المؤتمر السادس
لجمعية المكتبات والمعلومات السعودية
6th Annual Conference For Saudi Library and Information Association

البيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات

المنعقد بمدينة الرياض: خلال الفترة ٢١-٢٢ ربيع ثاني ١٤٣١هـ ٦-٧ أبريل ٢٠١٠م

القياسات الحيوية وأمن المعلومات

د. فايزة دسوقي أحمد
* أستاذ مساعد- قسم دراسات المعلومات
كلية علوم الحاسب الآلي والمعلومات
جامعة الإمام محمد بن سعود الإسلامية

المستخلص

تهدف الورقة إلى معرفة مدى إمكانية استخدام القياسات الحيوية في أمن المعلومات، وكذلك تقديم التوصيات التي يمكن من خلالها استخدام تلك القياسات بشكل فاعل في المؤسسات المختلفة لضمان أمن المعلومات بها.

ومن أهم النتائج التي توصلت إليها الدراسة :

– يُقصد بالقياسات الحيوية : تقنيات تحديد هوية الأفراد من خلال الخصائص البيولوجية الموجودة في الجسد [أو السلوك مثل بصمة الإصبع، وقزحية العين وشبكيتها، والصوت، والتوقيع، ....لتمييز شخص ما عن بقية الناس.

– يمكن تقسيم القياسات الحيوية إلى فئتين: الخصائص الجسدية، والخصائص السلوكية.

– توجد عدة أنواع من القياسات الحيوية يمكن استخدامها للتوثق من الشخصية، مثل: بصمات الأصابع، وشبكية العين، والقزحية، والوجه، وهندسة اليد، والتوقيع، وطريقة استخدام لوحة المفاتيح، والصوت، والحمض النووي.

– لتطبيق القياسات الحيوية فوائد عدة من أهمها: توفير درجة أمان لشبكات المعلومات لا توفرها الطرق الأخرى للتوثق من الشخصية، والسرعة في التحقق من الشخص، وعدم القدرة على إعادة إنتاجها، وعدم ضياعها، وعدم نسيانها، وأنها غير قابلة للسرقة، ولا يمكن تحويلها لشخص آخر، وصعوبة تزويرها، ووجودها مع الشخص في أي وقت وفي أي مكان.

– ومن المشكلات التي تكتنف استخدامها: إمكانية حدوث أخطاء أثناء تسجيل القياسات الحيوية أو أثناء المضاهاة، وإزعاج الشخص ومضايقته، والتكلفة المرتفعة لبعض الأنواع من القياسات، ومقاومة الأشخاص لهذا النوع من التقنيات، والخوف على خصوصية الشخص، وإساءة استخدام البيانات التي تم الحصول عليها باستخدام القياسات الحيوية في أغراض أخرى غير التي سُجلت من أجلها، وإمكانية تعرض أنظمة القياسات الحيوية للهجوم.

Abstract

Biometrics & Information Security

The paper aims to determine the feasibility of the use of biometrics in information security, as well as make recommendations that could use these measurements effectively in the various institutions to ensure the security of their information.

The main findings of the study:

Biometrics are: techniques to identify individuals through the biological characteristics found in the body [or behavioral], such as fingerprint, iris, voice, and signature, ... to distinguish a person from the rest of the people.

Biometrics can be divided into two categories: physical characteristics and behavioral characteristics.

There are several types of biometrics can be used to authenticate the identity, such as: fingerprints, retina, iris, face, hand geometry, signature, keystroke, sound, and DNA.

Biometrics have several benefits including: providing a degree of security of information networks not available in other ways to authenticate the identity, the speed in the verification of the person, the inability to reproduce, can not be forgotten, can not be stolen, can not be transferred to another person, the difficulty of forgery, and its presence with the person at any time and anywhere.

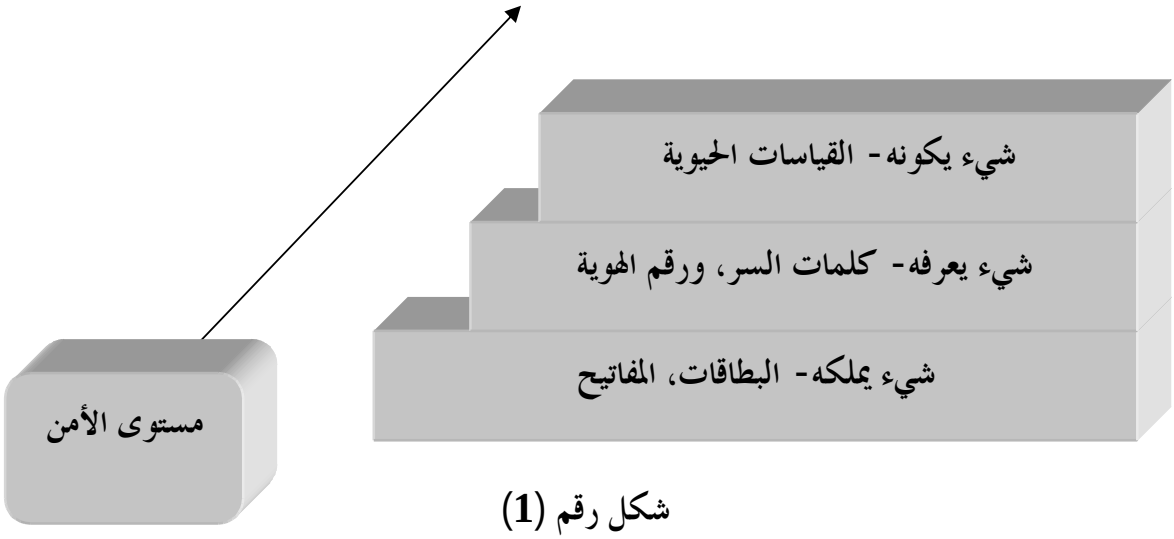
Biometrics have some drawbacks such as: the possibility of errors while recording or during the biometric matching, the harassment of the person, the high cost of some types of biometrics measurements, the resistance of people to this type of technology, fear for a person's privacy, misuse of the data that was obtained using biometric measurements, and the vulnerability of biometric systems.

المقدمة

تهدف الورقة إلى معرفة مدى إمكانية استخدام القياسات الحيوية في أمن المعلومات، وكذلك تقديم التوصيات التي يمكن من خلالها استخدام تلك القياسات بشكل فاعل في المؤسسات المختلفة لتأمين قواعد البيانات بها. ومن أهم النتائج التي توصلت إليها، وجود ثلاث فئات رئيسة يمكن استخدامها للتحقق من هوية المستخدم في مجال أمن الحاسبات والمعلومات: الفئة الأولى هي شيء يملكه الشخص، والثانية شيء يعرفه الشخص، والثالثة ما يكون عليه الشخص، أي خصائص جسدية معينة تتوافر فيه وهو ما يُعرف بالقياسات الحيوية. وأنه يمكن تقسيم القياسات الحيوية إلى فئتين: الخصائص الجسدية (المادية/الفسيولوجية)، والخصائص السلوكية. وأن هناك عدة أنواع من القياسات الحيوية يمكن استخدامها للتوثق من الشخصية، مثل: بصمات الأصابع، وشبكية العين، والقزحية، والوجه، وهندسة اليد، والتوقيع، وطريقة استخدام لوحة المفاتيح، والصوت، والحمض النووي. وأن نظم القياسات الحيوية تُستخدم إما لإثبات الهوية verification أو تحديد الهويةidentification . وأن تطبيق القياسات الحيوية يوفر فوائد عدة إلا أن هناك بعض المشكلات والعيوب التي تكتنفها.

1. علاقة القياسات الحيوية بأمن المعلومات

تلعب المعلومات في العصر الحالي المعروف بعصر المعلومات دورًا حيويًّا في نجاح أية منظمة بغض النظر عن نوعها حكومي أو خاص. وأمن تلك المعلومات أمر ضروري للمنظمات التي تهتم بحماية ممتلكاتها وخاصة أصولها الفكرية من الوقوع في أيدي المنافسين أو غيرها من الكيانات التي يمكنها إساءة استخدام تلك المعلومات (Alge and Hansen, 2007)مثل قراصنة الشبكات وإرهابيي الفضاء المعلوماتي. وهناك حاجة كذلك إلى التوثق من الأشخاص [سواء من داخل المنظمة أو خارجها] الذين يصلون إلى تلك المعلومات لضمان عدم تغييرهم لها أو الحذف منها أو التلاعب فيها. لذا فإن إدارة قواعد البيانات في حاجة إلى وجود آلية للتحقق من هوية الشخص قبل السماح له بالوصول إلى المعلومات المخزنة بها. وهناك عدة طرق رئيسة يمكن استخدام واحدة منها أو أكثر للتحقق من هوية المستخدم، يوضحها الشكل رقم (1).



شكل رقم (1)

طرق التحقق من الشخص

يتبين من الشكل السابق رقم (1) أن هناك ثلاث فئات رئيسة يمكن استخدامها للتحقق من هوية المستخدم. الفئة الأولى هي شيء يملكه الشخص مثل البطاقات الذكية، والبطاقات المعتمدة، والمفاتيح. والفئة الثانية شيء يعرفه الشخص مثل كلمات السر، وأرقام الهوية. والفئة الثالثة ما يكون عليه، أي خصائص معينة تتوافر فيه ويُقصد بها الخصائص الجسدية للشخص physical characteristic مثل بصمات الأصابع وشبكية العين وهو ما يُعرف بالقياسات الحيوية(McRobbie, 2003). وتعتبر الفئة الثالثة من أفضل النظم المستخدمة للتحقق من شخصية المستخدم؛ لأنها تعطي درجة عالية من الأمان مقارنة بالأساليب الأخرى للتوثق من الشخصية، حيث لا يمكن نسيانها أو سرقتها أو فقدها كما في كلمات السر والبطاقات والمفاتيح.

لذا هناك اتجاه الآن في مجال أمن الحاسبات والمعلومات باستبدال كلمات السر والبطاقات الذكية بالقياسات الحيوية واستخدامها لتحديد هوية الشخص والتعرف عليه، وتسمح له بالوصول جسديًّا أو منطقيًّا physical or logical access إلى مبنى، أو حاسب آلي، أو قاعدة بيانات، ... (Earley, 2006. p. 38)

ولأهمية تقنية القياسات الحيوية في حماية المعلومات من الوصول غير المصرح به، ستحاول الورقة الحالية إلقاء المزيد من الضوء على هذه التقنية.

2. تعريف القياسات الحيوية:

كلمة القياسات الحيوية Biometrics مأخوذة من اللغة اليونانية bios وتعني الحياة، وmetron أو metrikos وتعني القياس(Giesing, 2003. p.50). وكان المعنى القديم للقياسات الحيوية يشير إلى تطبيق الطرق الإحصائية والرياضية لتحليل البيانات في العلوم البيولوجية. أما الآن فإن المصطلح يشير أيضًا إلى تقنيات تحديد هوية الأفراد من خلال الخصائص البيولوجية الموجودة في الجسد [أو السلوك] مثل بصمة الإصبع، وقزحية العين وشبكيتها، والصوت، والتوقيع لتمييز شخص ما عن بقية الناس (Raab and Mason, 2003. p.83).

وقد نستخدم القياسات الحيوية بوعي أو بغير وعي؛ حيث نصف أحد الأشخاص أحيانًا على أنه "الفتى الطويل ذو الشعر البني" أو "الفتاة القصيرة ذات الشعر الأشقر والعيون الزرقاء". وهكذا نستخدم القياسات الحيوية لتحديد هوية الأشخاص بناءً على خصائصهم الجسدية(Guruprasad).

3. تاريخ استخدام القياسات الحيوية:

مرت القياسات الحيوية بكثير من مراحل التطور على مدى العصور المختلفة، ونتناول فيما يلي أهم الملامح الفارقة في تاريخ استخدام تلك القياسات:

- يوجد دليل على استخدام بصمات الأصابع منذ 500 عام قبل الميلاد، حيث أن الصفقات التجارية في بابل والمسجلة على ألواح الصلصال تحتوي على بصمات أصابع.
- استخدم قدماء التجار الصينيون بصمات الأصابع في العقود التجارية. كما استخدم الآباء الصينيون بصمات أصابع اليد والقدم لتمييز الأطفال عن بعضهم البعض.
- استخدم قدماء المصريون أوصاف الوجه لتحديد هوية التجار، وذلك للتمييز بين التجار المعروفين بسمعتهم الحسنة بناءً على المعاملات التجارية السابقة التي تم إبرامها عن التجار الجدد.

أما أهم العلامات الفارقة في العصر الحديث فتتمثل في:

- 1858م : سجل Sir William Herschel الذي كان يعمل لدى [شركة] Civil Service of India طبع اليد handprint في ظهر عقد كل عامل لتمييز العمال عن غير العمال والذين يدعون أنهم عمال يوم دفع الأجور. وكان هذا أول تسجيل نظامي لصور اليد والبصمات واستخدامها لأغراض التوثق من الشخصية.
- 1870م: طور Alphonse Bertillon طريقة تُعرف بـــ anthropometrics لتحديد هوية الأشخاص اعتمادًا على تفصيلات مسجلة عن قياسات أجسادهم، وأوصافهم الفيزيائية، وصورهم.
- 1892م: كتب Sir Francis Galton دراسة مفصلة عن بصمات الأصابع، وقد قدم تصنيفًا جديدًا باستخدام بصمات الأصابع العشر كلها. وما زالت التفاصيل (minutiae) التي استخدمها Galton مُستخدمة حتى اليوم.
- 1936م: اقترح طبيب العيون Frank Burch مبدأ استخدام شكل القزحية كطريقة للتعرف على الأشخاص.
- الستينيات: طُور نظام نصف آلي لأول مرة للتعرف إلى الوجه بواسطة Woodrow W. Bledsoe بتعاقد مع الحكومة الأمريكية.
- 1960م: نشر الأستاذ السويدي Gunnar Fant أول نموذج وصف من خلاله العناصر الفسيولوجية لإصدار الصوت. وقد اعتمدت نتائجه على تحليل أشعة إكس لأشخاص أصدروا أصوات معينة. وأُستخدمت هذه النتائج لتحسين فهم المكونات الحيوية للصوت، وتطوير نظام تعرف الصوت.
- 1963م: نشر معمل أبحاث Hughes Research Laboratories دراسة عن أتمتة تعرف بصمات الأصابع.
- 1965م: بدء أبحاث تعرف التوقيع آليًا.
- السبعينيات: تعرف الوجه خطى خطوة أخرى نحو الأتمتة، حيث استخدم A. J. Goldstein و L.D. Harmon و A. B. Lesk 21 وسيمة markers مثل لون الشعر وسماكة الشفاه لأتمتة تعرف الوجه. وكانت المشكلة لهذه الحلول المبكرة أن القياسات كانت تُجمع يدويًا.

- 1970م: طور الدكتور Joseph Perkell النموذج الأصلي لإصدار الصوت الذي قُدم في عام 1960، حيث استخدم أشعة إكس وضَّمن الفك واللسان. وقد قدم النموذج مزيدًا من فهم العناصر المعقدة لمكونات الصوت السلوكية والبيولوجية [الحيوية].
- 1974م: إتاحة نظام هندسة اليد تجاريًّا لأول مرة.
- 1977م: اخترعت شركة Veripen جهازًا يسمح بتسجيل الخصائص الديناميكية لسمات توقيع الشخص رقميًا. وقد أدى تطوير هذه التكنولوجيا إلى اختبار [جهاز] التحقق من الكتابة اليدوية آليًّا.
- 1985م: تأكيد طبيبا العيون Leonard Flom و Aran Safir أن قزحيات العيون لا يمكن أن تتشابه.
- 1985م: استخدام هندسة اليد لتوثيق الشخصية.
- 1994م: إقامة أول نظام آلي لتعرف بصمات الأصابع.
- 2000م: نشر أول بحث يصف استخدام الأوعية الدموية vascular للتعرف على الأشخاص. وهذه التقنية تستخدم شكل الأوعية الدموية الموجودة تحت الجلد في ظهر الأيدي لتحقيق التعرف (National Science Technology Council (a). 2006. P.1-19)

والجدير بالذكر أن استخدام تقنية القياسات الحيوية منذ بداية القرن العشرين كان منصبًا على الجهات الجنائية والعسكرية، ومع نهاية القرن بدأ القطاع الخاص (وبقية أجهزة القطاع العام مثل التعليم التي كانت في السابق ترفض استخدام هذه التقنية) في إدراك مزايا استخدام تلك التقنية في تحديد هوية الموظفين، والمرضى، وبقية الأفراد في مؤسساتهم.

وأكثر استخدامات تقنية القياسات الحيوية شيوعًا في القطاع الخاص هو استخدام بصمات الأصابع للمساعدة في إدارة العمل؛ حيث تُستخدم لتحديد هوية الموظفين وتتبع جداول أعمالهم ومراقبتها. واستخدام هذه التقنية يقلل من الاحتيال والخداع، ويزيد من دقة البيانات، ويقضى على ظاهرة توقيع أحد الموظفين بدلاً عن موظف آخر سواء للدخول أو عند الانصراف في الساعة المخصصة لذلك، كما أن الموظفين لم يعودوا في حاجة إلى تشارك بطاقات تحديد الهوية أو كلمات السر مما يزيد من سلامة البيانات.

وتقود أوروبا العالم الآن في استخدام القياسات الحيوية، أما أكبر سوق فمن المحتمل أنها ستكون في آسيا وبالتحديد في كوريا الجنوبية واليابان((M2SYS Technology (c).

4. فئات القياسات الحيوية:

يمكن تقسيم القياسات الحيوية إلى فئتين: الخصائص الجسدية (المادية/الفسيولوجية) physical characteristic، والخصائص السلوكية behavioral characteristics. ويُطلق على الفئة الأولى اسم القياسات الثابتة Static وهي تعتمد على استخلاص البيانات من القياسات التشريحية للشخص. أما الفئة الثانية فيُطلق عليها القياسات الديناميكية Dynamic وهي تعتمد على استخلاص البيانات من أفعال الشخص(Caldera-Serrano, 2008. p. 16). والفئة الثانية أقل ثباتًا من الأولى، وتتغير مع الضغط أو الضعف، كما أنها أقل أمنًا. ولكنها تمتلك ميزة عن الفئة الأولى حيث من الممكن أن تكون غير واضحة للشخص [أي يمكن تحديد هويته دون أن يدري أنه خضع لهذه العملية] وهي أكثر قبولاً من قبل الأشخاص لأنها أقل تطفلاً وفضولية عليهم (Giesing, 2003. p.64). ويوضح الجدول التالي رقم (1) أشهر أنواع القياسات التي تندرج تحت كل فئة منهما.

الجدول التالي رقم (1)

فئات القياسات الحيوية والأنواع التي تندرج تحتها

الخصائص الفسيولوجية	الخصائص السلوكية
• الحمض النووي (DNA). • بصمات الأصابع. • هندسة اليد أو الأصابع (hand geometry). • الوجه. • بصمة العين (قزحية العين). • شبكية العين.	• التعرف على الصوت. • التعرف على التوقيع (الإمضاء). • إيقاع حركة اليد في استخدام لوحة المفاتيح.

(المصدر: الحسين)

وينبغي أن تكون السمات الجسدية والسلوكية المستخدمة من أجل التعرف فريدة، أي أنها تكون موجودة في شخص واحد فقط وألا تظهر في شخصين على مستوى العالم. ودائمة permanent ، أي لا تتغير مع مرور الزمن أو لا يمكن تغييرها. وقابلة للقياس، أي تكون قابلة للقياس باتساق باستخدام الأدوات التقنية، كما يجب أن يكون المعلومات التي تم قياسها قابلة للتخزين على نحو فعال، وقابلة للمقارنة في قاعدة البيانات المرجعية الحيوية بحيث يمكن تحديد الفرد والتأكد منه باستخدامها. كما ينبغي أن يكون الحصول على ملامح هذه السمات غير ضار للشخص (Grandy)

5. أنواع القياسات الحيوية:

تتنوع القياسات الحيوية التي يمكن استخدامها للتوثق من الشخصية، ونتناول فيما يلي أهم تلك الأنواع:

1/5 تعرف بصمات الأصابع: Fingerprint Recognition

1/1/5 الماهية:

بصمة الإصبع عبارة عن نتوءات بارزة في بشرة الجلد تجاورها منخفضات، بحيث تجعل عملية الإمساك بالأشياء أكثر سهولة و لكل شخص شكلاً مميزاً لبصمة إصبعه. وقد ثبت أنه لا يمكن للبصمة أن تتطابق وتتماثل في شخصين في العالم حتى التوائم المتماثلة التي أصلها من بويضة واحدة، وهذه الخطوط تترك أثرها على كل جسم تلمسه وعلى الأسطح الملساء بشكل خاص (العبيد).

2/1/5 أسلوب العمل:

تعتبر تقنية تعرف بصمة الإصبع الأشهر والأكثر استخدامًا في أمن البيانات، مقارنة بمسح شبكية العين والوجه (Earley, 2006. p. 41). واستخدام نظام بصمة الإصبع نظام بسيط حيث يتم تسجيل البصمة، ثم تُصنف نماذج البصمات التي تم أخذها للشخص وفقًا لليد التي تم أخذها منها والأصابع كذلك. وبعد ذلك يتم استخدام بطاقة بصمة الإصبع لتحديد بعض النقاط الفريدة لتعرف بصمة الشخص. وتسمى هذه النقاط بعلامات markers بصمات الإصبع ويمكن استخدامها إذا تم استخدام نظام مضاهاة إلكتروني.

وقبل استخدام الكمبيوتر والتقنية المتقدمة، كانت المضاهاة تتم بالعين وكانت عملية مملة جدًا. وفي بعض الحيان كان قسم الشرطة يأخذ شهورًا طويلة لتحديد هوية المجرم الذي ارتكب جريمة ما.

وبصفة عامة، توجد 120 نقطة لتمييز بصمات الأصابع يمكن برمجتها داخل الحاسب الآلي والذي سوف يستخدمها في مضاهاة البصمة مع البصمات المخزنة في قاعدة البيانات (Guruprasad).

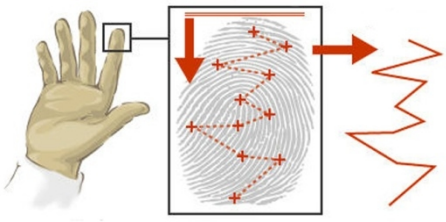
وعملية مطابقة بصمات الأصابع لا تتم على كامل البصمة؛ لأن ذلك يتطلب طاقة عالية, وسيكون من السهل سرقة البيانات المطبوعة. بالإضافة إلى أن الأوساخ أو عملية التشويه للأصبع تؤدي إلى عدم تطابق صورتين لنفس البصمة، لذلك فهي طريقة غير عملية. وبدلاً من ذلك تقوم معظم أنظمة قراءة البصمات بالمقارنة بين سمات ومعالم معينة في البصمة, وتعرف هذه الطريقة بـــالتفاصيل (minutiae). ويركز المحقق البشري و الحاسوبي على النقاط التي ينتهي عندها خط النتوء أو عند انفصال أحد النتوء إلى اثنان (تشعبات). وتسمى عادة هذه السمات المميزة بالـــ typica.

الشكل رقم (2)

السمات المميزة لبصمة الإصبع

(المصدر: العبيد)

وتستخدم برامج قارئ البصمات خوارزميات معقدة جداً للتحليل والتعرف إلى هذه التفاصيل. وتتلخص الطريقة في أن القارئ يقوم بالتعرف إلى الشكل التي تكونه التفاصيل المختلفة عند رسم خطوط مستقيمة بينها كما في الشكل التوضيحي التالي رقم (3).



الشكل رقم (3)

فكرة عمل قارئ البصمة

(المصدر: العبيد).

فإذا كان هناك بصمتان لهما نفس نهايات النتوء ونفس التشعبات, بحيث تشكل الشكل نفسه والأبعاد نفسها، فهناك احتمال كبير أن تكون لشخص واحد. وخلاصة القول أن قارئ البصمة لا يحتاج إلى أن يسجل كل التفاصيل في كلتا العينتين، بل يكفيه عدد معين من التفاصيل حتى يقارن بينهما، ويختلف هذا العدد باختلاف برنامج القارئ (العبيد).

ويتوقف أداء جهاز تعرف البصمات على طبيعة استخدامه، فإذا كان ذلك في بيئة مثل وكالات إنفاذ القانون فإن الدقة أمر ضروري والراحة والسرعة أقل أهمية؛ فعند محاولة التأكد من هوية مجرم، على سبيل المثال، فمن المهم أن يُرجع النظام تطابق تام، بغض النظر عن الوقت الذي يستغرقه ذلك. أما في بيئة مثل المدارس فإن السرعة والكفاءة لهما الأهمية القصوى، فعلى سبيل المثال، إذا كان 200 طفلاً يحاولون استخدام نظام البصمة في المدرسة، فالأكثر أهمية أن يعمل النظام بكفاءة وبمعدل عال من السرعة ((M2SYS Technology (b)).

3/1/5 المزايا

من أهم المزايا التي تتمتع بها هذه التقنية أنها:

- معروفة ومألوفة لدى الناس.
- تعمل بشكل جيد (Earley, 2006. p. 41).
- سهلة الاستخدام، وخاصة بعد استخدام الحاسب فيها (Guruprasad).
- أقل تدخلاً وضررًا بالنسبة للمستخدم (Muthukrishnan).

4/1/5 المشكلات:

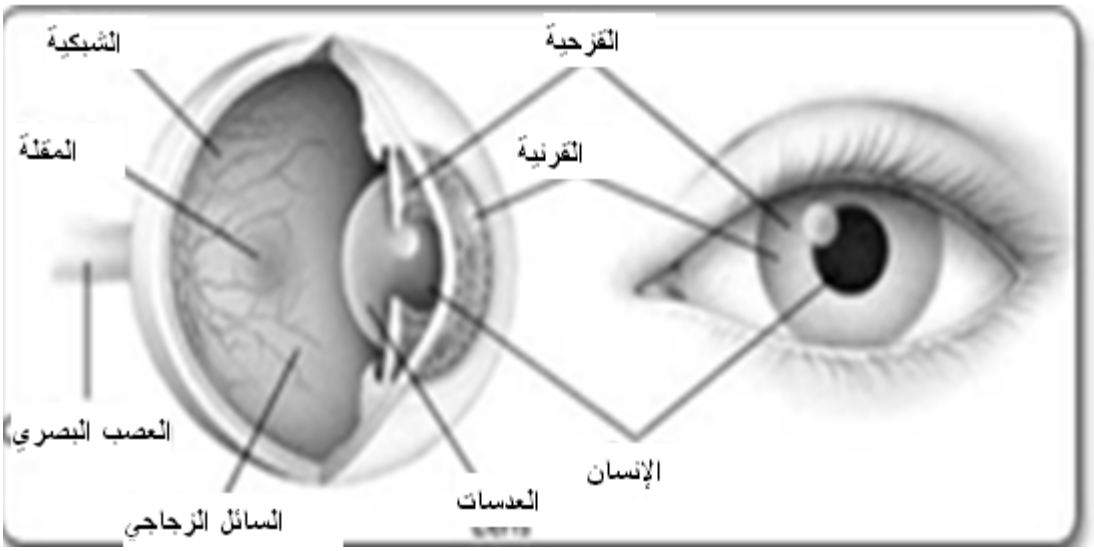
من أهم المشكلات التي تعترض هذه التقنية:

- **الإكراه:** إكراه مستخدم شرعي على استخدام إصبع يده للدخول من قبل شخص مهاجم. ويمكن التغلب على هذه المشكلة من خلال تسجيل بصمة إصبع سبابة اليد اليمنى كبصمة معتمدة للشخص، وتسجيل بصمة إصبع سبابة اليد اليسرى كبصمة "إكراه". لذا إذا تم إكراه هذا الشخص على استخدام بصمة إصبعه فعليه استخدام بصمة سبابة اليد اليسرى وبهذا سيفتح الباب، ولكن هذا سيُعطي إشارة للنظام أن هذا تم فعله تحت التهديد والإكراه وعليه سيتصرف الأمن بالطريقة المناسبة.
- **التزوير:** يمكن تزوير شكل البصمة، واستخدام صورة للبصمة. ولكن يمكن للأجهزة اكتشاف ذلك حيث يمكنها التعرف إلى الجلد الميت من الحي وذلك من خلال فحص امتصاص الطيف أو انعكاسه، حيث يختلف الطول الموجي المنعكس أو الممتص من الجلد الميت عن الحي، كما يمكن فحص تدفق الدم في الجلد (Earley, 2006. p. 41).
- **القبول الزائف:** قد يحدث قبول زائف عندما يقوم المستخدم الذي لم يسبق أن تم تسجيله في النظام (وبالتالي لا يوجد عنه معلومات مخزنة) بتلقي إما الإذن للوصول إلى نظام أو منحه التحقق من الهوية. ويمكن أيضا أن يحدث قبول زائف عندما يحدد النظام خطأً المستخدم كمستخدم مختلف في قاعدة البيانات. (M2SYS Technology. (b)). ونسبة احتمال حدوث قبول زائف في نظم التحقق الحديثة المعتمدة على بصمة الإصبع أقل من واحد في المليون (alamoudi).
- **الرفض الزائف:** قد يحدث رفض زائف عندما يفشل النظام في التعرف على مستخدم مُسجل. وبعبارة أخرى، على الرغم من وجود بيانات مُسجلة عن المستخدم فإن النظام يقوم بإرجاع "لم يتم العثور على تطابق" ونتيجة لذلك، يتم رفض المصادقة على المستخدم. وقد يحدث هذا أيضًا إذا كان هناك انحراف في

البصمة عند تسجيلها في قاعدة البيانات. ولمكافحة هذه المشكلة، يجب أن تكون نظم التحقق من الهوية مبرمجة "للتعلم" من العينات لاتخاذ قرار يستند إلى مجموعة من عينات البصمات، بدلا من إعداد المقارنة باستخدام عينة واحدة ((M2SYS Technology. (b). وترفض نظم التحقق الحديثة المعتمدة على بصمة الإصبع حوالي 3% من المستخدمين المرخصين (alamoudi).

2/5 تعرف شبكية العين Retina Recognition

تَعرف الشبكية يتعلق بتسجيل وتحليل أشكال الأوردة الدموية الموجودة في العصب الموجود في خلفية مقلة العين eyeball والذي يعالج الضوء الداخل من خلال إنسان العين [يوضح الشكل رقم (4) مكان وجود الشبكية]. وطريقة عمل هذه التقنية يتلخص في إطلاق شعاع من الضوء ذو شدة منخفضة داخل مقلة العين وتسجيل شكل الأوردة في العين. وينبغي أن يكون الشخص قريب جدًا من عدسات جهاز مسح الشبكية، ويحدق مباشرة في العدسات، ويظل ساكنًا أثناء مرور الضوء داخل إنسان العين، وأية حركة من الشخص قد تتطلب إعادة العملية من البداية(Rhodes, 8-9).



الشكل رقم (4)

تشريح العين

(المصدر: Muthukrishnan).

ومن أهم مزايا تعرف الشبكية أن أشكالها متميزة جدًا، وكل عين لها شكل فريد من الأوعية الدموية؛ وحتى أعين التوائم المتماثلة مختلفة. إلا أن استخدامها في التعرف على الأشخاص يكتنفه بعض العيوب منها:

- رغم أن شكل الشبكية ثابت على مر عمر الإنسان، إلا أنها يمكن أن تتأثر بأمراض مثل المياه الزرقاء أو البيضاء، والبول السكري، وضغط الدم المرتفع.
- صغر الشبكية ووجودها داخل العين وصعوبة قياسها يجعل من الصعب الحصول على صورة منها(Rhodes, P. 9).
- هناك مخاوف من أن مصدر الضوء المستخدم قد يسبب أضرارًا للعين.
- تكلفة تكنولوجيا مسح شبكية العين وعدم قدرتها على التطور وفقا لأحدث التكنولوجيا جعلت من أجهزة المسح الضوئي لشبكية العين أمر غير عملي بالنسبة لمعظم الحالات(Grandy, 2005).
- تلقى مقاومة شديدة من الأشخاص؛ لأنهم يخافون على أعينهم(Giesing, 2003,64).

3/5 تعرف القزحية: Iris recognition

القزحية (المنطقة الملونة في العين) هي العضو الداخلي المحمي من العين، تقع خلف القرنية وأمام العدسات [يوضح الشكل رقم (4) مكان وجود القزحية]. وتتمثل طريقة عمل نظم تعرف القزحية في إنارة الماسح للقزحية بضوء الأشعة تحت الحمراء غير المرئية، مما يبين تفاصيل أكثر تكون غير مرئية للعين المجردة(Muthukrishnan)، والتقاط صورة أبيض وأسود ذات درجة وضوح عالية للقزحية باستخدام كاميرا صغيرة ذات جودة عالية. ثم يحدد النظام حدود القزحية، ويُنشئ نظام إحداثيات ويحدد مناطق التحليل في هذا النظام. (Rhodes ,P. 8)

وقد تم تطوير نظم تعرف قزحية العين كنظم متطورة من نظم مسح الشبكية التي تُستخدم ولكن لا يتم قبولها على نطاق واسع بسبب العديد من المشكلات وعدم الدقة التي تعترضها، لذا تم استبدالها بنظم التعرف إلى القزحية. ورائد هذه النظم هو الدكتور John Daugman من قسم علم الحاسب الآلي بجامعة كامبردج

Cambridge والخوارزمية المستخدمة اليوم لمسح القزحية تُسمى باسمه Daugman algorithm (Guruprasad).

ومن أهم مزايا استخدام هذه التقنية:

- تتكون القزحية خلال الشهر الثامن للحمل، ولا تتغير خصائصها على مر عمر الإنسان إلا إذا تعرضت لأذى(Rhodes ,P. 8).
- يمكن الحصول على صور للقزحية تكون كافية لتحديد الهوية الشخصية مع ثقة عالية جدًا من مسافة تصل إلى حوالي 3 أقدام (Muthukrishnan).
- عدد نقاط التعرف تصل إلى 580 نقطة متميزة لكل شخص اعتمادًا على وضوح صورة القزحية التي تم الحصول عليها أثناء المسح. ولأن عدد نقاط المضاهاة الفريدة كبير، ويكفي عدد صغير من هذه النقاط للحصول على مضاهاة إيجابية لشخص واحد على كوكب الأرض، فإن هذه النظم تتميز بموثوقية عالية. لا تؤثر العدسات الملونة أو اللاصقة على نظام تعرف القزحية، لذا لا يمكن الاحتيال عليها بسهولة(Guruprasad).
- سهلة الاستخدام حيث لا تستغرق سوى عدة ثوان(Grandy, 2005).

ومن عيوبها:

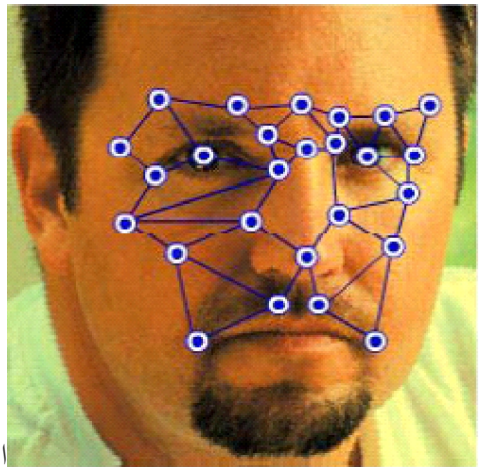
- قد تتضرر العين من استخدام الأشعة تحت الحمراء لمسح القزحية، أو تصيبها بعض الأمراض البصرية إذا كانت هناك حاجة للتحقق من هوية الشخص أكثر من مرة في اليوم.
- إذا تم مسح الشخص الميت جسديًّا أو مخيًّا ببصمة القزحية فإن المضاهاة تتم بنجاح(Muthukrishnan).
- تكلفة شراء الأجهزة والتشغيل مرتفعة.
- ينبغي أن يكون الشخص معتدل وثابت عند المسح [تتطلب جلسة معينة حتى تتم بدقة].

- يجب أن تكون جودة صورة القزحية مرتفعة جدًا حتى يقبلها النظام ويعالجها. وإذا كانت جودة الصورة قليلة، فإن نظام تعرف القزحية لن يتمكن من معالجتها بشكل مناسب ويمكن أن يؤدي ذلك إلى تحديد هوية خاطئ (Guruprasad).

4/5 تعرف الوجه Facial recognition

تعرف الوجه وتحديد [الهوية عن طريق الصور] هي استخدام آخر واسع النطاق للقياسات الحيوية. ويُستخدم هذا النوع من التعرف في جميع أنحاء العالم للحالات المهمة، مثل جوازات السفر الدولية، والحالات التي تحتوي على أسماء(Grandy, 2005).

ويعتمد نظام تعرف الوجه على التعرف إلى هيكل الوجه، فالمسافات بين العين والأنف والفم،... إلخ فريدة في الشخص وفرصة تكرارها في شخص آخر نادرة جدًا. وتعرف الوجه هو رسم خريطة لوجه الشخص وتذكر البيانات الأساسية عن محيط الوجه والمسافات بين مكوناته وعند المسح يتم محاولة البحث عن أقرب مضاهاة(Guruprasad). ويوجد أكثر من 80 نقطة في بنية الوجه يمكن استخدامها في تحديد الوجه بشكل لا لبس فيه. ولا تستخدم النظم المختلفة عادة هذه النقاط جميعها، ولكنها تحلل عدد صغير منها من خلال تحليل المسافات بين النقاط. وتتأثر عملية تصوير الوجه بالعديد من العوامل منها الإضاءة، وزاوية التصوير، والمسافة بين جهاز التصوير والشخص، وجودة جهاز التصوير(Caldera-Serrano, 2008. 17).



الشكل رقم (5)

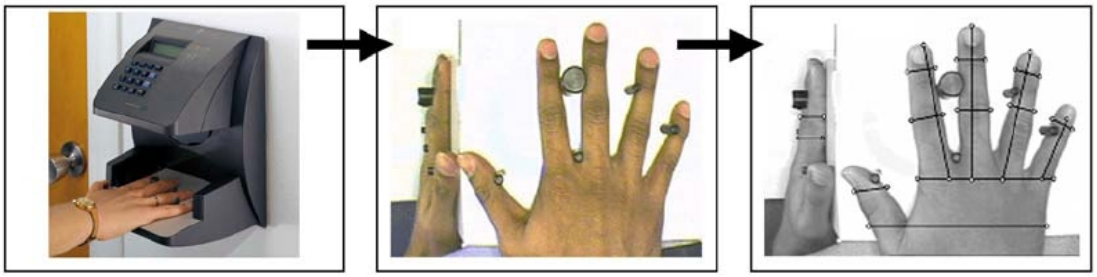
حديد بنية الوجه

ومن عيوب تعرف الوجه:

- تعرف الوجه ليس الشكل الأكثر دقة لتحديد الهوية بسبب التشابه الموجود في بنية [هيكل] الوجه، وخاصة بين الأقارب والأخوات [وبصفة خاصة التوائم المتماثلة].
- يمكن إجراء التغييرات الفسيولوجية physical جراحيًّا بسهولة نسبية(Grandy, 2005).
- وجود موانع تتعلق بكشف الوجه لأسباب دينية أو ثقافية(Giesing, 2003,63).

5/5 هندسة اليد Hand Geometry

تُستخدم هندسة اليد منذ 30 عامًا تقريبًا للتحكم في دخول الأماكن. وتأخذ تقنية هندسة اليد 96 قياسًا لليد، تشمل العرض، والطول، وطول الأصابع، والمسافات بين ملتقى الأصابع وعُقلها، وأشكال المفاصل. وتستخدم نظم هندسة اليد كاميرا ضوئية وضوءاً يُطلق من صمام ثنائي وعاكسات لتسجيل صورة متعامدة وثنائية الأبعاد لظهر اليد وجوانبها(Rhodes ,P. 8). ويتم ترقيم digit القياسات المأخوذة لليد ومقارنتها بالبيانات المخزنة من قبل لصور الأيدي (National Science Technology Council, 2006(b). p. 4) . ورغم أن الشكل الأساسي ليد الشخص تبقى ثابتة نسبيًا على مدى عمره، فإن العوامل الطبيعية والبيئية يمكن أن تسبب اختلافات طفيفة (Rhodes ,P. 8).



شكل رقم (6)

هندسة اليد

(المصدر: National Science Technology Council, 2006(b))

ومن مزايا هندسة اليد:

- نظام سهل الاستخدام.
- طريقة تناسب [الحالة] التي يكون مطلوب فيها التحقق من عدد كبير من الأشخاص.
- لا تتأثر بحالة الجلد(Giesing, 2003. 58-59,62).

ومن عيوبها:

- تحتاج إلى جهاز حجمه كبير.
- تحتاج إلى وجود الشخص نفسه في المكان. تواجد جسدي(Giesing, 2003,62).

6/5 تعرف التوقيع Signature Recognition

يتم في هذه التقنية تحديد الهوية باستخدام توقيعات خط اليد. ونظم تَعرف التوقيع تحلل عنصرين الأول التوقيع ذاته (شكل التوقيع)، والثاني الملامح المميزة لعملية التوقيع (آلية التوقيع) مثل السرعة والضغط على القلم والاتجاهات. وربما يكون من الممكن تقليد التوقيع، ولكن من الصعب إن لم يكن من المستحيل تقليد آلية التوقيع(Giesing, 2003. 61).

وتستخدم نظم تعرف التوقيع أدوات مختلفة منها اللوح الرقمي حيث يوقع الشخص باسمه على اللوح [الشكل رقم (7)] ، ثم يحلل النظام آليات التوقيع ويمكنه تتبع اختلافات التوقيع عبر الزمن. ثم يتم ترميز بيانات آليات التوقيع وضغطها في قالبtemplate(Rhodes, P. 9). ومن هذه الأدوات أيضًا الماسحات الضوئية البسيطة، وكاميرات الفيديو، والأقلام التي تحتوي على مجسات [أجهزة حساسة] sensors، والموجات فوق الصوتية(Grandy, 2005). وأهم مزايا تعرف التوقيع أنه يحظى بقبول شديد من الشخص. أما أهم عيوبه أنه غير ثابت مع الزمن(Giesing, 2003,62). ويتأثر بالمرض والتقليد(alamoudi) .

الشكل رقم (7)

تعرف التوقيع

7/5 استخدام لوحة المفاتيح Keystroke

تعتمد فكرة هذه التقنية على تسجيل بعض سمات استخدام الشخص للوحة المفاتيح، ثم محاولة التعرف على شخص ما إذا كان يتبع هذه السمات(Guruprasad). ويقيس نظام تعرف استخدام لوحة المفاتيح متغيرين أساسيين هما وقت الكمون Dwell time (طول الوقت الذي يكمن فيه الشخص على مفتاح معين)، ووقت الانتقال Flight time (طول الوقت الذي يستغرقه الشخص للانتقال بين المفاتيح) .(Giesing, 2003. 64).

8/5 تعرف الصوت Sound recognition

للصوت عناصر وخصائص مميزة له مثل نغمة الصوت، وإيقاعه، ونبرته وملامح أخرى تجعل تلك الخصائص محددة لشخص معين، وهذا ما تعتمد عليه نظم تعرف الصوت في التوثق من الشخص.

والتعرف إلى الكلام آليًّا Automatic speech recognition (ASR) هو مجال بحثي حديث، يحظى باهتمام عدد كبير من مهندسي الحاسب الآلي للعمل على تحسين نظم المحادثة بين الإنسان والآلة. وتسمح هذه النظم بالوصول إلى المعلومات المخزنة في الحاسبات بوسائل طبيعية وعامة للاتصال مثل الحديث. ويمكن

تطبيق استخدام تعرف الصوت بعدة طرق من أهمها، تحدث الشخص من خلال استخدام مكبر صوت، أو من خلال استخدام نظم IVR (interactive voice response) ، ويعتمد هذا التطبيق على استخدام الهاتف للوصول إلى المعلومات المسجلة على الحاسب، وتعمل نظم IVR في هذه الحالة كجسر بين الأشخاص وقواعد البيانات المحسبة من خلال توصيل المستخدمين بالمعلومات المطلوبة من أي مكان وفي أي وقت.

ومثل هذه النظم تفيد الأشخاص ذوي الاحتياجات الخاصة مثل المكفوفين، وهي مقبولة لدي الأشخاص. إلا أنها تواجه عدد من الصعوبات [سواء عند التسجيل أو المضاهاة]؛ حيث تتأثر بالظروف المحيطة مثل استخدام مكبرات صوت microphones ذات خصائص مختلفة، وتغير جودة قنوات التسجيل، وارتداد الصوت والصدى، والمسافة والاتجاه لمكبرات الصوت الحرة hands-free ، والضوضاء الموجودة في الخلفية وتشوه إشارات الصوت الداخلة(Caldera-Serrano, 2008. P.16-17). وتأثر الصوت بالمرض وإمكانية تقليده (alamoudi) وتغيره مع الزمن.

9/5 الحمض النووي DNA

تُستخدم قياسات الحمض النووي DNA على نطاق واسع في الحالات القضائية. وخاصة في حالات الاغتصاب والاعتداء الجنسي لتحديد مرتكبها. ويمكن استخلاص الحمض النووي من أي مصدر جسدي مثل الشعر أو الدم أو العرق والإفرازات وأية سوائل جسدية أخرى. ولا يمكن أن تتكرر مضاهاة الحمض النووي DNA في أكثر من 200 مليون حالة (Guruprasad).

ومن الممكن استخدام الحمض النووي في تأمين شبكات المعلومات. وهو يختلف عن القياسات الحيوية الأخرى بعدة طرق:

- يتطلب تحليل الحمض النووي وجود عينة مادية مثل الشعر أو الدم.
- لا تتم المضاهاة في الحمض النووي في الوقت ذاته، وحاليًا لا تتم جميع المراحل بشكل آلي.
- مضاهاة الحمض النووي لا تستخدم القوالب templates أو استخلاص الملامح، ولكنها تمثل مقارنة بين عينات حقيقية.

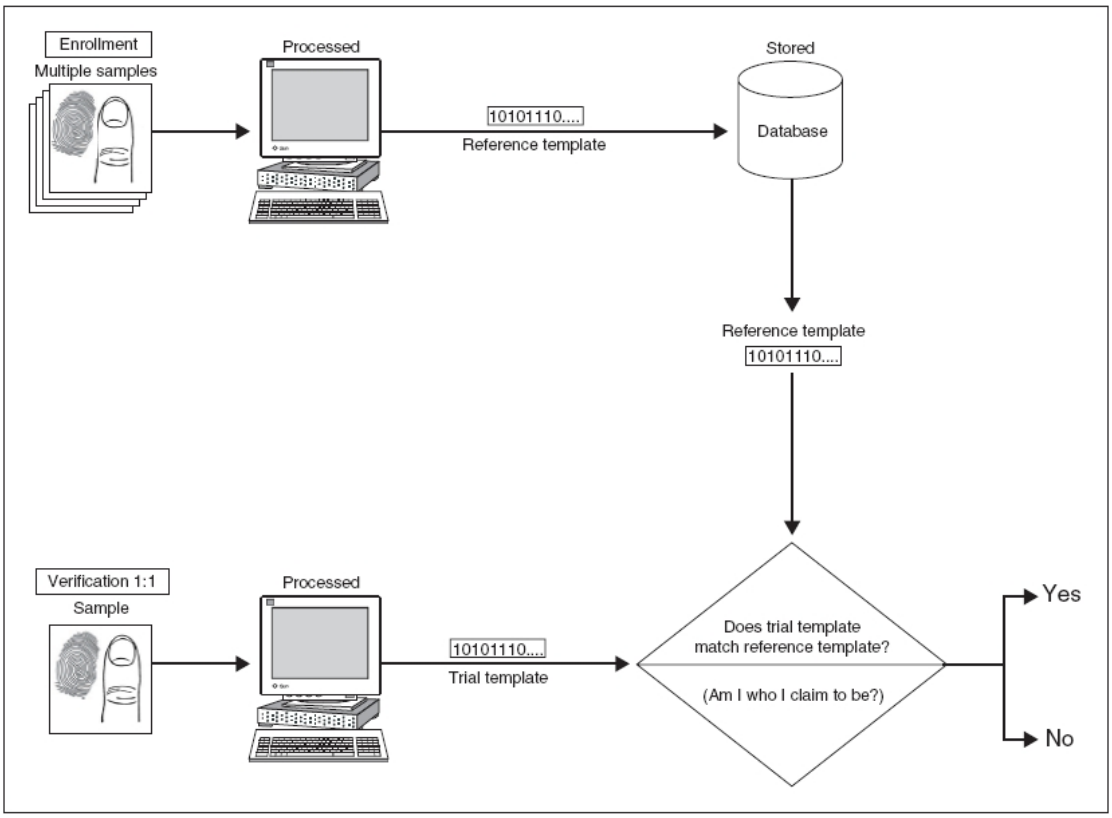
وبغض النظر عن هذه الاختلافات فإن الحمض النووي نوع من القياسات الحيوية التي تستخدم الخصائص الفسيولوجية لتحديد الهوية. ومن مزاياه أنه أكثر القياسات الحيوية دقة. إلا أن تحليل الحمض النووي قد يأخذ أسابيع أو شهورًا حتى تتم معالجته [وهذا لا يتناسب مع طبيعة الحاجة إلى الوصول الآني إلى قواعد البيانات المخزنة في الحاسبات الآلية في المؤسسات المختلفة]، ولكن مع الأبحاث المستمرة في هذا المجال سيتمكن العلماء من تقليل زمن تلك العملية إلى أقل من نصف ساعة(Maestre and Nichols. P.8,11)

6.طريقة عمل القياسات الحيوية:

أشرنا عند الحديث عن أنواع القياسات الحيوية إلى طريقة عمل كل منها، ويمكن القول بأن تقنيات القياسات الحيوية تختلف في تعقيدها، وقدراتها، وأدائها إلا أنها تتشارك جميعًا في العديد من العناصر. فهي نظم صُممت أساسًا للتعرف على الأشخاص، وهي تستخدم أدوات مثل آلات التصوير والفحص scanning للحصول على صور أو تسجيلات أو قياسات لخصائص الفرد، واستخدام الحاسبات والبرمجيات لاستخلاص، وترميز، وتخزين، ومقارنة هذه الخصائص، إلا أنها ورغم أن تقنيات القياسات الحيوية تقيس خصائص مختلفة بطرق مختلفة، فإن نظم القياسات الحيوية تعتمد على نفس العمليات والتي يمكن تقسيمها إلى مرحلتين متمايزتين هما التسجيل enrollment وإثبات الهوية أو تحديدها. وتتلخص الخطوات في كل من المرحلتين في:

1. أخذ العينات من الشخص، سواء عينات من الخصائص الفيزيائية أو السلوكية بواسطة الأجهزة.
2. معالجة العينات لاستخلاص الملامح المميزة فيها.
3. تخزين قوالب العينات.
4. مضاهاة قوالب العينات المخزنة بالخصائص المأخوذة من الشخص المطلوب تحديد هويته.
5. اتخاذ قرار يبين ما إذا كان هذا هو الشخص المقصود أم لا(Giesing, 2003. p.55-57)

ووفقًا للتطبيق يمكن استخدام نظم القياسات الحيوية إما لإثبات الهوية verification أو تحديد الهوية identification. ويتحقق النظام في حالة "إثبات الهوية" –يُطلق عليه أيضًا التوثق authentication- من أن هوية الشخص هي بالفعل كما يدعيها بناءً على البيانات المسجلة عنه مسبقًا، وتسمى هذه المضاهاة (واحد إلى واحد one-to-one). (Podio and Dunn. p. 2)

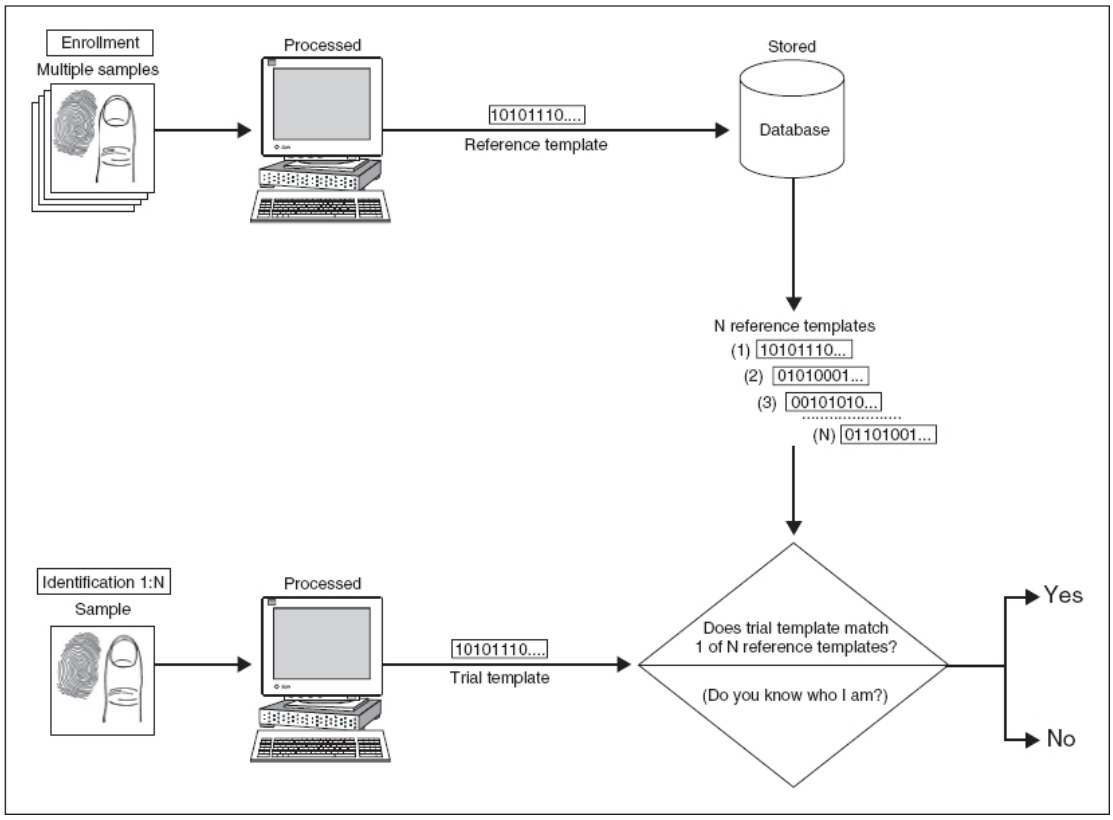


الشكل رقم (8)

إثبات الهوية باستخدام القياسات الحيوية

(المصدر: Rhodes, p. 4)

وفي حالة "تحديد الهوية" فإن نظام القياسات الحيوية يحدد الشخص من بين جميع الأشخاص المسجلين في قاعدة البيانات [أي أن النظام يعمل على تحديد من يكون هذا الشخص]، وتُسمى هذه الطريقة في بعض الأحيان مضاهاة (واحد إلى العديد one-to-many). (Podio and Dunn. p. 2) .



الشكل رقم (9)

تحديد الهوية باستخدام القياسات الحيوية

(المصدر: Rhodes, p. 6)

وفي غالبية بيئات الوصول للحاسبات أو الوصول للشبكات فإن الأنسب لها استخدام حالة "إثبات الهوية". حيث يقوم الشخص بإدخال حسابه، أو اسمه، أو بطاقة ذكية، وبدلاً من إدخال كلمة سر يقوم بوضع إصبعه على الجهاز الإحساس أو يكفي النظر إلى آلة تصوير للتوثق منه(Podio and Dunn. p. 2).

7. فوائد تطبيق القياسات الحيوية

لتطبيق القياسات الحيوية فوائد عدة من أهمها:

- توفير درجة أمان لشبكات المعلومات لا توفرها الطرق الأخرى للتوثق من الشخصية.
- السرعة في التحقق من الشخص؛ لأن معظم القياسات الحيوية تتم آليًّا فإن عملية التحقق عادة ما تكون سريعة جدًا، وفي أغلب الحالات تأخذ عدة ثوان فقط(Rhodes, 2).
- عدم الحاجة إلى أرقام شخصية لتحديد الهوية.
- عدم القدرة على إعادة إنتاجها.
- عدم ضياعها، مما يعني زيادة الأمن.
- غير قابلة للنسيان.
- غير قابلة للسرقة.
- لا يمكن تحويلها لشخص آخر.
- موجودة دائمًا مع الشخص في أي وقت وفي أي مكان.
- خفض التكلفة من خلال التخلص من تكلفة إدارة كلمات السر، وهذه ميزة اقتصادية كبيرة(Giesing, 2003. P66-67)
- صعوبة التزوير.
- لا يمكن تخمين بصمة الإصبع مثلاً, مثل ما نستطيع تخمين كلمة السر (العبيد).

8. عيوب القياسات الحيوية

من أهم عيوب ومشكلات القياسات الحيوية:

- إمكانية حدوث أخطاء أثناء تسجيل القياسات الحيوية أو أثناء المضاهاة.
- إزعاج الشخص ومضايقته.
- التكلفة المرتفعة لبعض الأنواع من القياسات.
- الحاجة إلى تعليم المستخدمين وتدريبهم.
- مقاومة الأشخاص لهذا النوع من التقنيات.

- فقد المعلومات المخزنة والتي يتم الحصول عليها من القياسات الحيوية، ويستدعي ذلك توفير حماية لها.
- وجود اعتبارات شخصية وثقافية ودينية، حيث توحي الكلمة للبعض بسلوك إجرامي، والخوف على خصوصية الشخص؛ لأن المعلومات لا تُجمع عن الشخص بل من جسده.
- فقد أجزاء الجسم، أو عدم وجودها أساسًا مثل الأطراف(Giesing, 2003. p.67).
- إساءة استخدام البيانات التي تم الحصول عليها باستخدام القياسات الحيوية في أغراض أخرى غير التي سُجلت من أجلها(Maestre and Nichols. P.9) .
- تعرض أنظمة القياسات الحيوية للهجوم، فعلى سبيل المثال يمكن:
  - **تقديم مقياس حيوي مزيف لجهاز الإحساس:** يتم تقديم مقياس حيوي مزيف كمدخل (input) لجهاز الإحساس, ومن الأمثلة على ذلك: أصبع مزيف, نسخة من التوقيع, قناع للوجه, وغيرها.
  - **إعادة إرسال الإشارات المخزنة من إرسال سابق:** يتم تسجيل الإشارة المرسلة من جهاز الإحساس أثناء دخول المستخدم الحقيقي إلى النظام, ثم إعادة إرسالها في وقت لاحق من خلال القناة التي تلي جهاز الإحساس دون الحاجة لاستخدام جهاز الإحساس. ومن الأمثلة على ذلك إرسال صورة سابقة للبصمة أو تسجيل سابق للصوت.
  - **السيطرة على عملية استخراج الملامح المميزة:** يتم هذا الهجوم باستخدام حصان طروادة (Trojan horse) على مستخرج الملامح, حيث يجعله ينتج ملامح محددة من قبل المهاجم.
  - **استبدال الملامح المميزة المستخرجة:** يقوم المهاجم بالدخول على القناة التي تربط مستخرج الملامح بالمقارن ويستبدل الملامح المميزة المستخرجة بأخرى محددة من قبل المهاجم.
  - **تحريف المقارنة:** تتم مهاجمة المقارن بحيث ينتج نتائج تطابق محددة.
  - **تغيير القالب المخزن:** تتم مهاجمة قاعدة البيانات وتغيير القالب المخزن.
  - **الهجوم على القناة بين قاعدة البيانات والمقارن:** واستبدال القالب المرسل إلى المقارن بقالب آخر.
  - **تحريف النتيجة النهائية:** إذا كان هذا الهجوم ممكنًا فسوف يصبح نظام التوثق من المستخدم عديم الفائدة (الحسين).

9. النتائج

من أهم النتائج التي توصلت لها الورقة الحالية:

- توجد ثلاث فئات رئيسة يمكن استخدامها للتحقق من هوية المستخدم في مجال أمن الحاسبات والمعلومات: الفئة الأولى هي شيء يملكه الشخص مثل البطاقات الذكية، والبطاقات المعتمدة، والمفاتيح. والفئة الثانية شيء يعرفه الشخص مثل كلمات السر، وأرقام الهوية. والفئة الثالثة ما يكون عليه، أي خصائص معينة تتوافر فيه، ويُقصد بها الخصائص الجسدية للشخص مثل بصمات الأصابع وشبكية العين وهو ما يُعرف بالقياسات الحيوية.
- يُقصد بالقياسات الحيوية "تقنيات تحديد هوية الأفراد من خلال الخصائص البيولوجية الموجودة في الجسد [أو السلوك] مثل بصمة الإصبع، وقزحية العين وشبكيتها، والصوت، والتوقيع، ....لتمييز شخص ما عن بقية الناس".

- يوجد دليل على استخدام بصمات الأصابع منذ 500 عام قبل الميلاد لتحديد هوية الأشخاص.
- يمكن تقسيم القياسات الحيوية إلى فئتين: الخصائص الجسدية (المادية/الفسيولوجية) physical characteristic، والخصائص السلوكية behavioral characteristics.
- تتنوع أنواع القياسات الحيوية التي يمكن استخدامها للتوثق من الشخصية، ومن أهمها: بصمات الأصابع، وشبكية العين، والقزحية، والوجه، وهندسة اليد، والتوقيع، وطريقة استخدام لوحة المفاتيح، والصوت، والحمض النووي.
- يمكن استخدام نظم القياسات الحيوية إما لإثبات الهوية verification ، أو تحديد الهوية identification.
- لتطبيق القياسات الحيوية فوائد عدة من أهمها: توفير درجة أمان لشبكات المعلومات لا توفرها الطرق الأخرى للتوثق من الشخصية، والسرعة في التحقق من الشخص، وعدم القدرة على إعادة إنتاجها، وعدم ضياعها، وعدم نسيانها، وأنها غير قابلة للسرقة، ولا يمكن تحويلها لشخص آخر، وصعوبة تزويرها، ووجودها مع الشخص في أي وقت وفي أي مكان.
- ومن المشكلات التي تكتنف استخدامها: إمكانية حدوث أخطاء أثناء تسجيل القياسات الحيوية أو أثناء المضاهاة، وإزعاج الشخص ومضايقته، والتكلفة المرتفعة لبعض الأنواع من القياسات، ومقاومة

الأشخاص لهذا النوع من التقنيات، والخوف على خصوصية الشخص، وإساءة استخدام البيانات التي تم الحصول عليها باستخدام القياسات الحيوية في أغراض أخرى غير التي سُجلت من أجلها، وإمكانية تعرض أنظمة القياسات الحيوية للهجوم.

10. التوصيات:

حتى نضمن استخدام القياسات الحيوية في تأمين المعلومات في مختلف المؤسسات بشكل فاعل، يمكن تقديم التوصيات التالية:

- على المؤسسات أن تعلم أنه لا يوجد نظام قياس حيوي واحد أفضل من بقية القياسات، فالقياسات الحيوية تختلف في تكلفتها وملاءمتها للتطبيقات المختلفة. وقبل اختيار المؤسسة لحل تحديد هوية المستخدم عن طريق القياسات الحيوية عليها أن تقيم احتجاجاتها بدقة. والقائمة التالية تحتوي على العناصر الواجب أخذها في الاعتبار عند اختيار نظام القياسات الحيوية في مؤسسة ما:
  - مستوى الأمن المطلوب.
  - الدقة.
  - التكلفة ووقت الإنجاز.
  - تقبل المستخدم لها(Muthukrishnan).
- إن الخصائص الحيوية هي معلومات شخصية تفصح عن الكثير من خصائص الشخص وعمره والأمراض التي يعاني منها، لذا ينبغي توفير العناصر التالية لها:
  - الإعلام: ينبغي إعلام الشخص بما سيتم فعله مع البيانات [المخزنة عنه].
  - الاختيار: الشخص في حاجة إلى الموافقة على جمع البيانات عنه.
  - الوصول: الشخص في حاجة إلى الوصول إلى المعلومات المخزنة عنه في وقت الحاجة.
  - الأمن: ينبغي توفير الحماية للبيانات المخزنة عن الشخص من قبل المؤسسة (Giesing, 2003. P. 72-73).
- تعليم المستخدمين الحاليين والمستقبليين عن حقائق ومزايا تقنية القياسات الحيوية حتى نضمن لها القبول(M2SYS Technology (a)).

- دمج القياسات الحيوية مع التقنيات الأخرى مثل البطاقات الذكية (Raab and Mason, 2003. p.84).
- زيادة الأمان في أنظمة التوثق من الشخصية المعتمدة على المقاييس الحيوية: ويمكن ذلك بعدة طرق من أهمها:
  - استخدام عدة نماذج، واستخدام عدة أجهزة إحساس، واستخدام أكثر من مقياس حيوي (كاستخدام بصمة الأصبع وبصمة العين معًا، واستخدام أكثر من وحدة (كاستخدام بصمة الإبهام وبصمة السبابة معًا)، واستخدام أكثر من صورة (حيث يُطلب من المستخدم إدخال نفس المقياس أكثر من مرة).
  - استخدام العلامة المائية (Watermarking): وهي تضمين معلومات عن الوسائط المتعددة (مصدر البيانات, وجهتها.. الخ) داخل البيانات نفسها (صورة, صوت.. الخ), هذا التضمين قد يكون ظاهر للمستخدم أو غير ظاهر. والهدف من استخدام العلامة المائية في المقاييس الحيوية هو التأكد من مصدر البيانات بالإضافة إلى اكتشاف أي تغيير قد يحدث فيها.
  - التشفير (Encryption): هناك طريقتين للجمع بين استخدام التشفير واستخدام المقاييس الحيوية في أنظمة حماية المعلومات:
    - تشفير القوالب المخزنة في قاعدة البيانات لحمايتها من المهاجمين.
    - استخدام المقاييس الرقمية كمفتاح لتشفير البيانات (الحسين).

المراجع:

(1)الحسين، أروى. استخدام المقاييس الحيوية *(Biometrics)* في التوثق من الشخصية.- متاح في: http://knol.google.com/k/arwa-alhussain/biometrics/1k8z259px1m4v/1#.- تم الوصول إليه في: 2/7/2009.).

(2) العبيد، أمينة. قارئ بصمة الأصابع.- متاح في: http://knol.google.com/k/amina-alobaid/-/2vtwdmzpxv2gl/9#.- تم الوصول إليه في: 10/7/2009.

(3) alamoudi, omar. *Biometrics*.- Available at: http://knol.google.com/k/omar-alamoudi/biometrics/1szreovl9owjx/3#.- Accessed at: 22/7/2009.

(4) Alge, Bradley J. and Hansen, S. Duane. (2007) *Information Privacy in Organizations*.- In: 21st Century Management: A Reference Handbook,.- Available at: http://sage-ereference.com/management/Article_n87.html.- Accessed at: 10/9/2009.

(5) Caldera-Serrano, Jorge (2008). Changes in the management of information in audio-visual archives following digitization: Current and future outlook.- *Journal of Librarianship and Information Science*, 40 (1).- pp. 13- 20.

(6) Earley, Mark. (2006). Are Biometrics the key to data security?.- *EContent*. 29 (7).- pp.38-42.

(7) Giesing, Ilse (Compiler).(2003). *Biometrics*.- University of Pretoria.- pp. 49-76.

(8) Grandy, John K. (2005). Biometrics. In: *Encyclopedia of Anthropology*.- Available at: http://sage-ereference.com/anthropology/Article_n116.html. Accessed at: 8/9/2009.

(9) Guruprasad, Gokul. *Biometrics and applications*.- Available at: http://knol.google.com/k/gokul-guruprasad/biometrics-and-applications/26uzst0ozey3j/4#.- Accessed at: 29/7/2009.

(10) M2SYS Technology(a). *Dispelling the Myths About Biometrics*.- Available at: http://knol.google.com/k/m2sys-technology/dispelling-the-myths-about-biometrics/j4tytpka6zfm/2#.- Accessed at: 2/8/2009.

(11) M2SYS Technology(b). *Biometric Dynamic Profiling Techniques*.- Available at: http://knol.google.com/k/m2sys-technology/biometric-dynamic-profiling-techniques/j4tytpka6zfm/3#.- Accessed at: 5/7/2009.

(12) M2SYS Technology(c). *What is Fingerprint Biometrics?*.- Available at: http://knol.google.com/k/m2sys-technology/what-is-fingerprint-biometrics/j4tytpka6zfm/4.- Accessed at: 5/7/2009.

(13) Maestre, Sandra and Nichols, Sean. *DNA BIOMETRICS*.- 12p.- Available at: danishbiometrics.files.wordpress.com/2009/08/nst.pdf. Accessed at: 15/8/2009.

(14) McRobbie, Michael. (2003). "*It Security*". In: Encyclopedia of Distributed Learning.- Available at: http://sage-ereference.com/distributedlearning/Article_n92.html.- Accessed at: 9 /9 2009.

(15) Muthukrishnan, arvind. Biometrics - *Finger print, Iris, Retina and Pupil Recognition*.- Available at: http://knol.google.com/k/arvind-muthukrishnan/biometrics-finger-print-iris-retina-and/3ktp6efifnl1p/7#.- Accessed at: 14/8/2009.

(16) National Science Technology Council (USA). (2006,a). *Biometrics history*.- 27p.- Available at: www.Biometics.gov/documents/biohistory.pdf.- Accessed at:22/7/2009.

(18) National Science Technology Council (USA). (2006, b). *Biometrics overview*.- 27p.- Available at: www.Biometics.gov/documents/biooverview.pdf.- Accessed at:22/7/2009.

(19) Podio, Fernando L. and Dunn, Jeffrey S.. *Biometric Authentication Technology: From the Movies to Your Desktop*.- 8p. .- Available at www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf.- Accessed at: 20/7/2009.

(20) Raab, Charles D. and Mason, David. (2003). Privacy, surveillance, trust and regulation.- *Information, Communication & Society*, 6 (1).- pp. 83–84.

(21) Rhodes, Keith A. *Information Security: Challenges in Using Biometrics*.- United States General Accounting Office.- 27 p.

وآخر دعوانا أن الحمد لله رب العالمين