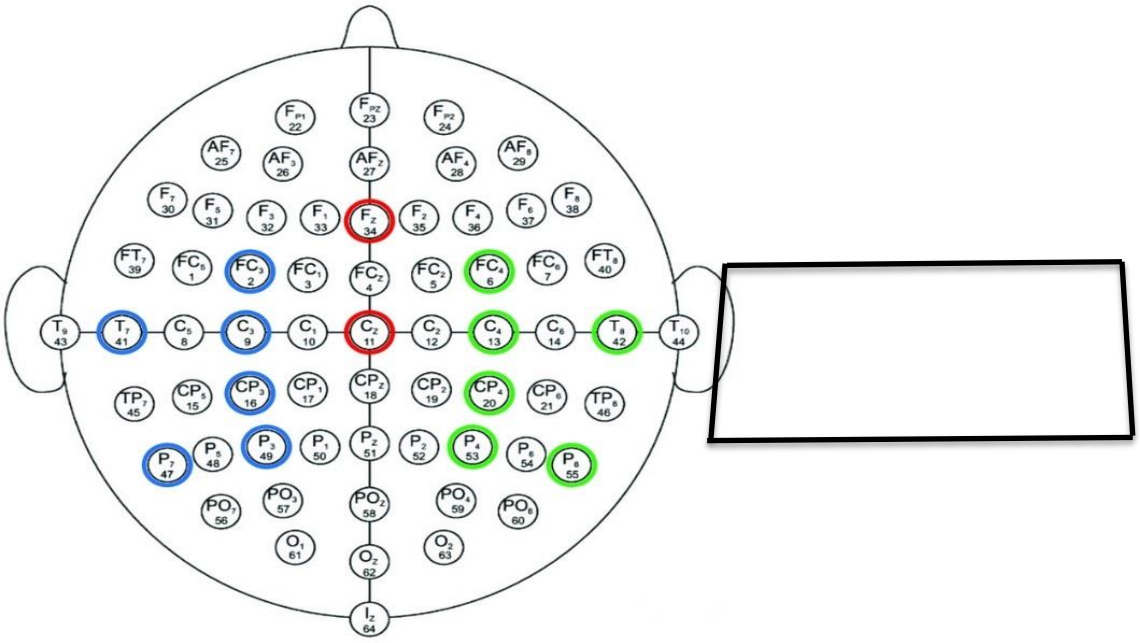
١. الدراسة المرجعية:

١,١ تخطيط كهربائية الدماغ (EEG) ElectroEncephaloGraphy :

هو عبارة عن تقنية لتسجيل النشاط الكهربائي للدماغ باستخدام أقطاب أو ما يُسمى الكترودات توضع على فروة الرأس وفق ترتيب معين، حيث تقيس هذه الأقطاب تغيرات الجهد من مرتبة الميكرو فولت والتي يسببها التيار الأيوني داخل الخلايا العصبية، وتعرض على شكل سلسلة من الموجات، وهو وسيلة غير جراحية وآمنة لقياس نشاط الدماغ، ويستخدم على نطاق واسع في فهم وظائف الدماغ، تشخيص الاضطرابات العصبية، التصنيف، وغيرها من التطبيقات الطبية[7].

تتألف إشارة EEG من مصفوفة ثنائية البعد من القيم الحقيقية (قناة ، زمن) والتي تمثل جهود الدماغ الكهربائية المتعلقة بالمهمة. يمثل هذان البعدان المعلومات المكانية والزمانية لإشارة EEG حيث يشير البعد المكاني إلى المواضع المكانية للأقطاب الكهربائية على فروة الرأس (عدد الأقطاب الكهربائية)، بينما يشير البعد الزمني إلى عدد النقاط الزمنية في الثانية (أي معدل أخذ العينات). تتراوح الدقة المكانية من 1 إلى 256 قطب كهربائي ولكن عادة ما تستخدم مجموعة من 21 إلى 64 قطب كهربائي لأغراض البحث والأغراض السريرية. يتراوح معدل أخذ العينات عادة من ١٢٨ إلى ١٠٠٠ هرتز.

تعتمد أسماء الأقطاب الكهربائية على موقعها: C مركزي (Central) و T صدغي (Temporal) و F أمامي (Frontal) و Fp قبل الجبهة (prefrontal) و P جداري (Parietal) و O قذالي (Occipital) و (AF و FC و FT و CP و TP و PO)هي أقطاب وسيطة بين (C و T و F و Fp وP و O) ، ويبين الشكل (١) توزع هذه الأقطاب على فروة الرأس باستخدام نظام ١٠-١٠ القياسي، حيث تشير الخطوط الغامقة إلى الأقطاب الكهربائية في القشرة الحسية الحركية[7,8].



الشكل (١): توزع ٦٤ قطباً كهربائياً على فروة الرأس وفق المعيار ١٠-١٠ القياسي

تُقسم إشارة EEG إلى ٥ نطاقات ترددية وهي: دلتا (0.5-3 Hz) ، ثيتا (4-7 Hz) ، ألفا (8-13 Hz) ، بيتا (14-30 Hz) و غاما (>30 Hz) .

أمواج دلتا: مرتبطة بالنوم العميق ويمكن ملاحظتها أيضاً في حالة المشي.

أمواج ثيتا: مرتبطة بحالات الإلهام والتأمل العميق.

أمواج ألفا: وتظهر في حالة الراحة والتركيز.

أمواج بيتا: مرتبطة بالتفكير العميق وحل المشاكل والانتباه.

أمواج غاما: تملك مطالاً منخفضاً، ومرتبطة بحركة الأصابع واللسان.

١,٢ استخدام تخطيط كهربائية الدماغ EEG في توليد أرقام عشوائية:

تتمتع إشارات تخطيط الدماغ بالعديد من المميزات والتي تجعل منها علامة حيوية مناسبة وفعالة في توليد أرقام عشوائية، فهي: علامة حيوية فريدة ومميزة، وموثوقة، وصعب تقليدها أو سرقتها إذ أن النشاط الدماغي حساس لحالة الفرد إذ أنه يتغير ويتأثر بمزاج الفرد أو تحت الضغط والتهديد، إضافة إلى أنها علامة حيَّة فلا يمكن استخلاصها من الشخص بعد موته[4,7].

دُرس النشاط الكهربائي للدماغ في عدة حالات:

١- **<u>حالة الراحة:</u>** حيث أن الشخص لا يمارس أي نشاط أو مهمة، وإنما يبقى هادئاً ومستيقظاً فقط. وبينت الدراسات أن النشاط الدماغي لأشخاص مختلفين وهم في حالة السكون أو الراحة يكون مختلفاً ومتمايزاً بين هؤلاء الأشخاص، وأن الخصائص التي يحملها هذا التسجيل تكون فريدة ومميزة. ولكن تطبيق هذه الحالة صعبة في العالم الخارجي الحقيقي، إذ أنه من الصعب تأمين حالة سكون تام للشخص.

في المرجع [9]، طبقت الدراسة على أشخاص أصحاء وأشخاص مرضى مصابين بالصرع في حالتين (أعين مفتوحة وأعين مغلقة) وهم في حالة سكون دون القيام بأي نشاط، واستخدمت ١٠٠ قناة وحصلت الترددات من القيم الصحيحة

لإشارة EEG ومن ثم ولدت سلاسل بطول $^{٦}١٠$، ولكن بينت هذه الدراسة أنه لا يمكن استخدام إشارة EEG بشكل مباشر كمولد لسلاسل الأرقام العشوائية، وإنما يجب إخضاع هذه السلاسل لعميات تحويل رياضية لجعلها عشوائية.

في المرجع [1]، طورت الدراسة السابقة، وأُخذت قيم حقيقية وضربت بـ 10^m لتحويلها إلى قيم صحيحة ومن ثم أجرت إزاحة نحو اليمين، استخدم ٦٤ الكترود، وأنتجت سلاسل بطول $^{٦}١٠$، وبينت هذه الدراسة أن النطاق الترددي غاما(gamma) قد أعطى أفضل النتائج.

٢- **<u>حالة الحركة:</u>** يعني تسجيل النشاط الدماغي للفرد أثناء قيامه بأداء مهمة معينة أو إدراكه لفعل معين. أو تسجيل النشاط الدماغي للفرد استجابة لتأثير بصري خارجي، مثل صورة مرئية أو فلاش.

اعتمدت الدراسة [10] على تسجيل النشاط الدماغي لـ ٧ أشخاص أثناء قيامهم بأداء ٥ مهام عقلية معينة، استخدمت ٦ قنوات، واستمر التسجيل الكهربائي لمدة ١٠ ثواني، ومن ثم أجريت المعالجة واستخراج المميزات باستخدام تحويلي ويفلت المتقطع وفوريه المتقطع، وبالنتيجة تم الحصول على مفاتيح بطول ٢٣٠ بت.

في الدراسة [11] أجريت عملية تحقق بيومتري من خلال تسجيل النشاط الدماغي للأشخاص وهم يقومون بالتوقيع على هواتفهم، حيث دمجت مميزات إشارة EEG والتي تم تحصيلها باستخدام تحويل فوريه المتقطع DFT مع مميزات التوقيع الديناميكي. واستخدمت استخدام ١٤ قناة.

في الدراسة [12] سُجل النشاط الدماغي للأفراد وهم يقومون بإدخال كلمات مرور معينة من خلال لوحة المفاتيح. استخدمت ٥ قنوات وتم الحصول على سلاسل أرقام عشوائية بطول ١٦٠ بت.

في الدراسة [13] سُجل النشاط الدماغي للأشخاص استجابة لتأثير بصري خارجي من خلال النظر إلى صورة فيها خطوط بيضاء وسوداء واعتمدوا على الالكترود Cz لتوليد رمز PIN لاستخدامه في أغراض التحقق والأمن.

٣- **<u>حالة تخيل الحركة:</u>** يُسجل النشاط الدماغي للفرد أثناء تخيله تحريك جزء معين من جسمه أو تخيله القيام بمهمة معينة، وبينت الدراسات أن التسجيل الدماغي هنا يمتلك خصائص فريدة ومميزة، وأن هذا النوع أقل عرضة للضجيج من حالة الحركة الفعلية، وهذا ما جعله مناسباً للاستخدام في عمليات التوثيق والتحقق. وهو قابل للتطبيق ومناسب لكل أنواع المرضى المختلفين عن بعضهم بالمقدرات الفيزيائية والبصرية.

في الدراسة [14] وُضِع مخطط أمني بيومتري من أجل عمليات التحقق والتوثيق يعتمد على إشارات تخطيط الدماغ الخاصة بتخيل حركة الأرجل والأذرع والتي جمعت بواسطة 17 الكترود، نفذت التجربة اعتماداً على ٤٠ شخص، مستخدمين خوارزميات التعلم العميق.

أيضاً تمكنت الدراسة [15] من تحسين دقة التحقق البيومتري اعتماداً على أربع مميزات من إشارات تخطيط الدماغ الخاصة بتخيل الحركة، والتي جمعت باستخدام ٣٦ الكترود. واستخدم مرشح تمرير حزمة Hz (30-8) خلال طور المعالجة البدائية، واستغرقت التجربة ١٠ ثواني.

كان هناك أيضاً العديد من الأبحاث حول استخدام إشارات تخطيط الدماغ EEG في توليد أرقام عشوائية يمكن استخدامها كمفاتيح تعمية نذكر منها:

الدراسة [16] اعتمدت على التسجيلات الكهربائية لـ ٣٢ شخص مختارة بشكل عشوائي من قاعدة البيانات GrazIIIa، حيث استخدمت ٦٤ قناة، واستخرجت المميزات الترددية (PSD(power spectral density، وباستخدام التكميم وُلِدت مفاتيح طول كل منها ٢٥٦ بت.

الدراسة [17] اعتمدت على الالتزام الضبابي (fuzzy commitment) في عملية استخراج المميزات من إشارة تخطيط الدماغ لـ ٤٢ شخص، وأُنتجت سلاسل بتات عشوائية بطول ٤٠٠ بت يمكن استخدامها كمفاتيح تعمية أو في أغراض التحقق.

نلاحظ من هذه الدراسات المرجعية السابقة فعالية إشارات تخطيط الدماغ EEG في استخدامها كعلامة حيوية في توليد أرقام عشوائية وأغراض التحقق، وخاصة في حالة الدراسات التي اعتمدت على تخيل الحركة بدلاً من الحركة الفعلية، لذلك نسعى في بحثنا هذا إلى تطوير هذه الدراسات من خلال تخفيض تعقيد النظام وزيادة طول السلاسل العشوائية الناتجة وإجراء المعالجة الأولية المناسبة لتخفيض الضجيج المرافق لهذه الإشارات.

٢. الجزء العملي:

٢-١ توصيف قاعدة البيانات :

اعتمدنا في دراستنا على قاعدة البيانات EEG Motor Movement/Imagery Dataset V1.0.0، والتي تضم تسجيلات EEG لـ ١٠٩ أشخاص مشاركين ، حيث تتضمن ٤ مهام و ١٤ جولة تجريبية.

سُجلت إشارات تخطيط الدماغ للمشاركين باستخدام ٦٤ قناة وهم يقومون بمهام تخيل الحركة (MI) وذلك بالاعتماد على المعيار BCI2000 باستخدام نظام ١٠-١٠ الدولي بمعدل أخذ عينات ١٦٠ هرتز.

أجرى المشاركون ١٤ عملية تجريبية وهي: تشغيلان أساسيان مع فتح العينين (run1) ومع إغلاق العينين (run2) لمدة دقيقة واحدة لكل تشغيل، بالإضافة لـ ٣ عمليات تشغيل لكل من المهام الأربعة التالية مدة كل منها دقيقتين وهي:

a- التجربة ٣، ٧، ١١: يظهر الهدف على الجانب الأيسر أو الأيمن من الشاشة، يقوم المشارك بفتح وغلق القبضة المقابلة حتى يختفي الهدف ثم يرتاح المشارك.

b- التجربة ٤، ٨، ١٢: يظهر الهدف على الجانب الأيسر أو الأيمن من الشاشة، ثم يتخيل المشارك فتح وإغلاق القبضة المقابلة حتى يختفي الهدف ثم يرتاح المشارك.

c- التجربة ٥، ٩، ١٣: يظهر الهدف في الجزء العلوي أو السفلي من الشاشة، يفتح المشارك ويغلق قبضتي اليد (إذا كان الهدف في الأعلى) أو يحرك قدميه كلتيهما (إذا كان الهدف في الأسفل) حتى يختفي الهدف ثم يرتاح المشارك.

d- التجربة ٦، ١٠، ١٤: يظهر الهدف في الجزء العلوي أو السفلي من الشاشة، ثم يتخيل المشارك فتح وغلق قبضتي اليد (إذا كان الهدف في الأعلى) أو يتخيل تحريك قدميه كلتيهما (إذا كان الهدف في الأسفل) حتى يختفي الهدف ثم يرتاح المشارك.

سنستخدم هنا فقط مجموعات المهام b و d والتي تتضمن الحركات المتخيلة أي الأشواط التجريبية 4 ، 6 ، 8 ، 10، ١٢ ، ١٤ .

تبدأ التجربة عند اللحظة t=-2 ثم يرتاح الشخص لمدة 2 ثانية ويظهر الهدف على الشاشة عند t=0

- تشير L إلى الخيال الحركي للقبضة اليسرى التي تُفتح وتُغلق.
- تشير R إلى الخيال الحركي للقبضة اليمنى التي تُفتح وتُغلق.
- يشير BLR إلى الخيال الحركي لكلا القبضتين اللتين تُفتحان وتُغلقان.
- يشير BF إلى الخيال الحركي لكلا القدمين اللتين تُفتحان وتُغلقان.

تبدأ تجربة جديدة بعد استراحة لمدة ثانيتين، يعمل تخيل التحريك لمدة 4 ثوانٍ تقريباً في كل مرة بتردد أخذ عينات يبلغ 160هرتز، لذا يبلغ حجم البيانات الفعالة لكل قطب في كل اختبار هو ٦٤٠ عينة.

٢-٢-المعالجة الأولية (preprocessing):

تتضمن الخطوات الآتية:

١- **اختيار القناة:** تُختار قنوات EEG الأكثر ملاءمة لمهام تخيل الحركة (MI)، حيث يفضل استخدام عدد أقل من قنوات EEG من أجل تقليل التكلفة الحسابية والذاكرة المطلوبة وتخفيض تعقيد النظام وتكلفة المعدات اللازمة عند وضع الأقطاب الكهربائية. ولكن يجب الأخذ بالحسبان وضع هذه الأقطاب في المكان المناسب تجنباً لفقدان معلومات مفيدة، لذلك يجب اختيار العدد الأمثل للأقطاب الكهربائية والمواضع المناسبة لها. اخترنا في بحثنا هذا ٦ قنوات فقط وهي موجودة في منطقة القشرة الحسية الحركية (FC6 , FC5 , FC4 , FC3 , FC2 , FC1) وهي المسؤولة عن إشارات تخيل الحركة.

٢- **ترشيح الإشارة:** اختير النطاق الترددي الأكثر ملاءمة لمهام MI، حيث بينت الدراسات بالنسبة لإشارات تخيل الحركة تحدث التغيرات في الطاقة للإيقاعات الحسية الحركية بشكل رئيسي في نطاقي الترددات (α وβ) لذلك استخدمنا في دراستنا مرشح تمرير حزمة (0–40)Hz . تتضمن هذه المرحلة أيضاً ترشيح وإزالة الإشارات غير المرغوب فيها وإشارات الضجيج الناجمة عن الحركات الإرادية وضجيج مخطط كهربائية العضلات (EMG) وضجيج إشارات العين (EOG) من خلال المكتبة البرمجية mne والتي تتيح توابع خاصة بإزالة هذه الإشارات.

٣- **إزالة الشوائب:** بالرغم من استخدام مرشح تمرير حزمة إلا أنه يبقى من الصعب استبعاد جميع الشوائب، لذلك طبقنا التابع البرمجي del- annotation لحذف الإشارات غير المرغوبة وغير المفيدة.

٢-٣-استخراج المميزات:

تحوي إشارات تخطيط الدماغ ضمن مميزاتها الزمنية والترددية معلومات مفيدة تعبر عن هذه الإشارات، لذا اعتمدنا في دراستنا على استخراج بعض هذه المميزات، والتي تَعدّ من أهم المميزات المعتمدة في الأبحاث والدراسات عند دراسة النشاط الكهربائي للدماغ وهي [12]:

٢-٣-١ المميزات الزمنية :

- المتوسط الحسابي (Mean) : يعطى بالعلاقة الرياضية الآتية:

$$\overline{x} = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (1)$$

حيث x_i تمثل العينة رقم i ، و n تمثل عدد العينات الأعظمي.

- الانحراف المعياري (Standard Deviation): يستخدم لقياس مدى التبعثر الإحصائي، أي أنه يدل على مدى امتداد مجالات القيم ضمن مجموعة البيانات الإحصائية، ويعطى بالعلاقة الرياضية الآتية:

$$S = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{n-1}} \qquad (2)$$

- معامل اللاتماثل أو التجانف (Skewness): هو مؤشر لقياس درجة واتجاه لاتماثل تابع التوزيع الاحتمالي لمتغير عشوائي حقيقي، ويوصف بالعلاقة الرياضية الآتية:

$$g = \frac{\sum_{i=1}^{n} (x_i - \overline{x})^3 / n}{s^3} \qquad (3)$$

- معامل التسطح أو درجة التقوس (Kurtosis): هو مؤشر لقياس درجة تحدب أو تقوس تابع التوزيع الاحتمالي لمتغير عشوائي حقيقي، ويوصف بالعلاقة الرياضية الآتية:

$$k = \frac{\sum_{i=1}^{n} (x_i - \overline{x})^4 / n}{s^4} \qquad (4)$$

يعد معاملي التجانف والتسطح من أهم معالم أشكال توزيع المتغيرات العشوائية، ويمكّن من توصيف شكل توزيع الاحتمالات في جوار القيمة المتوقعة.

٢-٣-٢ المميزات الترددية :

درسنا الكثافة الطيفية للطاقة PSD (power spectral density) والتي تمثل كيفية توزيع طاقة الإشارة أو السلسلة الزمنية مع التردد، وتُستخدم هذه المميزة في عمليات التصنيف والترميز، وتعطى بالعلاقة الآتية:

$$PSD(x) = \lim_{T\to\infty} \frac{1}{2\,T} \int_{-T}^{T} \left| s(t) e^{-j2\pi x t} dt \right|^2 \qquad (5)$$

٢-٤ تشكيل سلاسل الأرقام الثنائية:

بعد أن أجرينا المعالجة الأولية لإشارات تخطيط الدماغ، حصلنا على ملفات تتضمن إشارات تخطيط الدماغ الخاصة بتخيل الحركة MI-EEG. تضم هذه الملفات البيانات الوصفية بحجم ١١٤٩٦ عنصر وهي عبارة عن قيم من رتبة الميكرو فولت، وسُجلت لمدة ٤ ثواني بتردد تقطيع ١٦٠ هرتز، فحصلنا على ٦٤٠ عينة لكل قناة من القنوات الستة المدروسة (FC_1 , FC_2 , FC_3 , FC_4 , FC_5 , FC_6)، فأصبح لدينا مصفوفة ثلاثية الأبعاد (11496,6,640) أي تتضمن ١١٤٩٦ عنصراً وكل عنصر هو مصفوفة ثنائية البعد (6,640) ، بعد ذلك أجرينا عملية تكميم لقيم هذه المصفوفة ما بين (−1,+1) ومن ثم استخرجنا **المميزات الزمنية** التي عرفناها سابقاً، وجمعنا هذه المميزات الأربعة للقنوات الستة، ومن أجل **المميزات الترددية** ، قسمنا النطاق الترددي إلى ٥ مجالات ترددية، واستخرجنا الطاقة العظمى لكل نطاق ترددي على حدا من خلال خوارزمية التقدير welch والتي تستخدم لتقدير معاملات النماذج الإحصائية عندما تكون بعض البيانات مفقودة أو غير مرئية. ومن ثم جمعنا المميزات الزمنية مع المميزات الترددية لـ ١٠٠٠٠ عينة مدروسة وحولناها إلى الصيغة الثنائية، فحصلنا على سلاسل ثنائية طول كل منها ٣٢٩ بت كما هو مبين في الشكل (٢).

B1	B2	B3	.....	B329

الشكل(٢): سلسلة البتات المستخلصة من مميزات EEG

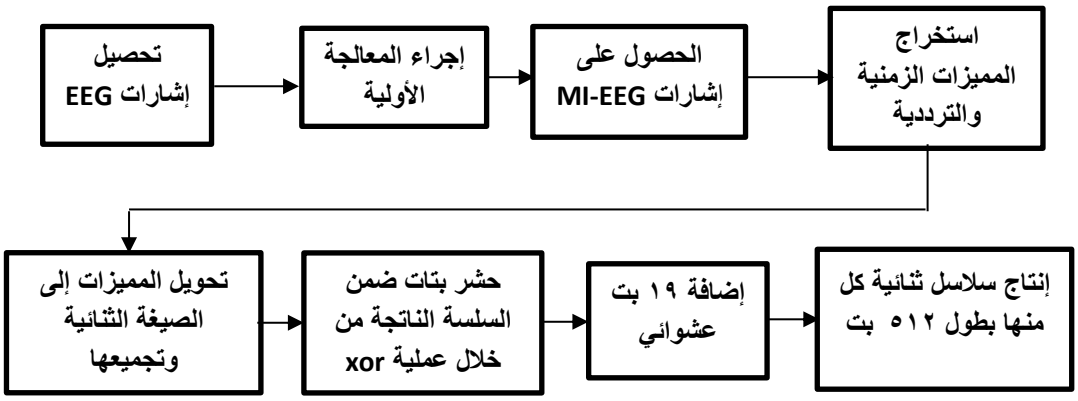
بعد ذلك أجرينا عملية حشر لبتات ضمن كل سلسلة، من خلال إجراء عملية xor لكل خانتين متتاليين وحشر النتيجة في الخانة الثالثة، وهكذا تتكرر العملية للحصول على سلسلة ثنائية بطول ٤٩٣ بت، ومن ثم إضافة 19 بت مختارة بشكل عشوائي فيصبح الناتج ٥١٢ بت لكل سلسلة، لنحصل بالنتيجة على ١٠٠٠٠سلسلة ثنائية طول كل منها ٥١٢ بت، كما هو موضح في الشكل (٣).

B_1	B_2	C_1	B_3	B_4	C_2	.....	19 بت عشوائي

$C_1 = B_1$ xor B_2

الشكل(٣): آلية تشكيل سلسلة البتات الثنائية بطول ٥١٢ بت

ويبين الشكل (4) خطوات توليد السلاسل الثنائية من إشارات تخطيط الدماغ وفق المخطط المقترح:



الشكل(٤): مخطط توليد سلاسل أرقام ثنائية من إشارات تخطيط الدماغ EEG

٣. تقييم نتائج المخطط المقترح:

تمكنا من خلال المخطط المقترح سابقاً من الحصول على سلاسل ثنائية كل منها بطول ٥١٢ بت، وفيما يأتي سنقيم هذه السلاسل من خلال عدة إحصائيات معتمدة عالمياً لمعرفة إمكانية استخدامها كسلاسل عشوائية في التطبيقات الأمنية وغيرها.

٣-١ اختبار العشوائية:

يوجد العديد من الاختبارت التي تدرس عشوائية السلاسل الثنائية، اعتمدنا في بحثنا على هذا الاختبار National Institute of Standards and Technology (NIST) الذي يُعدّ من أهمها، لأنه مخصص لدراسة عشوائية السلاسل المستخدمة لأغراض التشفير وحماية البيانات.

يتضمن اختبار NIST خمسة عشر اختباراً طورت لدراسة عشوائية السلاسل الثنائية المولدة من عتاد صلب أو برمجي بالاعتماد على مولدات الأرقام العشوائية أو شبه العشوائية [18].

طورت العديد من هذه الاختبارات من أجل سلاسل بطول كبير من مرتبة 10^3 إلى 10^7 بت، ولكن بما أنه في دراستنا نولد سلاسل بطول صغير نسبياً (٥١٢ بت) لذلك اكتفينا بمجموعة الاختبارات القابلة للتطبيق من أجل هذا الطول من السلاسل.

طبقنا اختبارات NIST على ١٢٠ سلسلة ثنائية مولدة وفق المخطط الذي اقترحناه سابقاً.

يُحدد الحد الأدنى لعدد الاختبارات الواجب اجتيازها لكل من اختبارات NIST وفق المعادلة الآتية [18]:

$$mpr = (1-\alpha) - 3\sqrt{\frac{\alpha(1-\alpha)}{k}} \qquad (٦)$$

حيث، α تمثل مستوى الأهمية وهنا تأخذ القيمة 0.01 ، أما k فيمثل عدد السلاسل المختبرة وهنا $k = 120$.

ومنه يكون الحد الأدنى للنجاح هو $96\ \%$. أي من أجل كل اختبار يجب أن يكون عدد السلاسل الناجحة (العشوائية) هو ١١٥ سلسلة أو أكثر من أصل ١٢٠ سلسلة مختبرة.

ينتج عن كل اختبار قيمة لـ P والتي من خلالها يُحدد فيما إذا كانت السلسة عشوائية أم لا. فإذا كانت قيمة P الناتجة أكبر من قيمة α تكون السلسلة عشوائية وعدا ذلك تكون غير عشوائية. يبين الجدول (٢) نتائج الاختبارات التي نفذناها باستخدام اختبار NISTSP800-22 [19].

الجدول (٢): يمثل نتائج اختبارات NIST

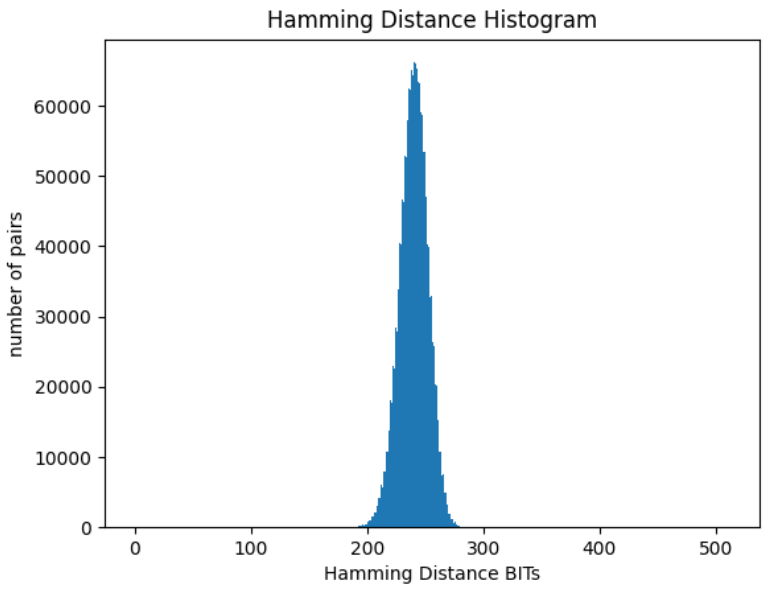
الاختبار	نسبة النجاح	النتيجة
The frequency(monobit)test	99%	pass
Frequency test within a block	100%	Pass
The Runs test	97%	Pass
The longest Run of ones in a block	96%	Pass
The discrete Fourier Transform test	98%	Pass
The Approximate Entropy test	97%	Pass
The cumulative sum test(Forward)	96%	Pass
The cumulative sum test(backward)	96%	Pass
The serial test	97%	Pass

نلاحظ من الجدول السابق أن السلاسل الثنائية المولدة وفق المخطط المقترح قد اجتازت جميع الاختبارات ويمكن أن نحكم عليها بأنها سلاسل عشوائية.

٣-٢ اختبار التميز (التفرد):

نعتمد على هذه الإحصائية لتحديد مدى التميز (الاختلاف) بين السلاسل العشوائية المولدة من أجسام مختلفة، وتقاس هذه الإحصائية من خلال مسافة هامينغ HD(Hamming Distance) والتي تحسب عدد المواضع المختلفة بين كل سلسلتين. بالنسبة للسلاسل الثنائية يجب أن تكون مسافة هامينغ تابعة للتوزع الطبيعي ومنه يجب أن يكون متوسط مسافة هامينغ مساوياً تقريباً لـ 50% من طول السلسلة العشوائية[11].

من أجل تطبيق مسافة هامينغ ولدنا ملف يحوي ٢٠٠٠ سلسلة عشوائية من قاعدة البيانات التي اعتمدناها في بحثنا هذا. وحسبنا مسافة هامينغ بين هذه السلاسل فحصلنا على النتيجة الموضحة في الشكل (5)، حيث يمثل المحور الأفقي مسافة هامينغ مقدرة بالبت، والمحور الشاقولي يمثل عدد الأزواج التي تمتلك نفس مسافة هامينغ.



الشكل(5): مسافة هامينغ للسلاسل الثنائية المولدة

نلاحظ من الشكل السابق التوزع الطبيعي لمسافة هامينغ، إذ أن متوسط HD يساوي ٤٦,٨ % وهو قريب جداً من ٥٠% من طول السلسلة العشوائية، ومنه نستنتج أن السلاسل المولدة وفق المخطط المقترح في بحثنا هذا فريدة ومتمايزة .

الاستنتاجات والتوصيات:

تمكنا في بحثنا هذا من توليد سلاسل بتات اعتماداً على إشارة تخطيط الدماغ الخاصة بتخيل الحركة EEG-MI، حيث أجرينا المعالجة الأولية لهذه الإشارات، ومن ثم وضعنا آلية معينة لاستخلاص المميزات المفيدة من هذه الإشارات وترتيبها وفق نمط معين لتشكيل سلاسل ثنائية بطول ٥١٢ بت. يتمتع المخطط المقترح في بحثنا بما يأتي:

١- أكثر فعالية من الدراسات السابقة من ناحية تعقيد النظام والتكلفة، إذ اعتمدنا في بحثنا على ٦ الكترودات فقط موجودة ضمن منطقة القشرة الحسية الحركية، والتي كانت كافية لتزويدنا بالمعلومات المفيدة المطلوبة. كما أنه أكثر فعالية من ناحية الاستهلاك الزمني، إذ استغرقت التجربة المستخدمة فقط ٤ ثواني، وتمكنا من خلالها توليد سلاسل بطول ٥١٢ بت.

٢- أخضعت السلاسل الناتجة عن هذا المخطط لاختبار العشوائية NIST وقد تبين معنا أن هذه السلاسل قد اجتازت الاختبارات القابلة للتطبيق من أجل سلاسل بطول ٥١٢ بت.

٣- درسنا مسافة هامينغ للسلاسل الثنائية لمعرفة مدى التميز، وقد تبين أن هذه السلاسل متمايزة وفريدة، وهذا يضمن عدم القدرة على التنبؤ بمميزات إشارة EGG لشخص ما من معرفة مميزات إشارة EGG لشخص آخر.

٤- يتمتع المخطط المقترح ببساطة العمليات المستخدمة إذ لم تُستخدم توابع رياضية معقدة أو تخضع السلسلة لأي نوع من الترميز التي قد تستهلك موارد الشبكة المحدودة إذ أنه بعد استخلاص المميزات استخدمنا فقط عملية XOR والتي تعد من أبسط العمليات المنطقية.

مما سبق نستنتج فعالية استخدام إشارات تخطيط الدماغ في توليد أرقام عشوائية، إذ يمكن اعتبار إشارات EEG مصدراً للأرقام العشوائية الصحيحة TRNGs، أو يمكن استخدامها كدخل لمولدات الأرقام شبه العشوائية PRNGs . ونستنتج أيضاً أن السلاسل الثنائية المولدة وفق المخطط المقترح في هذا البحث يمكن استخدامها كمفاتيح تعمية في شبكات WBSNs وغيرها من التطبيقات الأمنية، إذ أن هذه السلاسل تتميز بالعشوائية والخصوصية التامة، وتمتلك الطول المناسب لتطبيقها مع خوارزميات التشفير الشهيرة. إضافة إلى أنها لا تستهلك موارد الشبكة المحدودة.

نقترح في نهاية بحثنا دراسة إمكانية تطوير المخطط المقترح هنا لتوليد سلاسل بتات عشوائية من خلال إشارات تخطيط الدماغ بفعالية أكبر مستفيدين من تقنيات الذكاء الصنعي. ودراسة إمكانية دمج أكثر من علامة حيوية لإنتاج سلاسل ثنائية أكثر طولاً وصالحة لاستخدامها كمفاتيح تعمية في شبكات WBSNs .

References:

[1] NGUYEN, D.; TRAN, D.; MA, W. and NGUYEN, Kh., *EEG-Based Random Number Generators*. Springer International Publishing AG, PP. 248-256, 2017.

[2] GAVAS, R. and Navalyal, G., *Fast and Secure Random Number Generation using Low-cost EEG and Pseudo Random Number Generator*, IEEE, International Conference On Smart Technology for Smart Nation, PP.369- 374, 2017.

[3] KAUR, P.; KUMAR, N. and SINGH, M., *Biometric cryptosystem: a comprehensive survey*. Multimed Tools Appl, Vol.82, PP.16635-16690, 2023.

[4] BANSAL, M.; KARDAM, H.; KHAIRWAL, H.; SHARMA, J. and NARANG, S., *Review on using biometric signals in random number generators*. No.2320-5407, PP. 1543-1550 , 2019.

[5] EEG Motor Movement/Imagery Dataset. https://physionet.org/content/eegmmidb/1.0.0/. Last visit at August 2024.

[6] https://www.python.org/downloads/release/python-31011/. Last visit at August 2024.

[7] RAKHMATULIN, I.; DAO, M.; MANDIC, D. and NASSIBI, A., *Exploring Convolutional Neural Network Architectures for EEG Feature Extraction*, sensors, 2024.

[8] BEYROUTHY, T.; MOSTAFA, N.; ROSHDY,A.; KARAR, A. and ALKORK, S., *Review of EEG-Based Biometrics in 5G-IoT: Current Trends and Future Prospects*, applied sciences, 2024.

[9] CHEN, G., *Are electroencephalogram (EEG) signals pseudo-random number generators?*, J. Comput. Appl. Math. 268, PP.1– 4 , 2014.

[10] BAJWA, G. and DANTU, R., *Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms*, ScienceDirect, No. 62, PP.95 – 113, 2016.

[11] KUMAR, P.; SAINI , R.; KAUR , B.; ROY, P. and SCHEME, E., *Fusion of Neuro-Signals and Dynamic Signatures for Person Authentication*, sensors, Vol. 19, No. 4641, 2019.

[12] RAHMAN, A.; CHOWDHURY, M.; KHANDAKAR, A.; KIRANYAZ,S. and et al, *Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms*, IEEE, Vol. 2017, 2021.

[13] ZEYNALI, M.; SEYEDARABI, H. and TAZEHKAND, M., *Development of a Unique Biometric-based Cryptographic Key Generation with Repeatability using Brain Signals*, Journal of AI and Data Mining, Vol. 8, No. 3, PP.343-356, 2020.

[14] DAS, R.; MAIORANA, E. and P. CAMPISI, P., *Motor imagery for EEG biometrics using convolutional neural network*, in Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2062–2066, IEEE, Calgary, Canada, April 2018.

[15] BAK, S. and JEONG, J., *User Biometric Identification Methodology via EEG-Based Motor Imagery Signals*, IEEE, Vol. 2017-0-00451, 2023.

[16] Nguyen, D.; Tran, D.; Sharma, D. and Ma, W., On *the study of EEG-based cryptographic key generation*, Procedia Computer Science, vol. 112, PP. 936–945, 2017.

[17] DAMAŠEVIIIUS, R.; MASKELINAS, R.; KAZANAVIIIUS, E. and WOFNIAK, M., *Combining Cryptography with EEG Biometrics***,** Computational Intelligence and Neuroscience, 2018.

[18] RUKHIN, A.; SOTO, J.; NECHVATAL, J.; SMID, M. and BARKER, E., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Natl. Inst. Standards Technol., Gaithersburg, USA, Tech. Rep. 800-22rev1a, 2010.

[19] https://github.com/stevenang/randomness_testsuite . Last visit at August 2024.