Generation Secured Cryptography Keys In Wireless Body Sensor Networks Using Electrocardiogram (ECG) Signals

Dr. Boushra Maala[*]
Khadijeh Iskander[**]

(Received 23 / 4 / 2024. Accepted 3 / 10 / 2024)

□ ABSTRACT □

Wireless Body Sensor Networks (WBSNs) consist of number of small size and limited sources sensor nodes. These sensors can be placed permanently or semi- permanently inside patient body or it can be located on the patient skin for medical issue. These sensors can sense certain parameters from the body that called biometric parameters. Considering the importance of transmitted data in these networks, so the study of security issues and protecting telecommunication are very important for these special-cases and limited-resources networks.

Using biometric parameters is very effective way to protect communication over WBSNs. We can use patient body to generate cryptography keys by biometric parameters, and we call them biometric keys. Even that using traditional biometric parameters increases security degree in protection systems, it has many disadvantages, which encouraged using more effective biometric parameters such as Electrocardiograms (ECG).

In this research, we use ECG signal to generate binary strings depending on MIT_BIH Arrhythmia database. We could generate binary strings, each of them has size at 512 bits. We study the randomness of these strings by NIST. Also, we study distinctiveness by Hamming Distance. This research proved that these binary strings could be used as cryptography keys in WBSNs.

Keywords: Wireless Body Sensor Networks (WBSNs), biometric parameters, ElectroCardioGram (ECG), random number generation, NIST.

[*] **Associate Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. boushra.maala@gmail.com**
[**] **PhD Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. khadijeh.iskander@tishreen.edu.sy**

توليد مفاتيح تعمية آمنة في شبكات حساسات الجسم اللاسلكية باستخدام إشارة تخطيط القلب الكهربائية ECG

د. بشرى معلا•

خديجة اسكندر ••

(تاريخ الإيداع 23 / 4 / 2024. قُبِل للنشر في 3/ 10 / 2024)

□ ملخّص □

تتكون شبكة حساسات الجسم اللاسلكية Wireless Body Sensor Networks (WBSNs) من عقد حساسة صغيرة الحجم ومحدودة الموارد قابلة للزرع بشكل دائم أو شبه دائم داخل جسم المريض، أو تتوضّع على سطح الجلد لأغراض طبية محددة، إذ تتحسّس بارامترات معينة من جسم المريض، تدعى هذه البارامترات بالعلامات الحيوية. ونظراً لحساسية البيانات المرسلة، فإن دراسة القضايا الأمنية وتوفير سبل الحماية للاتصالات يعدّ أمراً مهمّاً في هذا النوع من الشبكات ذات الطبيعة الخاصة والموارد المحدودة.

يعدّ استخدام العلامات الحيوية من أكثر الطرائق الفعالة في حماية الاتصالات ضمن شبكات الـ (WBSNs)، إذ يُستخدم جسم المريض نفسه كوسيلة لتوليد مفاتيح تعمية من خلال العلامات الحيوية ويطلق عليها اسم المفاتيح البيومترية. ورغم أن استخدام العلامات الحيوية التقليدية قد رفع مستوى الأمن ضمن أنظمة الحماية إلا أنه يعاني من عدة سلبيات، مما دفع إلى التوجه إلى علامات حيوية جديدة أكثر فعالية مثل حساسات تخطيط كهربائية القلب ElectroCardioGram (ECG).

اعتمد البحث على إشارة تخطيط القلب الكهربائية (ECG) في توليد سلاسل من البتات باستخدام قاعدة البيانات MIT_BIH Arrhythmia ، إذ ولدت سلاسل ثنائية كل منها بطول 512 بت ، ودرست عشوائية هذه السلاسل من خلال الاختبارات الإحصائية للمعهد الوطني للمعايير والتكنولوجيا NIST، كما دُرست خاصية التميز (التفرد) لهذه السلاسل من خلال مسافة هامينغ، وتبين أن هذه السلاسل آمنة لاستخدامها كمفاتيح تعمية في شبكات WBSNs.

الكلمات المفتاحية: شبكات حساسات الجسم اللاسلكية (WBSNs) ، العلامات الحيوية، حساس تخطيط كهربائية القلب (ECG)، توليد أرقام عشوائية، NIST .

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

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

مقدّمة:

وفقاً لمنظمة الصحة العالمية، تُعدّ أمراض القلب والأوعية الدموية السبب الرئيس للوفيات في العالم. إذ يمكن التقدير أنَ عدد الوفيات الناتجة عن أمراض القلب والسكتة القلبية سيصل إلى 23.3 مليون في حلول عام 2030. كما أشارت هذه المنظمة إلى أنّه في حلول عام 2025 سيكون عدد الأشخاص الذين تتجاوز أعمارهم الستين عاماً أكبر من عدد الأطفال الذين لم يتجاوزوا الخمس سنوات. ومن المتوقع حسب مكتب الإحصاء في الولايات المتحدة أن يتجاوز عدد المسنين الذين يحتاجون إلى رعاية صحية السبعين مليوناً في حلول عام 2025. وهذا ما دفع العديد من البلدان والدول المتقدمة إلى دعم هيئات الرعاية الصحية ودور المسنين والعمل على كيفية تطويرها[1].

إن التطور في مجال الالكترونيات وتقنيات الاتصالات اللاسلكية وتصميم وحدات المعالجة والحساسات صغيرة الحجم والتي تستهلك مقداراً منخفضاً من الاستطاعة قد ساهم في توجه الباحثين إلى تطوير نمط جديد من الشبكات يُعرف بشبكات حساسات الجسم اللاسلكية Wireless Body Sensor Networks (WBSNs) التي تُعدّ تقنية للمراقبة المستمرة عن بُعد للنشاط الفيزيولوجي والسلوكي لجسم الإنسان فتلعب بذلك دوراً كبيراً في تأمين الرعاية الصحية عن بعد [2].

تتألف هذه الشبكة من عقد حساسة صغيرة الحجم، ذاتية التغذية ومحدودة الموارد قابلة للزرع بشكل دائم أو شبه دائم داخل جسم المريض أو تتوضع على سطح الجلد لأغراض طبية محددة، إذ تتحسس بارامترات معينة من جسم المريض مثل تخطيط كهربائية القلب ElectroCardioGram (ECG) وتخطيط كهربائية الدماغ (EEG) ElectroEncephaloGraphy، و مراقبة الحركة، وضغط الدم، وحرارة الجسم، ونسبة السكر في الدم...الخ [2].

لقد أثبتت شبكات WBSN أنها أساس مهم في منظومة العناية الصحية، لذا فإن استخدامها يلحظ انتشاراً واسعاً في السنوات الأخيرة، ونظراً لحساسية البيانات المنقولة عبر الشبكة و المتعلقة بالحالة الصحية للمريض فإن قضايا الأمن والخصوصية تُعدّ أمراً مهماً للدراسة، إذ أنّ أي تسريب أو تلاعب في سجلات المريض قد تودي بحياته، ومن الممكن استغلال هذه السجلات لأغراض أخرى. لذا كان هناك العديد من الهيئات والمنظمات المختصة بوضع قواعد وقوانين تخصّ قضايا الأمن في شبكات WBSN وأهمها[3]:

The American Health Insurance Portability and Accountability Act(HIPAA)
Health Information Technology for Economic and Clinical Health Act(HITECH).

اقترحت العديد من تقنيات الحماية لضمان متطلبات الأمن في هذه الشبكات، وتعدّ عملية توليد مفاتيح تعمية آمنة وتوزيعها وحمايتها أمراً مهمّاً لضمان فعالية هذه التقنيات. استخدمت العلامات الحيوية التي تعدّ من أكثر الوسائل الأمنية فعالية في هذه الشبكات، إذ تستخدم خصائص جسم المريض كوسيلة لتوليد مفاتيح وبصمات حيوية خاصة بهذا المريض [3,4].

أهمية البحث وأهدافه:

إن تطور شبكات WBSNs ودورها الفعال المهم في الرعاية الصحية والمراقبة الطبية عن بعد للمرضى والمسنين بالإضافة إلى تطبيقاتها العديدة، جعل هذا النوع من الشبكات قضية مهمة في الكثير من البلدان، ونظراً لحساسية المعلومات المرسلة عبر هذه الشبكة والخطورة الناتجة عن اختراق هذه المعلومات التي قد تودي بحياة الإنسان في بعض الحالات، فإن تحقيق متطلبات الأمن والعمل على توفير الحماية لهذا النوع من الشبكات يعدّ أمراً مهماً.

يهدف هذا البحث إلى استخدام العلامة الحيوية ECG المقاسة من جسم المريض في توليد سلاسل بتات عشوائية يمكن استخدامها كمفاتيح تعمية آمنة.

طرائق البحث ومواده:

تم تحصيل إشارة تخطيط القلب الكهربائية من قاعدة البيانات MIT-BIH Arrhythmia المضمنة في PhysioBank التي تعدّ من أشهر قواعد البيانات المستخدمة لأغراض التصنيف ودراسة القضايا الأمنية المتعلقة بالعلامات الحيوية. تتضمن قاعدة البيانات هذه العديد من تسجيلات إشارة ECG لأشخاص من الجنسين تتراوح أعمارهم من 23 وحتى 89 سنة، مدة كل منها 30 دقيقة، وتردد أخذ العينات هو 360عينة في الثانية [5].

اعتمدت هذه الدراسة على قاعدة البيانات waveform (WFDB) وهي عبارة عن حزمة برمجية تتضمن العديد من المودولات التي تتعامل مع إشارة تخطيط القلب الكهربائية من خلال قراءتها وتحليل بارامتراتها [6].

وبرمجت جميع خطوات المخطط المقترح هنا باستخدام لغة الـ Python الإصدار 3.10 [7].

1- الدراسات المرجعية:

نظراً لطبيعة شبكات الـ WBSNs ومحدودية موارد الشبكة فإنّ هذا يفرض قيوداً على استخدام الخوارزميات التقليدية من أجل توليد سلاسل عشوائية لاستخدامها كمفاتيح تعمية، لذا كما ذكرنا سابقاً إنّ استخدام العلامات الحيوية هو الطريقة الأكثر شيوعاً لتأمين الاتصال ضمن شبكات الـ WBSN، إذ يُستخدم جسم المريض نفسه كوسيلة لتوليد مفاتيح التشفير للحساسات المتصلة بالجسم من خلال العلامات الحيوية مثل بصمة الإصبع وبصمة القزحية وبصمة الوجه، ويُطلق على هذه المفاتيح اسم المفاتيح البيوميترية [8].

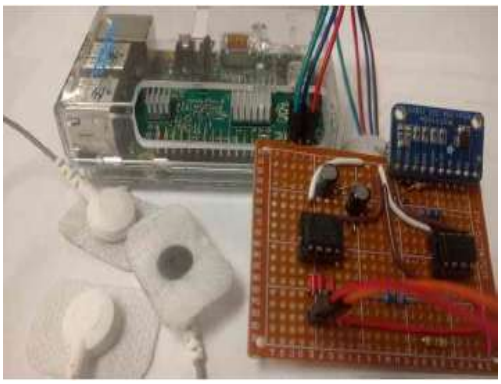
رغم أن استخدام العلامات الحيوية مثل بصمة الإصبع أو الوجه أو الصوت وخط اليد قد رفع مستوى الأمن ضمن أنظمة الحماية، ولكن المعلومات التي تحملها هذه العلامات الحيوية هي موروثة وفريدة ولا يمكن تغييرها من أجل استخدامها مع تطبيقات مختلفة، لذا في حال سُرقت العلامة الحيوية المستخدمة فإن جميع المفاتيح السرية المولدة 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 ضمان أمن أي نظام يتطلب تغيير مفاتيح التعمية كل فترة زمنية معينة. وبما أن العلامات الحيوية التقليدية موروثة وغير قابلة للتغيير فإن المفاتيح 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 [9].

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 [10] .

كل ما سبق دفع للتوجه لعلامات حيوية جديدة لا تمتلك نقاط الضعف الموجودة في العلامات الحيوية التقليدية، ونذكر منها إشارات حساسات تخطيط كهربائية القلب (ECG) ElectroCardioGram، وتخطيط كهربائية الدماغ ElectroEncephaloGraphy(EEG)، وتخطيط الصورة الضوئية PhotoPlethymoGram(PPG).

1- 1- حساس تخطيط كهربائية القلب (ECG) ElectroCardioGram:

يسجل هذا الحساس النشاط الكهربائي للقلب من خلال لصق الكترودات صغيرة في أماكن معينة من جسم الإنسان، إذ ينتج القلب نبضات كهربائية صغيرة تنتشر من خلال عضلة القلب وتتسبب في حدوث انقباض. تكشف هذه الالكترودات التغيرات الكهربائية الضئيلة على الجلد التي تنشأ عندما تتعرض عضلة القلب إلى إزالة الاستقطاب خلال كل نبضة. تُضخم وتُعالج هذه التغيرات وتُسجل الإشارة ECG التي تُعدّ انعكاساً لنشاط القلب الكهربائي، ويبين الشكل (1) صورة لحساس ECG.



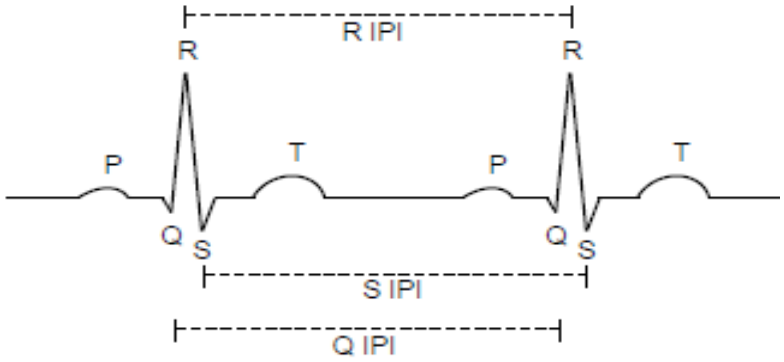
الشكل (1) صورة لحساس ECG

تساهم إشارة ECG في تشخيص حالات صحية مهمّة مثل [11,12]:

- عدم انتظام ضربات القلب.
- ضيق التنفس.
- التعب والإجهاد المستمر.
- وجود دقات غير طبيعية في القلب.
- تشخيص بعض أمراض القلب.
- متابعة كفاءة أدوية القلب.
- مراقبة نشاط القلب بعد إجراء تمارين معينة.
- وجود ألم في الصدر

يكون مطال إشارة ECG صغيراً جداً ويتراوح عادة بين (0.5−4)mV لذا تُضخم بمضخمات مناسبة، إنها تتألف من سلسلة من الموجات المتكررة، وكما هو مبين في الشكل (2) فإن كل دورة تتألف من 5 موجات أساسية هي: Q , P , R ,S ,T ، ترمز كل موجة من خلال نقطة معينة في القلب عند سريان التيار الكهربائي فيها تبدأ من الأذين وصولاً إلى البطين، وترمز الفترات الموجودة بين الموجات إلى الوقت الذي احتاجه التيار للوصول من نقطة إلى أخرى. كل المعلومات المزوّدة من خلال إشارة ECG موجودة بين الترددات Hz (0.05-100)، وطول QRS عموماً بين sec (0.06−0.1)، تشير الخاصية Inter-Pulse-Intervals (IPI) للفترة الزمنية الفاصلة بين قمتين متشابهتين متجاورتين [13].

تعدّ هذه الموجات الخمس: P,Q,R,S,T و الفترات (P-R) ، (Q-T) ، (Q - R) ، (R - S)، و IPI الصفات المميزة لإشارة ECG التي تُستخدم لأغراض الموثوقية في كثير من المخططات الأمنية.



الشكل(2): إشارة ECG

تتمتع إشارة ECG بالخصائص الآتية :

عامة universality ، فريدة uniqueness، مستقرة stability ، قابلة للقياس collectability، قابلة للتطبيق acceptability ، صعب تقليدها أو سرقتها Circumvention. وهذا ما يجعلها مناسبة للاستخدام في أغراض الوثوقية والأمن.

2-1- استخدام ECG في توليد أرقام عشوائية:

اعتمدت العديد من الدراسات على إشارة تخطيط القلب الكهربائية في توليد أرقام عشوائية، استخدمت بعض هذه الدراسات قيم مطالات إشارة ECG كمميزات لأغراض أمنية [13]، ولكن هذه المطالات لإشارتي ECG مقاستين بالتزامن من نقطتين مختلفتين من جسم الإنسان تكون متفاوتة بشكل ملحوظ وتعتمد بشكل أساس على المسافة من القلب. استخدمت دراسات أخرى قيم IPI فقط لإشارة ECG ولكن هذه الدراسات تعاني من أداء منخفض، إذ أن الزمن الفاصل بين نبضتي قلب متتاليتين يمكن تحديده من خلال كاميرا أو تحليل لون الجلد وهذا يجعل الخوارزمية المعتمدة على هذه القيم فقط أقل أماناً [14,15].

اعتمدت الدراسة [16] على قيم IPI، إذ أُخذت آخر أربع بتات فقط من كل قيمة IPI، فمن أجل توليد سلسلة بطول 128 بت كان هناك حاجة لـ 33 ضربة قلب؛ أي زمن يتراوح ما بين 20-30 ثانية. أما الدراسة [17] اعتمدت على نبضة قلب واحدة واستخرجت منها جميع المميزات لإنتاج (16 بت)، وبالنتيجة كان هناك حاجة لـ 8 نبضات قلب لإنتاج سلسلة بطول 128 بت وهذا يعد غير فعال من ناحية استهلاك الزمن.

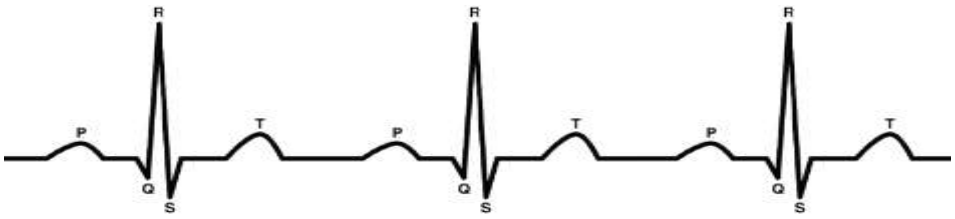
نستنتج مما سبق أهمية تطوير مخطط لتوليد سلاسل بتات عشوائية بالاعتماد على إشارة تخطيط القلب الكهربائية بحيث يراعي استهلاك الزمن ويحقق إنتاجية أعلى وبالنتيجة مستوى أمن أعلى.

2- المخطط المقترح :

نبين فيما يأتي الخطوات التي اتُّبعت لتوليد سلسلة بتات عشوائية من مميزات إشارة ECG بالاعتماد على قاعدة البيانات MIT_BIH Arrhythmia :

1- من أجل تسجيل معين، حُصلّت إشارة ECG لمدة زمنية بحيث تتضمن 3 نبضات قلب كاملة على الأقل.

2- استخلاص ثلاث نبضات قلب (PQRST) متتالية من التسجيل السابق كما هو موضح في الشكل (3).



الشكل(3): تتابع ثلاث نبضات من إشارة ECG

3- تطبيق خوارزمية XQRS لتحديد مواقع القمم R في النبضات المحصلة.

تعد خوارزمية XQRS أحد الأصناف المضمنة في الحزمة البرمجية WFDB، إذ تكتشف وتحدد موقع القمة R في التعقيد QRS ضمن إشارة ECG . تمتلك هذه الخوارزمية ميزة إضافية وهي تطبيق مرشح تمرير حزمة للإشارة بين (5-20) Hz [6]. ومنه سنحصل على مواقع القمم (R1 , R2 , R3).

4- تطبيق تابع diff للحصول على RR-interval . ومنه سينتج لدينا (R1R2 , R2R3).

5- من أجل كل نبضة قلب كاملة PQRST استُخلصت مواقع القمم P,Q,R,S,T وحُسبَ الوسيط mean . ومن ثم حساب الفروقات بين القمم : PQ, QR, RS, ST, RT, PR . كما هو موضح وفق خطوات الخوارزمية (1).

الخوارزمية(1): خطوات استخلاص مواقع القمم.

```
**Extract individual P, Q, R, S, T peaks:**
1:  **FOR EACH** segment:
2:      Find maximum value (R peak)
3:      Find minimum value before R (Q peak)
4:      Find maximum value before Q (P peak, handle edge cases)
5:      Find minimum value after R (S peak)
6:      Find maximum value after S (T peak):
**Calculate feature values:**
7:  Calculate P-Q, P-R, Q-R, R-S, R-T, S-T features
```

6- تحويل جميع القيم التي حُصلَ عليها من أجل نبضات PQRST الثلاثة إلى الصيغة الثنائية.

ترتيبها وفق آلية معينة للحصول على سلسلة ثنائية بطول 381 بت كما هو مبين في الشكل (4):

B1	B2	B3	.....	B381

الشكل(4): سلسلة البتات المستخلصة من ثلاث نبضات PQRST

7- من أجل هذه السلسلة الثنائية حُشرت بتات إضافية ضمنها وفق آلية معينة تتضمن عملية XOR للحصول على سلسلة ثنائية بطول 508 بت، ومن ثم إضافة الترميز الثنائي للعدد 3 ممثلاً بأربع خانات، ومنه سنحصل على سلسلة ثنائية مكونة من 512 بت كما هو موضح في الشكل (5).

B1	B2	B3	C1	B4	B5	B6	C2	.....	C508	0011

$C_1 = B_1 \text{ xor } B_2 \text{ xor } B_3$ $C_2 = B_4 \text{ xor } B_5 \text{ xor } B_6$

الشكل(5): سلسلة البتات الناتجة وفق المخطط المقترح

3- تقييم نتائج المخطط المقترح:

تمكنا من خلال المخطط المقترح سابقاً من الحصول على سلاسل ثنائية كل منها بطول 512 بت، وفيما يأتي سنقيم هذه السلاسل من خلال عدة إحصائيات معتمدة عالمياً لمعرفة إمكانية تطبيقها كمفاتيح تعمية في شبكات الـ WBSNs :

أولاً: اختبار العشوائية:

توجد 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 (512 بت) لذلك اكتفينا بمجموعة الاختبارات القابلة للتطبيق من أجل هذا الطول من السلاسل.

طبقنا اختبارات NIST على 100 سلسلة ثنائية مولدة وفق المخطط الذي اقترحناه سابقاً بالاعتماد على مجالات عينات مختلفة للتسجيلات الموجودة في قاعدة البيانات المعتمدة في دراستنا.

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

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

إذ تمثّل α مستوى الأهمية وهنا تأخذالقيمة 0.01 ، أما k فيمثل عدد السلاسل المختبرة وهنا $k = 100$.

ومنه يكون الحد الأدنى للنجاح هو 96% . أي من أجل كل اختبار يجب أن يكون عدد السلاسل الناجحة (العشوائية) هو 96 سلسلة أو أكثر من أصل 100 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 (1) نتائج الاختبارات التي نفذناها باستخدام اختبار NISTSP800-22 [19].

الجدول (1): نتائج اختبارات NIST

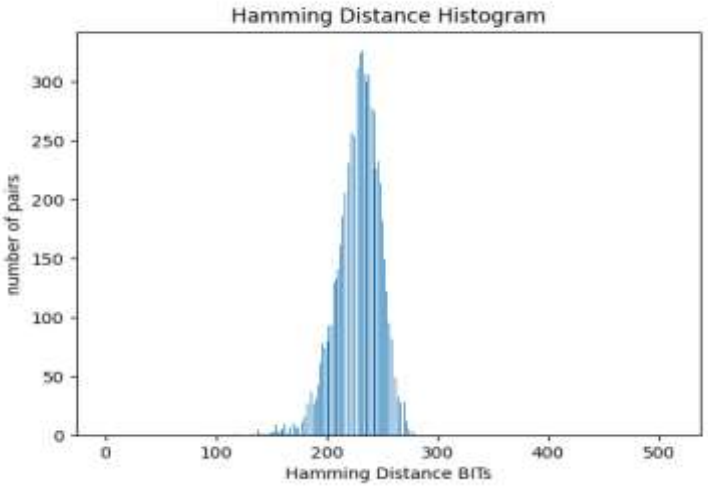
الاختبار	نسبة النجاح	النتيجة
The frequency(monobit)test	97%	pass
Frequency test within a block	100%	Pass
The Runs test	96%	Pass
The longest Run of ones in a block	96%	Pass
The discrete Fourier Transform test	98%	Pass
The Approximate Entropy test	100%	Pass
The cumulative sum test(Forward)	98%	Pass
The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

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

ثانياً: 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 [14].

من أجل تطبيق مسافة هامينغ ولدنا ملف يحوي 120 سلسلة عشوائية من قاعدة البيانات التي اعتمدناها في بحثنا هذا. وحسبنا مسافة هامينغ بين هذه السلاسل فحصلنا على النتيجة الموضحة في الشكل (6)، إذ يمثل المحور الأفقي مسافة هامينغ مقدرة بالبت، ويمثّل المحور الشاقولي عدد الأزواج التي تمتلك نفس مسافة هامينغ.



الشكل(6): مسافة هامينغ للسلاسل الثنائية المولدة

نلاحظ من الشكل السابق التوزع الطبيعي لمسافة هامينغ، إذ أن متوسط HD يساوي 45.31 % وهو قريب جداً من 50% من طول السلسلة العشوائية، ومنه نستنتج أن السلاسل المولدة وفق المخطط المقترح في بحثنا هذا فريدة ومتمايزة .

ثالثاً: تقييم الأمن:

كما ذكرنا سابقاً، تمتلك إشارة ECG خاصية التميز والتفرد ومنه فإنّ السلاسل الثنائية المستخلصة منها متمايزة وهذا ما يحقق متطلب السرية والخصوصية، أي؛ لا يمكن التنبؤ بمميزات إشارة ECG لشخص ما من معرفة مميزات إشارة ECG لشخص آخر.

تمتلك السلاسل الثنائية التي حصلنا عليها خاصية العشوائية، كما أنها تمتلك الطول الكافي الذي يجعل من الصعب كسرها، حتى لو عُرفت المميزات الخاصة بإشارة ECG فإنه من الصعب معرفة السلسة الثنائية المولدة منها، بسبب إخضاع هذه المميزات لخوارزمية معينة من أجل تشكيل السلاسل الثنائية من خلال ترتيبها وفق آلية معينة وحشر بتات إضافية ضمنها وإضافة خانات في نهايتها. هذا بدوره يزيد من عدم قدرة المهاجم من كشف المفتاح المولد من هذه العلامة الحيوية.

الاستنتاجات والتوصيات:

ولدنا في بحثنا هذا سلاسل بتات بالاعتماد على إشارة تخطيط القلب الكهربائية ECG، ووضعنا آلية معينة لاستخلاص مميزات إشارة ECG باستخدام توابع برمجية في مكتبة WFDB، ومن ثم تم التعامل مع هذه المميزات وترتيبها وفق نمط معين لتشكيل سلاسل ثنائية. يتمتع المخطط المقترح في بحثنا بما يأتي:

1- إنتاجية أعلى من الدراسات السابقة، إذ تمكنا من تشكيل سلاسل ثنائية بطول 512 بت انطلاقا من ثلاث نبضات قلب أي وسطيا (3 – 5) ثانية من تسجيل ECG بينما احتاجت الأبحاث السابقة لـ 33 ضربة قلب أي ما يعادل 20 إلى 30 ثانية لتشكيل سلسلة بطول 128 بت، وبعض الدراسات استخدمت نبضة قلب وحيدة ولكن أنتجت فقط 16 بت. لذا نجد أن هذا المخطط حقق إنتاجية أعلى خلال زمن أقل.

2- أُخضعت السلاسل الناتجة عن هذا المخطط لاختبار العشوائية NIST وقد تبين أن هذه السلاسل قد اجتازت الاختبارات القابلة للتطبيق من أجل سلاسل بطول 512 بت.

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

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

مما سبق نستنتج أنه يمكن استخدام السلاسل الثنائية المولدة وفق المخطط المقترح في هذا البحث كمفاتيح تعمية في شبكات WBSNs إذ أن هذه المفاتيح 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 توليد سلاسل ثنائية عشوائية بالاعتماد على علامات حيوية أخرى مثل إشارة تخطيط الدماغ EEG ، ودراسة إمكانية دمج أكثر من علامة حيوية لإنتاج سلاسل ثنائية أكثر طولاً وصالحة لاستخدامها كمفاتيح تعمية في شبكات WBSNs .

References:

[1] AL-JANABI, S.; AL-SHOURBAJI, I.; SHOJAFAR, M. and SHAMSHIR, Sh., *Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications.* Egyptian Informatics Journal, PP.113-122, 2017.

[2] YAGHOUBI, M.; AHMED, K. and MIAO, Y., *Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges*. Intelligent Technology Innovation Lab (ITIL), Victoria University, Ballarat Road, Footscray, Melbourne, VIC 3011, Australia, Vol.11, Issue 4, 2022.

[3] ZHONG, L.; HE, S.; LIN, J.; WU, J.; LI, X.; PANG, Y. and LI, Z. *Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey*. Sensors, Vol.22, Issue 9, 2022.

[4] JABEEN, T.; ASHRAF, H. and ULLAH, A., *A survey on healthcare data security in wireless body area networks*. Journal of Ambient Intelligence and Humanized Computing. Springer, PP. 9841–9854, 2021.

[5] MIT-BIH Arrhythmia Database. https://physionet.org/content/mitdb/1.0.0/ Last visit at December,2023.

[6] https://wfdb.readthedocs.io/en/latest/index.html . Last visit at December,2023.

[7] https://www.python.org/downloads/release/python-31011/. Last visit at December 2023

[8] WALIA, G. and GUPTA, A., *A Novel biometric cryptosystem based on cryptographic key binding with user biometrics*. ACM, Multimedia Systems, Vol.27, Issue 5, PP.877-891, 2021.

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

[10] 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.

[11] MERDJANOVSKA, E. and RASHKOVSKA, A., *Comprehensive survey of computational ECG analysis: Databases, methods and applications.* Expert Systems with Applications, Vol. 203, No. 117206, 2022.

[12] MELZI, P.; TOLOSANA, R. and RODRIGUEZ, R., *ECG Biometric Recognition: Review, System proposal, and Benchmark Evaluation.* IEEE, Vol.11, No. 3244651, PP.15555-15566, 2023.

[13] SAIFUL ISLAM, M. *Using ECG signal as an entropy source for efficient generation of long random bit sequences.* Journal of King Saud University – Computer and Information Sciences, 2022.

[14] SINHA, A.; MAHAPATRO, J. and BHABANI, B., *Random binary sequences generation using heartbeats for cryptographic keys in WBSNs*. International Journal of Sensor Networks, Vol.38, No.3, PP.191-203, 2022.

[15] PREMKUMAR, S. and MOHANA, J., *An efficient method for Secure ECG Feature Based Cryptographic Key Generation*. IJITEE, Vol.8, 8 Issue-12, PP.159-164, 2019.

[16] XU, F.; Qin, Z.; Tan, C.; Wang, B. and Li, Q., *IMDGuard: Securing implantable medical devices with the external wearable guardian*. IEEE INFOCOM, pp. 1862–1870, 2011.

[17] ZHENG, G.; FANG, G.; SHANKARAN, R.; ORGUN, M.; SALEEM, K.; and QIAO, L., *Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks.* IEEE Journal of Biomedical and Health Informatics, Vol. 21, No. 3, PP.655–663.2017.

[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 January 2024.