

تقنيات التعرف البيومتري ودورها في تعزيز وبناء هوية رقمية مؤمنة

Biometric identification technics and their role in promoting and constructing a secured digital identified.

عبد الحكيم بوقزولة*، جامعة المسيلة
مخبر العلوم السياسية الجديدة
Abdelhakim.boukezzoula@univ-msila.dz

خالد توازي، جامعة المسيلة
مخبر العلوم السياسية الجديدة
khaled.touazi@univ-msila.dz

تاريخ القبول: 2024/11/20

تاريخ الاستلام: 2024/09/30

ملخص:

في ظل التطور السريع للتكنولوجيا الذي يشهده العالم في مجال التقنيات والتطبيقات التحول الرقمي، لا سيما تقنيات التعرف البيومتري والتي تعد من بين أهم تطبيقات التكنولوجيا الرقمية الحديثة لبناء هوية رقمية للأفراد، إذ أن هاته التقنية تعتمد في الأساس على تحليل القياسات الحيوية الفريدة للأفراد باستخدام النظام البيومتري، لتشهد تقنية التعرف البيومتري العديد من الاختراقات والهجمات السيبرانية التي مست أنظمتها البيومترية بهدف الاستحواذ على بيانات المستخدمين وانتحال هويتهم واستخدامها بطرق غير قانونية للوصول إلى حساباتهم المصرفية، لذا أصبح من الضروري على العديد من الدول التفكير في تطوير تقنيات أمان متقدمة تتماشى ومتطلبات العصر الرقمي مع تعزيز الوعي الأمني لدى مستخدمي النظام البيومتري، لضمان فعاليته في حماية البيانات الشخصية للأفراد والحفاظ على خصوصيتهم وبناء هوية رقمية مؤمنة.

* المؤلف المراسل

وتأتي هاته الورقة البحثية لتقديم منظورا تحليليا حول تقنيات التعرف البيومترية واليات عملها لبناء هوية رقمية مؤمنة.

الكلمات المفتاحية: النظام البيومترية، القياسات الحيوية، البصمة البيومترية، الهوية الرقمية، التعرف البيومترية.

Abstract:

In light of the rapid development of technology worldwide in the field of technics applications, and digital transformation especially biometric identification technics , that are concerned among the important modern technology Cal digital applications to build a digital identity for individuals , to this technic depends mainly on the analysis of the unique measures of individuals using the biometric system, so that identification biometric technic witnesses many intrusions and cyberattacks that touches its biometric systems for the aim of acquiring users' information, and their identification using it in illegal ways to achieve their bank accounts, this is why it becomes necessary for many countries to think about the development of developed secured technic that go on with requirements of the digital age with rising awareness of users of the biometric system, to fulfil an effective in protection of the personal data of individuals, as building a secured digital identified.

This research paper comes to introduce an analysis look about technical biometric identity and its way of building a secured identified biometry.

Keywords: Biometric system, biometrics, biometric fingerprint, digital identify, biometric identification.



تعدُّ تقنية التعرف البيومترية واحدة من أبرز تقنيات علم الحوسبة والأمن الرقمي، حيث تعتمد هذه التقنية على استخدام القياسات الحيوية للأفراد وتحليلها بواسطة نظام بيومترية متقدم يستخدم تقنيات بيومترية للتعرف على الأفراد والتحقق من هويتهم بناءً على سماتهم البيولوجية كالوجه والأصابع وهندسة اليد وقزحية العين والسلوكية كال توقيع، الصوت وهي سمات فريدة مميزة وتختلف من فرد إلى آخر، حيث يعتمد هذا النظام على عدة التقنيات تعمل على بناء وتحديد الهوية البيومترية، عن طريق ما يسمى بخوارزميات التعرف وأنظمة مسح العينة البيومترية.

ونظراً لكون تحديد هوية الفرد البيومترية في المجتمع أصبح ضرورة حتمية لا سيما في ظل انتشار استخدام الخدمات الإلكترونية التي تُقدم عن بُعد، وجدت هذه التقنيات المتطورة تطبيقاً واسع النطاق في العديد من الخدمات الإلكترونية من خلال استخدامها الأجهزة الذكية مثل الهواتف الذكية وأنظمة الأمن والمراقبة، لذا أصبحت الحاجة إلى نظام إدارة الهوية بيومترية متطور ضرورة حتمية لتحقيق من هويات الأفراد بدقة وفعالية لحماية بياناتهم الشخصية والحد من مخاطر الاحتيال الرقمي، على اعتبار أن عملية بناء هوية رقمية مؤمنة لا تخلو من العديد من المخاطر والتهديدات، لا سيما فيما يتعلق بالأمن وسرية البيانات الشخصية.

ولفهم التعرف البيومترية يتطلب منا القيام بدراسة شاملة لمكوناته والتقنيات البيومترية المستخدمة، لذا جاءت هذه الدراسة بهدف تبسيط الضوء على آلية عمل تقنية القياسات الحيوية والنظام البيومترية باعتبارهما التقنيتين الأساسيتين لإحداث تعرف البيومترية حقيقي، مع إبراز دورهما في بناء الهوية البيومترية مؤمنة في ظل التحديات والعراقيل التي يواجهها، الأمر الذي يلزمنا طرح الإشكالية التالية:

كيف يمكن لتقنيات التعرف البيومترية أن تساهم في تعزيز الأمن الرقمي للهوية الرقمية والحد من ظاهرة انتحال الهوية؟

للإجابة على هاته الإشكالية قمنا بإتباع المنهج الوصفي التحليلي والذي يعتبر المنهج الأدق سبب والمتكامل الذي سيمكننا من تقديم رؤية شاملة ومعمقة لفهم تقنيات التعرف البيومتري (القياسات الحيوية، النظام البيومتري) من خلال شرح وصف معمق لكيفية عمل تقنيات التعرف للتحقق واذشاء الهوية البيومترية، لنقوم بتقسيم هذه الدراسة على أساس محورين رئيسيين:

- المحور الأول والذي سنتناول من خلاله شرح تقنية القياسات الحيوية واستعراض أهم الأنواع المختلفة لهاته التقنية (بصمة الإصبع، بصمة الوجه، بصمة قرنية العين، التوقيع الرقمي، البصمة الصوتية)، مع إبراز دورها كمرتكز أساسي في ظل بناء وتحديد الهوية البيومترية للأفراد.
- المحور الثاني والذي سنتطرق من خلاله إلى النظام البيومتري كتقنية رقمية والية عمله في ظل التحديات والعراقيل (داخل النظام وخارج النظام) التي قد تتخلله اثناء بناء هوية رقمية مؤمنة.

أولاً: القياسات الحيوية كمعرف لتحديد الهوية البيومترية:

تعد القياسات الحيوية كأحد الركائز الأساسية التي تعتمد عليها تقنية التعرف البيومتري لبناء هوية بيومترية للأفراد، باعتبارها معرفات فريدة للفرد وتختلف من شخص لآخر حيث لا يمكننا تصور هوية بيومترية دون استخدام السمات البيولوجية أو السلوكية.

1. تعريف القياسات الحيوية:

-تعرف القياسات الحيوية على أنها عملية التعرف على هوية الفرد أو تأكيدها بناء على سماته الفسيولوجية أو السلوكية، من خلال استخدام التقنيات البيومترية للتحقق منها، مع إمكانية الوصول إلى البيانات البيومترية، والرفع من مستوى الأمان المطلوب (ASHOK, VAKA, & P.V.G.S, 2010, p. 2402)

-يعرفها خاشك وإقبال (Khashk and Iqbal): بأنها تقنية رقمية تستخدم لتأكيد أو التعرف على هوية فرد على قيد الحياة، من خلال استخدام سماته

الفيولوجية أو السلوكية؛ وبالتالي فإن عملية التحقق تعتمد على خ صاء صنا المتأصلة أو أفعالنا (Iqbal & Qadir, 2012, p. 11).

- كما تعرفه المنظمة الدولية للتوحيد القياسي (ISO) مصطلح القياسات الحيوية على أنه "التعرف الآلي على الأفراد بناءً على خ صاء صهم البيولوجية والسلوكية". (BELHADJ, 2017, p. 5)

- أما المادة 4(14) من اللائحة العامة لحماية البيانات (اللائحة رقم 679 بتاريخ 27 أبريل 2016) فقد عرفت القياسات الحيوية على أنها "بيانات شخصية ناتجة عن معالجة تقنية محددة تتعلق بالخ صائص الفيزيائية أو الفسيولوجية أو السلوكية للشخص الطبيعي، والتي تسمح أو تؤكد التعريف الفريد لذلك الشخص الطبيعي، مثل صور الوجه أو بيانات بصمة الأصابع" (Hegheş, 2023)

2. المتطلبات الأساسية للقياسات الحيوية:

تشير السمة البيومترية إلى خاصية جسمية أو سلوكية للفرد والتي تميزه عن الآخرين، كما أنها قابلة للقياس الكمي، حيث تلعب هذه السمة دوراً مهماً في تحديد هوية البيومترية للفرد، لذا عند تصميم أي نظام بيومتري عملي فإن أحد الاعتبارات الرئيسية هي معالجة السؤال التالي: ما هي الخ صائص المحددة التي يجب أن يستخدمها النظام من أجل اتخاذ قرار دقيق بشأن هوية الفرد؟

وفقاً لـ Flynn و Anil K. Jane و Ross (2007)، هناك العديد من المتطلبات التي يجب أن تتوفر في الخ صائص البيومترية النموذجية حتى يتم اعتبارها موثوقة وفعالة، حيث تشمل هذه المتطلبات على سبيل المثال الدقة والانفراد والعالمية والديمومة وقابلية التحصيل والأداء والمقبولية ومقاومة الاحتيال وقابلية التوسع.

كما تشير الدقة إلى قدرة النظام البيومتري على تحديد الفرد بشكل صحيح، أما الانفراد فتعني أن كل فرد يمتلك سمة بيومترية تميزه عن الأفراد الآخرين، (Ross & Anil K, 2007, p17) وتتمثل هاته الخصائص فيما يلي:

✓ العالمية والانفرادية: إن كل فرد يمتلك خاصية فريدة تميزه عن غيره من الأفراد عبر انحاء العالم، لذا يجب أن تكون السمات الفيزيولوجية للأفراد مختلفة تماما، حيث لا ينبغي أن يتشارك الأفراد في خاصية واحدة وهو ما يمنح النظام البيومتري القدرة على التمييز بين شخصين (Scott, Hill, Acton, & Hughes, 2006) ويمكننا القول إن هاته الخاصية تساعد على التمييز بين التوائم الذين قد يتمتعون تقريبا بنفس السمات الفيزيولوجية (الوجه).

✓ الاستمرارية: تعتمد التقنية البيومترية على النظام الآلي لتعرف على السمات الفيزيولوجية التي لا تتأثر مع مرور الوقت، مما يجعل من الصعب تغييرها أو اتلافها إلا عمدا أو عن طريق الحوادث مثل البصمة الاصبع، قزحية العين... الخ، أما السمات التي تتغير بسرعة وبشكل كبير أثناء التقدم في العمر كالوجه والصوت فهي ليست مقبولة سائما حيويًا مفيدًا في الكثير من الأحيان (BELHADJ, 2017, p. 6)، حيث يتم الاعتماد عليها خلال فترة زمنية معينة.

✓ قابلية القياس: وتعني أن التقنية البيومترية قابلة للقياس الكمي من خلال سهولة عرضها على جهاز التعرف البيومتري (Scott, Hill, Acton, & Hughes, 2006) وكذا إمكانية رقمته الخ. صائص البيومترية وتحويلها إلى قالب بيومتري وإرسالها إلى نظام تحديد الهوية للتحليل والتحقق منها.

✓ دقة الأداء: يتمثل مفهوم الأداء في ضمان الدقة والسرع في تحديد البيانات البيومترية للهوية باستخدام نظام التعرف، للوصول إلى بيانات موثوقة في صحتها، مما يساهم ذلك في تحديد الهوية الرقمية للفرد بكل دقة (BELHADJ, 2017, p. 6)

✓ القابلية: وهي مدى استعداد الأفراد للتعاون مع النظام البيومتري وتقديم بياناتهم البيومترية بدون أي مقاومة، وهو ما يعكس ثقافتهم الرقمية من خلال مدى ميلهم للمشاركة الفعالة في توفير هذه البيانات لتحديد هويتهم في المستقبل.

✓ الاحتيال: يتم اللجوء إلى قياس الاحتيال على مستوى النظام البيومتري بصفة دورية لتقييم مدى سهولة تعرضه إلى الخداع أو المساس ببياناته، مع تقييم

قدرته في نفس الوقت على التصدي لمثل هاته الطرق، ومعرفة مدى قابلية النظام لاتخاذ القرارات الغير الدقيقة، الناتجة عن استخدام سمات بيومترية مزيفة كتقليد سمات الفرد باستخدام أدوات خاصة (الأصابع المزيفة) بهدف الوصول الغير المصرح به إلى البيانات البيو مترية لمستخدمين الأصليين (Ross & Anil K, 2007, p. 27)

3. **تقنيات القياسات الحيوية:** تم تصنيف القياسات الحيوية في العديد من الدراسات الحديثة الى نوعين رئيسيين هما:

1.3 القياسات الحيوية الثابتة: (المواصفات الفيزيولوجية أو المورفولوجية) :

وهي القياسات التي تعتمد على استخلاص البيانات البيومترية من القياسات الجسمانية للشخص، كالوجه، الأصبع، العين، قزحية العين، راحة اليد والحمض النووي إلخ. سوف نتطرق الى القياسات الحيوية الأكثر شيوعاً في الاستخدام عبر انحاء العالم وتشمل:

أ- **بصمة الوجه (Face print):** في بداية الستينيات، قام Woodrow Bledsoe بتطوير نظام شبه أوتوماتيكي مصمم للتعرف على سيمات الوجه، حيث أحدث هذا النظام ثورة في طريقة التعرف على الوجه، من خلال وضع معياراً جديداً للرفع من مستوى الدقة والفعالية في تحديد وجوه الأفراد، عن طريق استخدام الوسائل الرقمية (احمد، 2010، صفحة 5)، لذا يشكل تحديد الملامح البيومترية للوجه فيما يتعلق بالمساحة المحيطة باعتباره ميزة بيومترية تحديداً تقنياً كبيراً، حيث أدت التطورات التكنولوجية الحديثة في أساليب التعرف على الوجه إلى الرفع من دقة التعرف على الوجه، لا سيما على مدار السنوات الخمس الماضية.

ب- **خطوات التعرف على الوجوه:** ان التعرف على الوجه من خلال تبني القياسات الحيوية يتطلب اتباع الخطوات التالية، (Facial Recognition Technology, s.d.):

- اكتشاف الوجه: تتضمن هذه العملية المعقدة نوعاً ما فحصاً شاملاً للعثور على الوجه، صرنا نلاحظ الاختلافات للبنية العامة التي تشكل الوجه، مثل العينين والأنف والفم بحيث تعمل على تحديد ملامح الوجه في ظل البيئة المحيطة به وتحديد موقعها

بدقة داخل الإطار، فمن خلال هذه الميزات ستطبع التكنولوجيا تحديد واكتشاف وجود الوجه.

• تحليل الوجه: تتضمن هذه الخطوة تحليلاً شاملاً لملامح الوجه الذي يعتمد عادةً على مبادئ هندسة الوجه، التي يشار إليها في بعض الأحيان باسم المعالم أو النقاط العقدية، حيث يتم قياس وتقييم النقاط الرئيسية المختلفة على الوجه، كالمسافة بين العينين وشكل خط الفك والخصائص المحددة لعظام الخد والشفاه والأنف فيتم فحص هذه الجوانب بدقة، وتوليد فهم شامل لبنية الوجه المستهدفة.

• استخراج الميزة: بعد تحليل ملامح الوجه، يتم استخراج الملامح الرئيسية للوجه، بهدف استخدامها لاحقاً لإنشاء بصمة الوجه أو قالب بيومترى للوجه على شاكلة هندسة رقمية للخصائص الفريدة والمعقدة لوجه الشخص، حيث من خلال خاصية استخراج هذه البيانات وتخزينها تصبح التكنولوجيا قادرة على إنشاء نقطة مرجعية مميزة لكل وجه.

• المقارنة: وهي عملية التعرف على الوجوه من خلال مقارنة قالب الوجه الذي تم إنشاؤه مسبقاً وحفظه بقاعدة البيانات البيومترية الشاملة للوجوه المعرفة، من خلال استخدام خوارزميات المطابقة المتقدمة، التي تعمل على مقارنة قالب الوجه مع قاعدة البيانات التي تحتوي على قوالب مخزنة، في ظل ظروف الخارجية المحيطة (الإضاءة وتعبيرات الوجه المختلفة والزوايا المختلفة) وتحديد ما إذا كان التطابق موجوداً أم لا.

ب. بصمة قرنية العين (Iris recognition): يستخدم في عملية مسح قرنية العين ضوء الأشعة تحت الحمراء الغير المرئي لإضاءة قرنية العين، مما يسمح بتحديد الأنماط المميزة لقرنية العين والتي لا يمكن تحسسها بالعين المجردة، إلا من خلال استخدام كاميرا مخصصة لهذا الغرض، بهدف التقاط موضع بؤبؤ العين والقرنية، على اعتبار أن كل عين لها مميزات فريدة تميزها عن العيون الأخرى، ليتم لاحقاً تحويلها إلى قالب رقمي (Iris Recognition Technology, s.d.)

كما تتميز تقنية التعرف على قزحية العين بالدقة والكفاءة العالية مقارنة بالطرق الأخرى، هذه التقنية هي الخيار الافضل والأكثر دقة وأماناً، بفضل قدرتها على التحليل والمقارنة، حيث يتم تحليل أنماط قزحية العين الفريدة للحصول على دقة استثنائية، مما يجعلها أحد أهم القياسات الحيوية المناسبة للتطبيقات التي تحتاج إلى أعلى درجات الأمان والتحقق من الهوية (Iris Recognition Technology, s.d.)

ج. البصمة الأصابع (Finger print) :

بدأ استخدام التعرف على بصمات الأصابع كوسيلة لتحديد الهوية في عام 1823 (Eludire & EO, 2018, p. 2) ليقوم Sir Francis Galton بتقديم دراسة معمقة لبصمات الأصابع العشر التي طرحها من خلال بحثه المنشور عام 1892 مستنداً إلى التفاصيل الدقيقة للبصمة (احمد، 2010، صفحة 5)

وتعتبر إيفان جليستا بوركيني Evangelista Burkinى من جمهورية التشيك أول من تعرف على هذه التقنية، ومع بداية سبعينيات القرن العشرين تم تطوير قارئ إلكتروني لبصمات الأصابع، مما أدى إلى تطوير تقنيات متقدمة مثل قارئ هندسة اليد التي تم تطويرها في عام 1985 (Eludire & EO, 2018, p. 2)

كما تعد تقنية التعرف على بصمات الأصابع الطريقة الأكثر شيوعاً واستخداماً في النظام البيومتري، حيث تعمل على تسجيل وتصنيف الأنماط الفريدة لبصمات الأصابع الفرد، والتي يمكن استخدامها لأغراض تحديد الهوية من خلال استخدام هذه التقنية في نظام المطابقة الإلكترونية، نتيجة تواجد 120 نقطة لتمييز بصمات الأصابع والتي يمكن برمجتها داخل الحاسب الآلي من خلال برنامج قارئ بصمات الأصابع (احمد، 2010، الصفحات 8-9) والذي سوف يستخدم لاحقاً في مقارنة البصمة ومطابقتها مع البصمات المخزنة في قاعدة البيانات، من خلال استخدام خوارزميات التعرف على الأنماط والخصائص الفريدة (التلال والوديان والمسامات والانحناءات) الموجودة في البصمة، وهو ما يشار إليها باسم «نقوش البصمة» التي تنتج عن الواجهة الأساسية بين حليقات الجلد (Eludire & EO, 2018, p. 2).

وتتكون خوارزمية التعرف على بصمات الأصابع من خاسيتين آسا سيتين هما: (Iris Recognition Technology, s.d.)

✓ مستخرج الميزات (Feature Extractor): تم تصميم مستخرج الميزات خصيصاً لمعالجة صور بصمات الأصابع ضعيفة الجودة وغير المكتملة، الناتجة عن ظروف معينة أو أثناء التقاطها، من خلال استخدام تقنيات تحسين الصورة المتقدمة، حيث تعمل هاته الخوارزمية على تحسين جودة الصورة بشكل كبير وتصحيح أي عيوب محتملة دون التأثير على عملية التعرف.

✓ المطابقة الخوارزمية للبصمة (Algorithmic Matching): تعمل هاته الخاصية من الخوارزمية على مطابقة بصمات الأصابع، بهدف مقارنة نموذجين لبصمات الأصابع باستخدام قوالب بيومترية بدلاً من الصور الأصلية، من خلال إجراء بحث تعريفي عالي السرعة، مما يؤدي إلى الحصول على درجة تشابه معينة تحدد ما إذا كان القالب الرقمي ينتمي إلى نفس الإصبع أم لا.

وقد حدد جورمان Gorman بدقة ثلاثة مجالات رئيسية تستخدم فيها القياسات الحيوية لبصمات الأصابع وهي: (Eludire & EO, 2018, p. 2)

أ- مجال للتنفيذ القانون: حيث يهدف استخدام القياسات الحيوية إلى ضمان السلامة والحفاظ على الأمن العام، من خلال الاستخدام الأمثل لهذه التكنولوجيا بهدف تحديد المجرمين الحقيقيين والقبض عليهم.

• المجال لمنع الاحتيال: تعمل القياسات الحيوية لبصمات الأصابع التعرف على هويات الأفراد الذين يصلون إليها والتحقق من صحتها وبالتالي الحد بشكل فعال وأمن من الطرق الاحتيالية التي تعاني منها هذه الأنظمة.

• المجال متعدد الأوجه للوصول المادي: ويشمل التطبيقات واسعة النطاق لأنظمة التصوير الآلي لبصمات الأصابع (AFIS)، مما يمنع أي ولوج غير مسموح للوصول إلى المناطق المحظورة أو أنظمة الكمبيوتر، وبالتالي زيادة فعالية التدابير الأمنية.

2.3 القياسات الحيوية الديناميكية (المواصفات السلوكية):

تعتمد هاته القياسات على استخلاص البيانات من أفعال الشخص وتشمل:

أ- **التوقيع (Signature):** تستخدم أنظمة التعرف على التوقيع المكتوب بخط اليد لتحديد الهوية من خلال تحليل النموذج والميزات المميزة لعملية التوقيع، عن طريق استخدام أدوات رقمية متطورة مثل: الأجهزة اللوحية الرقمية والما سحات الضوئية، لالتقاط التوقيع وترميزه، مما يسمح لهاته الأنظمة بتتبع التغييرات التي تحدث في التوقيع مع مرور الوقت (احمد، 2010، صفحة 5).

وتشمل بصمة التوقيع عدة عيوب تتمثل أساسا في:

✓ سهولة تقليد التوقيع من طرف اشخاص اخرين.

✓ عدم الاحتفاظ به بسبب المرض (الزهايمر) وذسيانه بمرور الوقت (احمد،

2010، صفحة 5)

ويمكننا تقسيم التوقيع باختلاف انواعه إلى عدة أنواع أهمها:

1. **التوقيع الرقمي:** يتم استخدام التوقيع الرقمي لإنهاء المعاملات القانونية التي تتم من خلال الوسائل الإلكترونية، خاصة تلك التي تحدث عبر الإنترنت، هذا النوع من التوقيع موجود في نظام التشفير المعروف باسم Cryptographie، يشير إليه على أنه توقيع رقمي يعتمد على تقنية التشفير، باستخدام الخوارزميات لتحويل التوقيع من شكله الأصلي إلى شاكلة رقمية، مما يجعل من المستحيل العودة إلى تنسيقه المرئي بدون المفتاح المشفر.

كما يقوم التشفير على توفر عنصرين أساسيين يتمثلان في (رفعت، التوقيع الإلكتروني وحجيته في الاثبات المدني، 2019، صفحة 199):

✓ توفر البيانات المشفرة التي تختلف في شكلها سواء كانت ملفات كمبيوتر، إشارات، حروف أو أرقام.

✓ توفر برنامج التشفير الذي يعتمد على آلية تشفير، تعمل على تحويل البيانات من شاكلتها الأصلية المقروءة إلى شاكلة رموز أو إشارات.

2. **توقيع بالقلم الإلكتروني:** وهو التوقيع الشائع في النظام البيوميترية، حيث يتضمن التوقيع استخدام قلم إلكتروني مخصص لتوقيع المستندات إلكترونياً

باستعمال برنامج معين، من خلال اتباع خطوتين أساسيتين هما (رفعت، التوقيع الإلكتروني وحجته في الاثبات المدني، 2019، صفحة 200):

✓ التقاط التوقيع: في هاته المرحلة يقوم الفرد بإدخال بياناته عبر خانة معروضة على الشاشة، من خلال إتباع التعليمات اللازمة، فيقوم بالتوقيع باستخدام القلم الإلكتروني داخل منطقة المخصصة لذلك، فيقوم البرنامج بعد ذلك بعملية تحليل مختلف الجوانب المرتبطة بالتوقيع، مثل الحجم والشكل والشغل وغير ذلك، ليقوم الموقع بعد ذلك بتأكيد التوقيع أو رفضه، وعند الموافقة يقوم البرنامج بتشفير بيانات التوقيع وتخزينها لاستخدامها مستقبلاً.

✓ التحقق من صحة التوقيع: تتم عملية التحقق من خلال مقارنة التوقيع المخزن مع التوقيع المعروض على الشاشة للتأكد من صحته، ومع ذلك تتطلب هذه الطريقة معدات متخصصة وعمليات مصادقة معقدة، مما يجعلها مكلفة وتعتمد على عينات من الكتابة اليدوية للموقع التي قد تتعرض للنسيان.

3. التوقيع بواسطة البطاقة الممغنطة الرقم السري: يعد استخدام البطاقة الممغنطة للتوقيعات الإلكترونية ممارسة شائعة في البنوك، مما يتيح للعملاء إجراء المعاملات بشكل مستقل عن الكمبيوتر أو الشبكة، حيث تتيح البطاقة التي تقدمها مؤسسة مالية ما هو صول إلى السيولة المالية من خلال أجهزة الصراف الآلي باتباع إجراءات معينة، مثل إدخال البطاقة وإدخال الرقم السري وتحديد المبلغ واستلامه (رفعت، التوقيع الإلكتروني وحجته في الاثبات المدني، 2019، صفحة 201)

ب. **البصمة الصوتية (Voice print):** تم تبني هذه الطريقة البيومترية التي تستخدم الصوت كصفة بشرية مميزة على نطاق واسع في المجتمع الحديث، بسبب سهولة استخدامها للوصول إلى التقنيات التكنولوجية لا سيما أن معظم أجهزة الكمبيوتر الحديثة تحتوي على ميزات التسجيل والتشغيل الصوتي، حيث يتم تحديد ومعرفة المتحدث بناءً على صوته الفريد الذي يميزه عن الآخرين، إلا أن ما يعيب هاته التقنية هو إمكانية تأثرها بعوامل مختلفة مثل تعرض الاحبال الصوتية للتلوث بسبب التقدم في العمر، (سعيدة،

2021/2020، صفحة 206).بالإضافة الى عدم إمكانية اخذ هاته البصمة من الافراد الذين يجدون صعوبة في النطق او الذين يولدون بكماء.

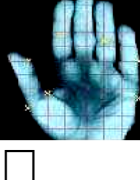
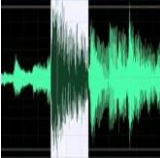
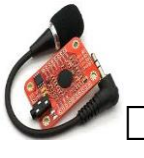
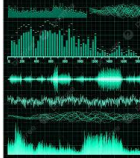
وفي عام 1960 قام البروفير سور ال سويدي Gunnar Fant بنشر أول نموذج يصف من خلاله العناصر الفسيولوجية المشاركة في تحديد الصوت، من خلال العمل على تحليل الأشعة السينية للأفراد الذين ينتجون أصواتاً معينة، وهو ما أدى إلى تطور كبير في فهم مكونات الصوت وتطوير تقنية التعرف على الصوت (احمد، 2010).

ليتم بعدها استخدام البصمة الصوتية فيما بعد بطريقتين شائعتين:

- الطريقة الأولى: وهي الطريقة التي يعتمد عليها خبراء الصوت عند محاولتهم التعرف على المتحدث في التحقيقات الجنائية، فبعد الحصول على التسجيل الصوتي الأولي ومقارنته بالتسجيلات الصوتية للمتحدث، يتم إذشاء تقرير عن التشابه بين الصوتين وتحديد ما إذا كان هناك تطابق أم لا.
- الطريقة الثانية: أدت التطورات التكنولوجية الحديثة إلى تطوير تقنية التحقق التلقائي من هوية الشخص من خلال تميز صوته عن الأصوات الأخرى، بهدف تعزيز الإجراءات الأمنية بشكل كبير، حيث أثبتت هذه الطريقة المبتكرة فعالية كبيرة في تأدية العديد من المهام، مثل الوصول إلى الحسابات المصرفية، وفتح الأبواب وتسجيل الدخول إلى المنصات عبر الإنترنت (الغامدي، 2005، صفحة 17).

كما تستخدم حالياً بعض الشركات الكورية هاته التقنية لغرض التعرف على المتحدثين باللغة الكورية، وتقديم أنظمة لا تستخدم بصمة الصوت ومن الأمثلة ذلك نظام Open sesame Web، الذي يسمح بالوصول الصوتي إلى مواقع الويب من خلال شبكة الويب (الغامدي، 2005، صفحة 15).

الجدول رقم 1: يوضح الية عمل تقنية التعرف البيومترية لبناء الهوية الرقمية
استنادا الى القياسات الحيوية

القياسات الحوية ☐	نموذج البيومترية القياسات الحيوية ☐	المستشعرات البيومترية ☐	طريقة الاستعمال	القلب البيومترية
الإصبع				
الوجه				
قزحية العين ☐				
هندسة اليد ☐				
التوقيع				
الصوت ☐				

من اعداد الباحثين

ثانياً: النظام البيومترية كتقنية رقمية لبناء هوية رقمية.

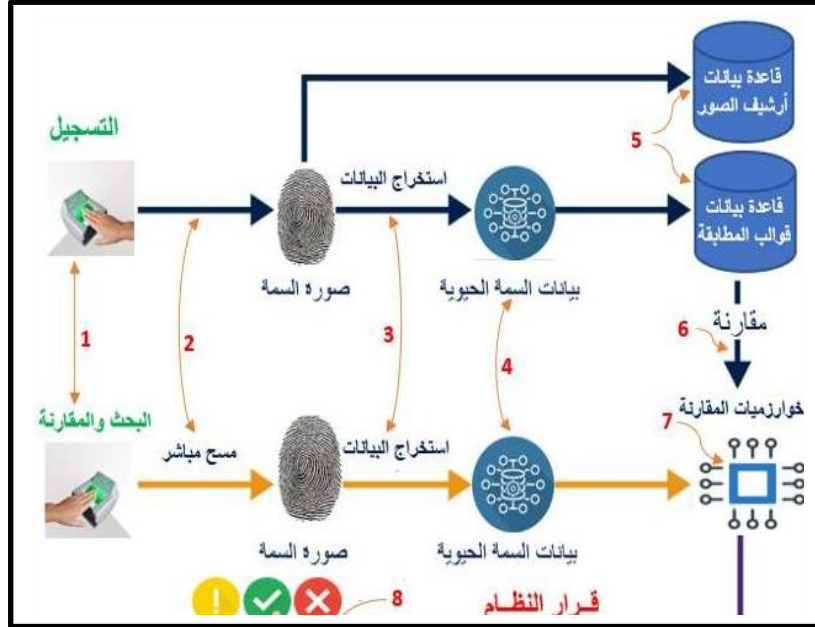
1. آلية عمل النظام البيومترية:

من خلال تتبعنا لآلية عمل النظام البيومترية، يمكننا تصنيف الإجراءات التشغيلية لتقنيات البيومترية داخل هذا النظام لتتضمن هوية بيومترية إلى عمليتين أساسيتين والتي سيتم التطرق إليهم بالتفصيل في المحور التالي وهي باختصار:

أ- **عملية التسجيل:** تعمل هاته العملية على تحديد والتعريف بهوية الشخص بناءً على الخصائص الجسدية أو الفسيولوجية أو السلوكية الفريدة للفرد والتي يتم ادراجها في النظام من خلال الإجابة على السؤال "من هذا الشخص؟" A (PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 2)

ب- **عملية المصادقة الرقمية أو التحقق:** تعمل هذه العملية على تأكيد الهوية الفرد يدعي أن لديه هوية معينة ويود الولوج إلى النظام، فيتم مقارنة بياناته البيومترية للتأكد من مدى تطابق قالبه البيومترية مع القالب المخزن في قاعدة بيانات المرتبطة بتلك الهوية، بهدف التحقق مما إذا كانت المطابقة سليمة أم لا من خلال الإجابة على السؤال "هل هذا هو الشخص نفسه الموجود في النظام" (Duller & Wendehorst, 2021, p. 20.)

الشكل رقم 1: طريقة عمل النظام البيوميترى لبناء هوية بيو مترية



المصدر: (عمر بن عبد العزيز اللعبون، <https://bit.ly/4eGnUdE>)

2. بناء الهوية الرقمية من خلال النظام البيوميترى:

تمر عملية بناء هوية رقمية لأي فرد داخل النظام البيوميترى بعدة مراحل أساسية وتتمثل هاته المراحل فيما يلي:

أ. **التسجيل البيوميترى لبناء الهوية الرقمية وتحديد هاته المرحلة:** يتم القيام بتسجيل الهوية الرقمية للفرد تشمل جميع معلوماته الشخصية بناء على الوثائق ثبوتية المقدمة من طرفه وكذا قيا ساته الحيوية، ليتم توثيقها داخل نظام البيوميترى، وتحويل هاته البيانات لقالب بيو مترى بغرض الرجوع اليه اثناء التحقق وتأكيد الهوية الفرد بدقة (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 2) حيث لا يتم الو وصول إلى هاته المرحلة إلا بعد تتبع الخطوات الاساسية التالية:

1. مرحلة التقاط العينة بيو مترية: كمرحلة أولية وأثناء عملية تحديد الهوية البيوميترية، يتم التقاط نموذج للعينة البيوميترية ذات جودة عالية باستخدام جهاز

مخصص لهذا الغرض، حيث تتم العملية إما تلقائياً أو بمساعدة بشرية لضمان
الدقة والموثوقية (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 2)

حيث يتم الحصول على العينة البيومترية من خلال طريقتين أساسيتين وهما:

- التقاط العينة عن طريق اللمس المباشر: يتم أخذ العينة البيومترية عن طريق اللمس المباشر للعينات الحيوية المراد أخذها للجهاز المخصص لهذا الغرض والذي يكون ثابت أو محمول على سبيل المثال بصمات الأصابع.
- التقاط العينة عن بُعد: وهي الطريقة التي يتم من خلالها أخذ العينة البيومترية دون الحاجة إلى لمس الجهاز على سبيل بصمة الوجه أو بصمة قزحية العين.

ويرتبط نجاح عملية التقاط العينة البيومترية على مدى جودة العينة الملتقطة، فالعينات المأخوذة ذات جودة رديئة التي يتم التقاطها، ستؤدي حتماً إلى تخفيض من فعالية أداء النظام، لذلك من المهم الحصول على بيانات بيومترية ذات جودة عالية من أجل الحصول على مطابقة جيدة أثناء عملية التحقق في المستقبل (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، ومعهد القياسات الحيوية، 2018، صفحة 14)

2. مرحلة تحويل العينة البيومترية إلى نموذج رقمي: بعد الانتهاء بنجاح من المرحلة الأولى، يتم الانتقال مباشرة إلى المرحلة التالية التي تعتبر خطوة حاسمة في هذه العملية، حيث يتم التركيز على كيفية نقل العينة البيومترية الملتقطة إلى نظام الآلي (ABIS) لتحديد الهوية البيومترية (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 2) مع تفادي الوقوع في الأخطاء التي يمكن أن تؤثر على عملية المطابقة في المستقبل على سبيل المثال تحويل عينة بيومترية مأخوذة ذات جودة رديئة إلى قالب بيوميترية يتم تخزينه بهدف الرجوع إليه أثناء المطابقة، ليقوم بعده النظام الآلي المخصص لهذا الغرض بمعالجة البيانات الأولية لتحديد الميزات الفريدة للعين، فيعمل على تحويل النمط المبسط للصورة الأصلية برمز رقمي وتحويلها إلى قالب بيوميترية يتم الاحتفاظ به داخل النظام البيوميترية، (Fund UNICEF, 2019, p. 8)،

بهدف الاستعانة بها لاحقاً عند التحقق ومقارنتها بالقوالب المرجعية المخزنة في قاعدة البيانات، وهو ما يساهم بشكل كبير في الرفع من أداء عملية التحقق من الهوية ويقلل بشكل كبير من مساحة التخزين المطلوبة داخل النظام، وبالتالي تحسن أمن وفعالية عملية التحقق من الهوية بأكملها وبالتالي تعزيز مستوى الأمان للهوية الرقمية (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، ومعهد القياسات الحيوية، 2018، صفحة 14)

3. مرحلة مقارنة العينة البيومترية: خلال هاته المرحلة يتم اخضاع النموذج لمقارنة شاملة مع جميع القوالب البيومترية المخزنة والمرتبطة بجميع الأفراد الموجودين داخل النظام، بغرض التحقق عند تسجيل البيانات البيومترية داخل النظام، وبالتالي ضمان عدم إجراء إدخال مكررة ينتج عنها الولوج عن طريق الخطأ لبيانات الأفراد المسجلين، وهو ما يشار إليها عادة باسم إزالة الازدواجية (Fund UNICEF, 2019, p. 9) مما يساهم في تسهيل عملية التحليل الشامل والدقيق لبيانات العينة البيومترية مع العينات الأخرى المخزنة وبالتالي تساعد هذه العملية في التحقق الدقيق والفعال للهوية، مع تقليل من احتمالية الوقوع في الأخطاء أو التلاعب بالبيانات (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، ومعهد القياسات الحيوية، 2018، صفحة 14).

لذا فإن الأنظمة البيومترية التي تمتاز بمستوى عالٍ من الأمان والدقة أثناء عملية التسجيل وتحديد الهوية، تكون فيها نسبة معدلات التحديد على النحو الآتي:

معدل القبول الصحيح TAR: يحدث معدل القبول الصحيح عندما يقوم النظام بالقبول بدقة عالية سمات البيومترية المسجلة للفرد مع قالبه البيوميتر المخزن في النظام (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، ومعهد القياسات الحيوية، 2018، صفحة 17)

معدل الرفض الصحيح TRR: يحدث معدل الرفض الحقيقي الحالات التي لا تتوافق فيها البيانات البيومترية للفرد بشكل صحيح أثناء التسجيل مع البيانات

الخاصة بالآخرين والمخزنة في قاعدة البيانات، (Fund UNICEF, 2019, p. 9)

ب. **مرحلة المطابقة البيومترية:** تمثل مرحلة المصادقة البيومترية مرحلة محورية وحاسمة، حيث تتم مطابقة البيانات البيومترية الملتقطة مع البيانات البيومترية المخزنة للفرد، من خلال مقارنة البيانات البيومترية المدرجة من طرف الفرد بهدف السماح له بالولوج الى قاعدة المعطيات، مع القالب البيومترية الذي تم انشاءه سابقا لغرض المصادقة والتأكد من أن الفرد الذي يود الوصول إلى النظام هو بالفعل نفس الشخص الذي تم تخزين بياناته سابقا، (Fund UNICEF, 2019, p. 9) وقد يحدث في بعض الأحيان فشل النظام في إجراء عملية المطابقة بسبب اعطاب تقنية تصيبه، لذا يصح من الضروري القيام بإجراء فحص التحقق اليدوي أو البشري لعملية المطابقة، لضمان أقصى مستوى من الدقة والأمان، الأمر الذي يستدعي وجود آليات مصادقة بديلة للتعامل مع أي أخطاء تقنية قد تطرأ على النظام أثناء عملية المطابقة وهذا أمر بالغ الأهمية بشكل خاص في الحالات التي يتم فيها استخدام المطابقة البيومترية (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, متري، 2022, p. 3) حيث يتم الوصول الى هاته المرحلة بعد المرور بالمراحل الثلاث التالية:

1. **التحقق البيومترية:** هو عملية مقارنة القياسات الحيوية التي تم جمعها مع البيانات البيومترية الحالية للفرد المراد ادخالها الى قاعدة البيانات، فيتم مقارنة القياسات المسجلة والنماذج المخزنة مسبقاً للتأكد من مطابقتها (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 3)، حيث يتم اللجوء الى هاته المرحلة، بهدف منع أشخاص من استخدام هوية الآخرين (Eludire & EO, 2018, p. 3) من خلال وضع العينة جنباً إلى جنب مع العينة المرجعية للفرد، التي تظل مخزنة دائماً داخل الجهاز (Vallance, 2018, p. 4). في حالة إذا تم تأكيد المطابقة، فإن هذا يشير إلى احتمالية أن الشخص هو نفسه المسجل على مستوى النظام، على سبيل المثال استخدام بصمة الإصبع كقياسات حيوية بيومترية، يتم قياس بصمة الإصبع الحالية

ومقارنتها مع البيانات الم سجله والمخزنه سابقا في النظام، فإذا تمت عملية المطابقة فإن النظام يقر بأن الشخص هو نفسه الذي تم تسجيله وفي حالة عدم المطابقة، يمكن اللجوء الى إجراء التحقق اليدوي من قبل موظف للتأكد من الهوية، (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 3)

هذه التقنية يتم العمل بها على مستوى جميع مطارات العالم، من خلال عملية التحقق من صورة الم سافر القادم مع الت صوير الرقمي المخزن في رقاقة جواز السفر الإلكتروني مما يؤدي إلى أتمتة وتسريع عملية نقل للركاب (Vallance, 2018, p. 4)

2. إلغاء الازدواجية البيومترية: يتضمن تسجيل الدخول إلى نظام الهوية الأساسي استخدام تقنية التكرار الديناميكي، حيث يُطلب من المستخدمين تقديم بياناتهم الأولية بهدف السماح لهم بالولوج إلى النظام، لتتم بعدها مقارنة البيانات الحيوية التي تم الحصول عليها مع قاعدة بيانات التسجيل للتحقق من عدم وجود أي تسجيل مكرر، اذ يعمل إجراء إلغاء البيانات المكررة على تخفيف مخاطر الاحتيال في الهوية من خلال منع الأفراد الذين يحاولون امتلاك هويات متعددة داخل نظام، حيث يتم استخدام هذه التقنية على نطاق واسع في مختلف الدول المتقدمة كجزء لا يتجزأ من عملية إصدار جوازات السفر، وبطاقات التعريف ورخص السياقة (A PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 57)

لذا فان الأنظمة البيومترية التي تمتاز بمستوى عال من الأمان والدقة في عملية مطابقة الهوية، تكون فيها نسبة معدلات التعريف مرتفعة على النحو الآتي: (Fund UNICEF, 2019, p. 9)

- ✓ معدل التعريف الإيجابي الحقيقي TPIR: نسبة المستخدمين المسجلين الذين تمت مطابقتهم بشكل صحيح مع قوالبهم البيومترية.
- ✓ معدل التعريف السلبي الحقيقي TNIR: نسبة المستخدمين الجدد الذين لم يتم مطابقتهم بشكل صحيح مع أي قوالب بيومترية في النظام.

3. التحديات النظام البيومتري:

يمكن التمييز بين نوعين من التحديات التي يمكن ان يواجهها النظام البيومتري اثناء القيام انشاء هوية او التأكد من الهوية وهما :

1.3 **تحديات على مستوى النظام نفسه**: تعتمد فعالية أي نظام بيومتري على مدى دقته في تحديد الهوية وانخفاض مستوى معدلات الخطأ، وكذا سرعته في معالجة الاستثناءات، الا ان أداء معظم الأنظمة البيومترية الحالية يتأثر بالعديد من الاعطاب التقنية التي قد تحدث اثناء المعالجة مما قد يؤثر ذلك على فعاليته في تحديد الهوية بدقة، وتتمثل هاته التحديات فيما يلي:

- معدلات خطأ تحديد الهوية البيومترية : أثناء تحديد الهوية البيومترية، تتم عملية مقارنة القالب البيومتري المسجل مع جميع قوالب البيومترية المخزنة في قاعدة البيانات؛ وخلال هاته العملية من المحتمل أن تحدث أخطاء محتملة في المطابقة، مما يؤدي إلى فشل النظام في تحديد الهوية او مطابقتها بدقة الامر الذي يسمح بالولوج الغير مسموح الى بيانات المستخدمين ويمكننا حصر معدلات الخطأ التقنية الشائعة اثناء التسجيل والمطابقة فيما يلي : (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، ومعهد القياسات الحيوية، 2018، صفحة 17)

✓ **معدل القبول الخاطئ FAR**: يحدث معدل القبول الخاطئ عندما يقوم النظام عن طريق الخطأ بتسجيل وانشاء قالب بيومتري لشخص ما مع قالب بيومتري لشخص آخر مخزن في قاعدة البيانات بسبب خطأ في النظام.

✓ **معدل الرفض الخاطئ FRR**: يشير معدل الرفض الخاطئ إلى الحالة التي يفشل النظام في عملية التحقق من قالب البيومتري لشخص ما مع القالب المخزن في قاعدة البيانات على الرغم من انها تعود لنفس الشخص .

✓ **معدل فشل الحيازة FTA**: يشير معدل فشل الحيازة الى الحالة التي يفشل فيها النظام في انشاء او الوصول الى قالب بيومتري لهوية شخص ما بسبب الاعطاب او الحوادث الناتجة عن عطل في النظام والتي حدثت أثناء عملية التسجيل على سبيل المثال: عدم التقاط صورة واضحة او وجود تشوه مؤقت في العينة البيومترية الملتقطة الخ بالإضافة الى عدم تخزين القالب البيومتري

نتيجة خلل تقني، لذا فإن معدل فشل الاستحواذ المرتفع يتطلب استراتيجية بديلة لتسجيل الأفراد ذوي القياسات الحيوية البيومترية التي يتعذر تسجيلها، وهو ما يستلزم إيجاد طرق بديلة لتخطي هاته الأخطاء، مثل استخدام الإبهام الأيسر بدلاً من الإبهام الأيمن، أو إخضاع الأفراد غير القادرين على التسجيل البيوميترى للتدقيق اليدوي من قبل الموظفين وهو ما يعرف باسم معالجة الاستثناءات (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، معهد القياسات الحيوية، 2018، صفحة 18).

✓ معدل التعريف السلبي الكاذب (FNIR) نسبة المستخدمين المسجلين الذين يتم رفضهم بشكل غير صحيح، بالرغم من وجود قالبهم البيوميترى في النظام.

✓ معدل التعريف الإيجابي الكاذب (FPIR) نسبة المستخدمين الغير مسجلين، الذين تمت مطابقتهم بشكل غير صحيح مع قالب بيوميترى مخزن خاص بمستخدم آخر.

✓ معدل الخطأ المتساوي EER: يشير إلى تساوي قيم كل من معدل الرفض الخاطئ ومعدل القبول الخاطئ، أي أن نسبة حالات القبول الخاطئة تساوي نسبة حالات الرفض الخاطئة (الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، معهد القياسات الحيوية، 2018، صفحة 35).

وعلى هذا الأساس ومن خلال معدل الخطأ المتساوي يمكننا قياس الأداء العام للنظام من حيث مدى الدقة والأمان:

- النظام البيوميترى الذي تكون فيه نسبة معدل القبول الخاطئ أكبر من نسبة معدل الرفض الخاطئ، يتميز بكونه أقل أماناً وعرضة للاحتيال على اعتبار أنه يسمح لفئة كبيرة من المستخدمين الغير مسجلين في قاعدة البيانات بالولوج إلى الأماكن المحظورة.

- النظام البيوميترى الذي تكون فيه نسبة معدل الرفض الخاطئ أكبر من نسبة معدل القبول الخاطئ، يتميز بكونه أكثر أماناً وصرامة على اعتبار أنه

يُسمح لفئة قليلة من المستخدمين الغير مسجلين في قاعدة البيانات بتخطي النظام.

الجدول رقم 2: قياس اداء الأنظمة البيومترية أثناء عملية التحقق والمصادقة

التسجيل والتحقق			
مستخدم صحيح	مستخدم غير صحيح	مستخدم صحيح	مستخدم غير صحيح
معدل القبول الصحيح	معدل القبول الخاطئ	معدل الرفض الكاذب	معدل الرفض الحقيقي
قبول النظام		رفض النظام	
نظام مؤمن	نظام غير مؤمن	نظام مؤمن	نظام غير مؤمن
المصادقة والمقارنة			
مستخدم غير مسجل	مستخدم مسجل	مستخدم غير مسجل	مستخدم مسجل
معدل التعريف الإيجابي الكاذب	معدل التعريف الإيجابي الحقيقي	معدل التعريف السلبي الكاذب	معدل التعريف السلبي الحقيقي
هوية مطابقة		هوية غير مطابقة	
نظام غير مؤمن	نظام مؤمن	نظام غير مؤمن	نظام مؤمن

من اعداد الباحثين بالاعتماد على المصدر: Fund UNICEF, 2019, p. 9

3. 2. تحديات خارج النظام البيوميترية:

هناك مجموعة من التحديات التي يمكن أن تؤثر على أداء النظام، خاصة أثناء القيام بعملية التسجيل أو التحقق، حيث يمكن تشمل العوامل التي يمكن أن تؤثر على أداء النظام ما يلي: (Fund UNICEF, 2019, p. 9)

✓ جودة المستشعر (مثل الكاميرا أو قارئ بصمات الأصابع): وتتمثل في مدى المستشعر على التقاط بيانات دقيقة وواضحة، التي على أساسها يتم تسجيل الفرد مما يؤثر ذلك على عملية التحقق أو المطابقة في المستقبل.

✓ تفاعل المستخدم مع المستشعر: والتي تظهر من خلال مدى قوة ضغط المستخدم على المستشعر لأخذ بصمته البيومترية، الأمر الذي ينتج عنه أخذ عينة بيومترية ضعيفة أو ناقصة، مما يصعب من إجراء عملية المطابقة التأكد منها في المستقبل.

✓ جودة الصورة الملتقطة أثناء التسجيل: تشير إلى مدى وضوح وتفاصيل الصورة التي تم التقاطها أثناء تسجيل بيانات المستخدم في نظام البيوميترية، حيث أن الصورة المشوهة أو غير الواضحة، تؤدي دائماً إلى حدوث مشاكل في التحقق لاحقاً، حيث يصعب على النظام إجراء عملية المطابقة بدقة.

✓ التغييرات في الخصائص البيومترية للفرد: والتي تحدث بسبب العمل اليدوي أو الحوادث أو الشيخوخة، مما لا يسمح للفرد بالولوج إلى النظام بالرغم من وجود العينة البيومترية الخاصة به مخزنة في قاعدة البيانات. (A. PRIMER ON BIOMETRICS FOR ID SYSTEMS, 2022, p. 34)

ويرى ما لتوني أن نقاط ضعف أداء النظام البيوميترية تكون نتيجة الاستخدام الغير قانوني للبيانات البيومترية من خلال: (Adler, 2008, p. 382)

✓ التحايل: هو عبارة عن المحاولات الغير قانونية لاختراق وتجاوز النظام، التي يقوم بها المستخدم الغير مسجل بتقديم بيانات مزورة، للوصول إلى قاعدة البيانات البيومترية، وعادة ما يتم اللجوء إلى استخدام هذه الطريقة على الأجهزة التي تحتوي على ثغرات على مستوى أنظمتها.

✓ الاستحواذ السري: ويقصد به استخدام البيانات البيومترية من طرف مستخدم غير مسجل والتي يتم الحصول عليها من المستخدمين المسجلين بهدف

الوصول إلى النظام، عن طريق خداع المستخدم على سبيل المثال الحصول على تسجيل صوتي لكلمات المرور الصوتية أو رفع بصمات الأصابع واستخدامهما في الولوج إلى النظام.

✓ التواطؤ والإكراه: هما ثغرات في النظام البيومتري يكون سببهما المستخدم الشرعي، ففي ثغرة التواطؤ يقوم المستخدم الشرعي بتسريب بياناته البيومترية (ربما مقابل مبلغ مالي) لمستخدم آخر حتى يتسنى له الولوج إلى النظام، في حين أن ثغرة الإكراه يقوم المستخدم الشرعي بتسريب بياناته البيومترية قسرياً لمستخدم آخر (من خلال التهديد الجسدي أو الابتزاز).

✓ رفض الخدمة (DOS): هو نوع من الهجمات الإلكترونية الهدف منها منع المستخدمين الشرعيين من الوصول إلى خدمة النظام، من خلال إرسال عدد كبير جداً من الطلبات إلى النظام في وقت قصير جداً، مما يؤدي إلى حدوث بطء شديد في الأداء أو توقف النظام عن العمل.

✓ إنكار الاستخدام: هو الحالة التي ينكر فيها المهاجم الوصول إلى النظام، قد ينكر المستخدم الشرعي أفعاله من خلال الادعاء بأن بياناته البيومترية قد سرقت منه سواء عن طريق الاستحواذ القسري أو التحايل أو أن المستخدم الآخر غير شرعي كان قادراً على تنفيذ الإجراءات الولوج بسبب القبول الخاطئ البيومتري.

خاتمة:

وفي الختام يُعد التعرف البيومتري من أحدث تقنيات التكنولوجيا التي تُساهم في بناء الهوية الرقمية الحديثة، من خلال قدرته على التحقق من الأفراد بدقة عالية باستخدام خصائصهم البيولوجية الفريدة، لذا فإن عملية وبناء هوية رقمية للأفراد تحمل مواصفات عالية من الأمان والخصوصية، يعد تحدي كبير يواجه العديد من الدول لا سيما تلك التي لا تمتلك تقنيات رقمية تتماشى والتطور المتسارع للتكنولوجيا الرقمية أو تفتقر إلى البنية التكنولوجية المتقدمة سواء على مستوى التطبيقات والأنظمة الرقمية أو على مستوى أفرادها الذين يتمتعون بمهارات رقمية دون المستوى الذي يمكنهم من إجراء معاملاتهم الرقمية دون أية مخاوف، الأمر الذي ساهم إلى حد كبير في انتشار ظاهرة الاحتيال في الهوية، والاستيلاء الغير المشروع على المعلومات الشخصية

واستغلالها في أغراض إجرامية، من هذا المنظور فإن استخدام التقنيات الرقمية لأنظمة بيومترية ذات مستوى أمني عال لأغراض تسجيل الهوية أو التحقق منها أصبح حتمية للتخفيف بشكل كبير من حدوث الاحتيال وتعزيز الأمان وتسهيل المعاملات الرقمية.

وعلى ضوء هاته الدراسة تم استخلاص النتائج والتوصيات التالية:

✓ ضرورة التوجه الى التقنيات الرقمية الحديثة والعمل على تطويرها، لتحسين أداء النظام البيومتري بما يسمح من الحد من الأخطاء التي تحدث على مستوى النظام البيومتري اثناء عملية التعرف البيومتري (التسجيل، المطابقة) خاصة الحالات التالية:

1- ارتفاع معدل القبول الخاطئ اثناء عملية التسجيل او التعريف عند الافراد التوائم خاصة عند وجود أحد التوائم مسجل سابقا في النظام البيومتري، مما سيؤدي الى ارتفاع معدل التحديد الإيجابي الكاذب (FPIR) للفرد التوائم اثناء المطابقة بشكل غير صحيح للقالب البيومتري، باعتبار ان التوائم يحملون تقريبا نفس ملامح الوجه.

2- تدهور القياسات الحيوية كبصمة الإصبع أو قرنية العين... الخ بسبب التقدم في العمر أو التعرض للحوادث، الامر الذي يستدعي تبني استراتيجيات تقنيات متعددة الوسائط التي تسمح بدمج بين أكثر من نوع من القياسات البيومترية كدمج التعرف على بصمة الإصبع مع تقنيات أخرى مثل التعرف على الوجه أو قرنية العين أو الصوت لتعزيز دقة النظام وتجاوز أي تغييرات طفيفة في الخصائص البيومترية للفرد.

✓ تعزيز الوعي الرقمي للمستخدمين وتطوير مهاراتهم الرقمية، قصد اكتشاف الرسائل الاحتيالية الإلكترونية، التعرف على التهديدات الإلكترونية مثل التصيد الإلكتروني (Phishing)، التي تستهدف سرقة بياناتهم البيومترية، لتفادي سرقة أو تقليد بياناتهم الرقمية، مما يستدعي تعزيز استخدام ما يعرف بالصادقة الثنائية كإضافة كلمة مرور أو شفيرة القياسات الحيوية، بهدف توفير مستوى ثاني من الأمان.

قائمة المراجع:

- A PRIMER ON BIOMETRICS FOR ID SYSTEMS. (2022). Washington: International Bank for Reconstitution and Development.
- Adler, A. (2008). Biometric System Security. Dans P. F. Anil K. Jain, Handbook of Biometrics. US: Springer.
- ASHOK, J., VAKA, S., & P.V.G.S, M. (2010). AN OVERVIEW OF BIOMETRICS. International Journal on Computer Science and Engineering, 02(07), pp. 2402-2408.
- BELHADJ, F. (2017). Biometric system for identification and authentication. Computer Vision and Pattern, Alger: Ecole Nationale Supérieure en Informatique.
- Duller, Y., & Wendehorst, C. (2021). Biometric Recognition and Behavioural Detection. JURI and PETI committees. Policy Department for Citizens' Rights and Constitutional Affairs.
- Eludire, A., & EO, A. (2018, April 18). Biometrics Technologies for Secured Identification and Personal Verification. Biostat Biometrics Open Acc, 6(2), pp. 1-4. doi:10.19080/BBOAJ.2018.06.555683
- Facial Recognition Technology. (s.d.). Consulté le 04 18, 2024, sur Innovatrics: bit.ly/3yeA4uG
- Fund UNICEF, T. U. (2019). Faces, Fingerprints & Feet Guidance on assessing the value of including biometric technologies. New York.
- Hegheş, N.-E. (2023). Biometric Identification: Opportunities and Challenges in the Digital World. RAIS Conference Proceedings,, (pp. 40-44).
- Iqbal, I., & Qadir, B. (2012, April). Biometrics Technology - Attitudes & influencing factors when trying to adopt this technology in Blekinge healthcare (Master Thesis). Blekinge Institute of Technology, Sweden: School of Computing.
- Iris Recognition Technology. (s.d.). Consulté le 05 01, 2024, sur Innovatrics - How it Works: bit.ly/3Y11jON
- Ross, A., & Anil K, J. (2007, January). Human Recognition Using Biometrics: An Overview. annals of telecommunications, 62(1), pp. 11-35.
- Scott, M., Hill, S., Acton, T., & Hughes, M. (2006). Biometric Identities and E-Government Services. Dans M. Khosrow-Pour, Encyclopedia of E-Commerce, E-Government, and Mobile Commerce.

- Vallance, P. (2018). Biometrics: a guide. London: Crown copyright.
- احمد محمد رفعت. (2019). التوقيع الالكتروني وحجته في الاثبات المدني. مجلة الفكر القانوني، كلية الحقوق جامعة بنها، 9(1)، الصفحات 189-256.
- بورحلة سعيدة. (2021/2020). الإدارة الالكترونية المحلية في الجزائر تطبيق النظام البيومتري على وثائق الهوية-بطاقة التعريف الوطنية وجواز السفر الدولي(اطروحة دكتوراه). كلية العلوم السياسية والعلاقات الدولية، الجزائر: جامعة الجزائر -3.
- فائزة دسوقي احمد. (2010). القياسات الحيوية وامن المعلومات. البيئة المعلوماتية الامنة: المفاهيم والتشريعات والتطبيقات(المؤتمر السادس). الرياض: جمعية المكتبات والمعلومات السعودية.
- مكتب الأمم المتحدة لمكافحة الإرهاب، المديرية التنفيذية للجنة مكافحة الإرهاب، و معهد القياسات الحيوية. (2018). عرض الأمم المتحدة التجمعي للممارسات الموصى بها بشأن الاستخدام والمشاركة المسؤولة للأنظمة البيومترية في مكافحة الإرهاب.
- منصور بن محمد الغامدي. (2005). البيانات الحيوية (البصمة الصوتية). التقنيات الحديثة في مكافحة الجريمة. الرياض: جامعة نايف العربية للعلوم الأمنية.