برنامج مقترح بالقياسات الحيوية مُنتج بمعالجة الصورة الرقمية للتغلب على بعض التهديدات الامنية فى البنوك

الأستاذ الدكتور
محمد سامي راضى
أستاذ المحاسبة والمراجعة - جامعة طنطا
وعميد المعهد العالى للإدارة وتكنولوجيا المعلومات - بكفرالشيخ
عمرو إبراهيم عوض الشورى
مدرس الحاسب الالى ونظم المعلومات
المعهد العالى للادارة وتكنولوجيا المعلومات – بكفرالشيخ

A Proposed Biometrics Program Produced with Digital Image Processing to Overcome Some Security Threats in Banks

Prof. Dr Mohamed Samy Rady
Professor of Accounting and Auditing - Tanta University
And Dean of the Higher Institute of Management and Information Technology - Kafr al-Sheikh
Dr. Amr Ibrahim Awd Al-Shora
Lcturer of Computer Science and Information Systems
Higher Institute of Management and Information Technology - Kafr El-Sheikh

ملخص الدراسة

هدفت الدراسة الى انتاج برنامج منتُج بطريقة القياسات الحيوية باستخدام معالجة الصورة للتغلب على بعض التهديدات الامنية فى البنوك، كما هدفت الدراسة الميدانية الى الوقوف على المتغيرات التالية : تحديد الوضع الأمني الحالي في البنوك المصرية، معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء في البنوك، معرفة اهم عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء ، وكانت عينة الدراسة في بعض البنوك بمحافظتى كفرالشيخ والدقهلية ، وانتهج البحث الحالي

المنهج الوصفي التحليلي في عرض البحوث والمنهج التجريبى في انتاج البرنامج وكانت اهم نتائج الدراسة : أن النظام الحالي للحماية بالبنك يحقق الغرض المطلوب ولكن ليس بالشكل الكافى الذي يحقق طمأنينه وثقة لتلك العملاء ، أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها في حماية وتأمين الحسابات الخاصة بهم من قبل البنوك وبصمة العين هي اهم وسيلة في القياسات الحيوية ، تعتبر القياسات الحيوية غير قابلة للأستيلاء من قبل الغير وتكون غير قابلة للتغيير فى نظامها كما تتصف بالثبات ، بصمة العين من الوسائل الإلكترونية الأكثر دقة فى تحديد هوية الأشخاص نظراً لأن أنماط القزحية صعبة ومعقدة ومتفردة فى كل شخص ولا تتغير بمرور الزمن ولا تحتاج لملامسة الأجهزة بشكل مباشر، كما يمكن رؤيتها من بعد ولذا تعتبر هى الطريقة الأفضل للتعرف على الهوية ، واوصت الدراسة بتبنى استخدام بصمة العين في القياسات الحيوية ، كما يمكن زيادة امان القياسات الحيوية بعدة طرق من بينها: استخدام أكثر من نموذج للقياسات الحيوية وأكثر من طريقة وأكثر من صورة بالإضافة الى تشفير الصور المستخدمة في عملية المضاهاة ، تفعيل القياسات الحيوية فى مختلف المؤسسات للتحقق من الهوية وحماية نظم وآمن المعلومات ، إستخدام القياسات الحيوية مع التقنيات الأخرى مثل البطاقات الذكية فى البنوك ، تطوير البرامج الخاصة بمعالجة الصور لإستخدامها فى أمن المعلومات داخل البنوك ، تدريب وتأهيل العاملين داخل البنوك على البرامج الخاصة بالقياسات الحيوية لحماية وأمن المعلومات بما ينعكس إجاباً على مصلحة العمل.

الكلمات المفتاحية: القياسات الحيوية، معالجة الصورة الرقمية، التهديدات الأمنية.

Abstract:

The study aimed to develop a program produced in a biometrics method-using image processing to overcome some security threats in banks. The field study also aimed at identifying the following variables: determining the current security situation in Egyptian banks, knowing the importance of biometrics in

securing data for clients in banks, and identifying the most important elements of biometrics that help protect clients' data. The study sample was in some banks in the governorates of Kafrelsheikh and Mansoura. The current study adopted the descriptive-analytical method to discuss relevant research and the experimental method to develop the program. The most important results of the study were: The current data security system in the banks achieves the desired purpose, but not sufficiently, that achieves clients' comfort and confidence. Biometrics is one of the most important insurance methods that must be relied upon to protect and secure their accounts and the eyerprint is the most important method in biometrics. Biometrics are cannot be stolen and they have a stable system. Eyeprint is one of the most accurate digital means for identifying people, given that iris patterns are difficult, complex and unique in each person. Eyeprint does not change over time and does not need direct contact with devices. Eyeprint can be scanned from a distance and is, therefore, the best way to verify identity. The study recommended the adoption of the use of the eyeprint in biometrics. The security of biometrics can also be increased in several ways, among them: Using more than one biometric template, more than one method, and more than one image, in addition to encoding the images used in the matching process. Enabling biometrics in various organizations to verify identity and protect information systems and security, using biometrics

with other technologies such as smart cards, developing image-processing programs for use in information security, and training and qualifying bank clerks on biometrics programs for protecting and securing information to achieve business interest.

Key words: biometrics, digital image processing, security threats

مقدمة الدراسة:

أدى التقدم العلمي إلى ظهور أساليب مبتكرة وإستراتيجيات جديدة تحاول حل المشكلات والتي عاده تتم من خلال إنتاج البرامج المختلفة بالأساليب التكنولوجية الحديثة، ويشهد العالم بصفة عامة ومصر بصفة خاصة الآن نهضة علمية تكنولوجية كبيرة لمواكبة التطورات التكنولوجية فى شتى المجالات تهدف إلى سـرعة اللحاق بالركب المتقدم، ويصعب تحقيق ذلك إلا بإستيعاب مفاهيم العصر وأنماطه الجديدة ولهذا تتضح ضرورة الإعتماد على البيانات الرقمية والتكنولوجيا الحديثة.

كما تلجأ المؤسسات فى الوقت الحالى لأنظمة حماية ورقابة للموظفين داخل المؤسسات للتأكد من الهوية بطريقة آلية وإستخدام تكنولوجيا المعلومات والإتصالات فى التحقق من الأفراد إستناداً إلى ملامحهم البدنية والسلوكية، حيث تعرف هذة الطريقة بالقياسات الحيوية ويوجد للعنصر البشرى العديد من هذة القياسات مثل بصمة الأصابع، بصمة الكف، بصمة الوجه، بصمة العين، بصمة الأذن، بصمة الحمض النووى وغيرها من البصمات (زين العابدين & الملحانى، ٢٠١٣)

وتعتبر القياسات الحيوية أحد الفروع المتميزة في مجال معالجة الصور والذكاء الأصطناعي، وقد حظي هذا المجال بإهتمام كبير من العديد من الباحثين، وتم إقتراح العديد من النظريات والأدوات في هذا المجال، حيث يهدف هذا المجال إلى إيجاد وتطوير تقنيات للتعرف على نمط أو شكل معين (Abod, 1998)

كما أن تقنية القياسات الحيوية أصبحت من الوسائل الأساسية واسعة النطاق ذوي الحماية العالية المستوى فى التحقق من الشخصية وتحديد هوية الأشخاص، فكلما زادت عمليات النصب والإحتيال والإختراقات الأمنية، زادت الحاجة إلى درجة عالية من الأمان

فى التحقق من الشخصية وتحديد الهوية، ولذلك فان الحلول المستندة إلى القياسات الحيوية قادرة على توفير السرية والخصوصية للبيانات الشخصية (زكى، ٢٠١٣)

وأصبح علم القياسات الحيوية جزءاً قوياً من أجزاء علوم آمن المعلومات، وتعتبر تقنية القياسات الحيوية هى طريقة آلية للتعرف على الشخصية بناءاً على الخواص الفسيولوجية للجسم البشرى والتى يتم قراءتها وتخزينها فى نظام الحاسب الألى، وتعتبر القياسات الحيوية للعنصر البشرى من أكثر الطرق أماناً وإعتماداً وإستخداماً فى التحقق من الشخصية (الحاج & زين العابدين، ٢٠١٣)

ولقد استطاع التقدم العلمى تمييز تعابير الوجة لكل شخص عن الأخر وإستخدامها فى تقنية الصورة والتى لاقت فى النهاية إهتماماً واسعاً فى شتى المجالات والمؤسسات الحكومية والخاصة، ثم تطور ابعد من ذلك وصولاً الى " قزحية العين " والجدير بالذكر ان العالم دوغمان من جامعة كمبردج البريطانية قام باجراء العديد من العمليات للتعرف على صفات القزحية فلم يتوصل إلى قزحيتين متطابقتين حتى في الشخص نفسه أو في التوائم المتشابهة الا ان الأمر تقدم الى ابعد من ذلك الا وهو عدم وجود تشابهة بين قزحية العين اليمنى عن اليسرى لنفس الشخص ، لذا تعتبر بصمة قزحية العين فى الوقت الحاضر أهم الطرق وافضلها على الإطلاق للتأكد من هوية الأشخاص (التمامى ، ٢٠١٨).

ومما سبق يتضح أن تقنية القياسات الحيوية لها دوراً مهماً فى العصر الحالى المعروف بعصر المعلومات كما أن لها دوراً فعال فى نجاح أى مؤسسة بغض النظر عن نشاطها، لحماية ممتلكاتها وأصولها الفكرية وغيرها من الكيانات التى يمكن إساءة إستخدامها، وذلك عن طريق أمن المعلومات المعرضة لقرصنة الشبكات، وكذلك الحاجة إلى التحقق من الأشخاص الذين يصلون إلى تلك المعلومات لضمان عدم التغيير والحذف أو التلاعب فيها، لذا فإن إدارة قواعد البيانات فى حاجة إلى وجود تقنيه فعالة مثل تقنية القياسات الحيوية.

مشكلة الدراسة:

يعتبر أمن المعلومات من القضايا الهامة فى البنوك، ومع زيادة الأفراد العاملين

فى القطاع المصرفي وزيادة الأرباح التى تحققها فرض عليها دوراً هاماً على المؤسسات للحفاظ على أمن وسرية المعلومات الخاصة بالعملاء ، ولكي تستمر البنوك فى القيام بهذا الدور يجب عليها المحافظة على قدرتها التنافسية ، وتطلب الامر الإلتزام بالضوابط الرقابية لعمليات الصرف الإلكترونى والقواعد المنظمة للبنوك بشأن تقديم الخدمات ، ووضع رقابة فعالة على المخاطر المرتبطة بسرية وأمن المعلومات ، وتقليل الإفصاح عن البيانات الهامة للمسئولين ، وتغير إسلوب الدخول بإستمرار مثل تغير كلمة السر ، وأساليب مادية والكترونية متعددة (نبيل & آلبير، 2015)

ومع إنتشار ظاهرة البنوك الإلكترونية أثبت الواقع أن الجرائم البنكية قد يقوم بها بعض موظفى البنوك المستخدمين لكلمة المرور الخاصة بالنظام لدى البنك، أو بعض العملاء أو ممن إستطاع بطريقة أو بأخرى الحصول على كلمة المرور الامر الذي أدى الى فشل أساليب الحماية المستخدمة فى مواجهتها، ويتم تحميل الأشخاص المشتبه بهم المسئولية الجنائية عن أفعالهم (ابوالعز، 2010)

ومن خلال إستخدام أحد الباحثين لرقم الفيزا الكارت الخاصة به وقيامة بشراء بعض الأشياء من الانترنت الا أنه بعد فترة لاحظ وجود رسائل من الحساب الخاص بة تفيد أنة تم خصم مبالغ مالية وباستطلاع الأمر بالبنك تبين أحد الباحثين أنة تمت عملية قرصنة على حسابة وتم تخمين رقم الكارت وهذا الامر هو ما يعرف بإختراق الأنظمة من قبل العملاء او الموظفين بغرض السرقة أو التعرف على الهوية.

من هنا جاءت فكرة البحث وبعد القراءة والإطلاع على الدراسات السابقة إستنتج الباحث أن الرقم السرى للكارت مهما كان حجمة إلا أنة يمكن تخمينة عن طريق برامج التباديل والتوافيق وأن جميع الدراسات أوصت بتبنى وسائل وطرق فى تامين البيانات آمنة لمسايرة التطورات والتقنيات الحديثة فى برامج الكراكرز ، والنظام الأمنى فى معظم البنوك يمتلك العديد من الطرق لتحقيق الطمانينة والمصداقية الا ان هذة الطرق لا تحقق المطلوب فى ظل ثورة علمية وتكنولوجية كبيرة ، من هنا جاءت فكرة إستخدام قزحية العين فى تأمين البنوك كحل أمنى بدلا من كلمات المرور لا يمكن اختراقة وبناء رؤية واستراتيجية حديثة لحل مشكلات التقنيات الأخرى غير آمنة.

ونتيجة لما سبق لابد أن تضع البنوك سياسات وإستراتيجيات واضحة، لضبط الرقابة اللازمة لحماية العمليات البنكية من الإنتهاكات الأمنية، ومنع أى أطراف داخلية أو خارجية، من الوصول إلى قواعد البيانات الخاصة بالخدمات الإلكترونية، وتتحدد مشكلة الدراسة فى محاولة الإجابة عن التساؤل الرئيسي التالي: -

- **ما تأثير برنامج منتج بطريقة القياسات الحيوية بإستخدام معالجة الصورة الرقمية للتغلب على بعض التهديدات الأمنية فى البنوك؟**

أهداف الدراسة:

- تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.
- معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.
- معرفة عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.
- تقديم برنامج مُنتج بطريقة القياسات الحيوية بإستخدام معالجة الصورة للتغلب على بعض التهديدات الأمنية فى البنوك.
- تسليط الضوء على التهديدات الأمنية المختلفة فى البنوك المصرية.
- حماية الخدمات البنكية والإستجابة لسرعة معالجة التهديدات الأمنية للعملاء.
- تقديم مقترحات لمواجهة التهديدات الأمنية للعملاء فى البنوك بإستخدام معالجة الصور.
- إستخدام قزحية العين في المساعدة على التعرف على الأشخاص بدقة بشكل لا يمكن إختراقة.
- تطوير مفهوم الأمن والحماية للبنوك فى ضوء التطورات والتقنيات الحديثة.
- طمانة المستخدمين للحسابات البنكية فى جميع أنحاء العالم.

أهمية البحث:

قد تعود أهمية هذة الدراسة الى ما يلي: -

- تفيد هذة الدراسة في التوصل إلى مواصفات فنية خاصة بتصميم وإنتاج برامج معالجة الصورة الرقمية من خلال أحد وسائل القياسات الحيوية.

- الوصول الى أفضل الأساليب الحديثة المستخدمة فى إنتاج برامج معالجة الصورة الرقمية باستخدام القياسات الحيوية.
- إرتباط مجال الدراسة الحالية بمجال القياسات الحيوية ومعالجة الصورة الرقمية وهو مجالان يتطلبان مزيد من الدراسات الخاصة بمعايير تصميم وإنتاج هذه البرامج لتوفير قاعدة تنظيمية تستند عليها أسس الإنتاج وذلك للإسهام فى تحسين هذه البرامج وزيادة فعاليتها.
- إدارة السياسات الأمنية وتوفير الضوابط والمتابعة المستمرة فى النظم الأمنية لضمان فاعلية تأمين الخدمات المصرفية.
- إتخاذ الإجراءات اللازمة لحماية العمليات البنكية من أى تهديدات توجه إليهم بإستخدام القياسات الحيوية ومعالجة الصور.
- محاولة إبراز الوسائل اللازمة لمواجهة التهديدات الأمنية لدى العملاء فى البنوك المصرية.
- نشر الثقافة الأمنية على كافة مستويات البنوك لضمان فاعلية تأمين الخدمات المصرفية.
- تقييم متطلبات الحماية اللازمة لأمن المعلومات، ونظم المعلومات فى ظل وسائل التخزين الآلية فى البنوك.

منهج البحث:

يتبع البحث الحالي المنهج الوصفي التحليلي في عرض البحوث ودراستها وتحليلها واستخلاص بنود الاستبيان ومن ثم تحليل النتائج والتوصل الى الاجابة على نتائج الدراسة، كما يتبع المنهج التجريبى في انتاج البرنامج.

مصطلحات الدراسة:

القياسات الحيوية:

تعرف القياسات الحيوية بأنها تقنية تحديد هوية الأفراد من خلال الخصائص البيولوجية الموجودة فى الجسد مثل بصمة الأصابع وقزحية العين وشبكيتها، والصوت، والتوقيع لتمييز شخص ما عن بقية الناس (Raab & Mason ,2003)،

وعرفها (عبد العزيز، ٢٠٠٧) بأنها أساليب آلية يمكن من خلالها التعرف على الأشخاص بناءاً على خصائص فسيولوجية وسلوكية يمكن إستخدامها فى الأنظمة الأمنية للمساعدة على حماية الأشياء المهمة.

معالجة الصورة:

تمثيل الصورة ثنائية الأبعاد على الحاسب بواسطة (1 , 0) تتكون الصورة من مجموعة من البكسلات وتتكون الصورة من مجموعة من الصفوف والأعمدة، كلما زاد عدد البكسلات في الصورة كلما كانت الصورة أوضح (Solomon & Breckon, 2010)

مفهوم أمن المعلومات:

يري (Whitman & Mattod ,2011) أن أمن المعلومات هو الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل الحفظ والمعالجة، ذلك عبر التطبيق الفعلى للسياسات الأمنية من خلال التدريب والتعليم، ويُعرف أمن المعلومات بأنه العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التى تهددها (خير، ٢٠٠٩)

التهديدات التى تواجه البنوك:

ويقصد بالتهديد هو كل تصرف يمكن أن يؤثر سلبياً على عناصر الأمن المصرفى داخل البنوك (فيلا & شليل، ٢٠١٨)

ويرى الباحثين انة يوجد الكثير من المخاطر المصاحبة لإستخدام التكنولوجيا على الرغم مما تحققه التكنولوجيا المصرفية من مزايا متعددة فى القطاع المصرفى وتشمل هذه المخاطر مايلى: أخطاء ناتجة عن عدم المعرفة أو السهو، خيانة بعض العاملين، تخمين رقم الحساب لاى مستخدم بالبرامج التكنولوجية الحديثة.

خطة الدراسة أو تنظيم الدراسة:

بعد استعراض الإطار العام للدراسة فان ما تبقى من البحث يمكن تقسيمة على النحو التالى:

١-الدراسات السابقة وتحديد الفجوة البحثية.

أولاً: دراسات تتعلق بالقياسات الحيوية.

ثانيا: دراسات تتعلق بمعالجة الصورة.

ثالثاً: دراسات تتعلق بأمن المعلومات بالبنوك.

رابعا: التعليق على الدراسات السابقة والفجوة البحثية.

٢-الإطار النظرى:

يشتمل الإطار النظرى لهذة الدراسة على ثلاث محاور أساسية تتمثل في الاتى:

أولاً: القياسات الحيوية.

ثانيا: معالجة الصورة.

ثالثا: أنواع التهديدات على النظم داخل البنوك.

٣-الدراسة الميدانية.

٤-تنفيذ البرنامج.

٥-نتائج الدراسة.

٦-التوصيات

٧-مقترحات لابحاث مستقبلية.

١-

٢- الدراسات السابقة وتحديد الفجوة البحثية:

تم تقسيم الدراسات السابقة إلى ثلاث مجموعات المجموعة الأولى دراسات تتعلق بالقياسات الحيوية، المجموعة الثانية دراسات تتعلق بمعالجة الصورة والمجموعة الثالثة دراسات تتعلق بأمن المعلومات فى البنوك.

أولاً: دراسات تتعلق بالقياسات الحيوية:

- **دراسة (احمد ،٢٠١٠)**

هدفت الدراسة إلى معرفة إمكانية إستخدام القياسات الحيوية فى أمن المعلومات وحددت الدراسة المعايير التى يجب اتباعها عند استخدام القياسات الحيوية، وتوصلت الدراسة الى إمكانية تقسيم القياسات الحيوية إلى قسمين الأول يتعلق

بالخصائص الجسدية والثانى يتعلق بالخصائص السلوكية وأكدت الدراسة على أهمية القياسات الحيوية والتى من الممكن أن توفر درجة عالية من الأمان فى أمن المعلومات لا تتوفر فى الطرق الأخرى.

- **دراسة (سليمان ،٢٠١١)**

هدفت الدراسة إلى بناء نظام حاسب ذكي لتمييز قزحية العين لتحديد كفاءة القزحية وتم إستخدام قاعدة بيانات تشتمل على صورة رقمية للعين ذات التدرج الرمادى، وتكونت العينة من ٤٢ عينة لقزحيات عيون أشخاص مختلفيين، وتوصلت الدراسة الى محاكاة الشبكة العصبية الإصطناعية ايلمان، والتى تمتلك ذاكرة ديناميكية مستخدمة لإتخاز القرارات فى تمييز القزحية.

- **دراسة (ذكي، ٢٠١٢)**

هدفت الدراسة إلى استخدام بصمة العين للتعرف على الأشخاص عن طريق صورة القزحية وتطبيق برنامج Matlab لمطابقة صور بصمة العين للأشخاص مع الصور المخزنة داخل قاعدة البيانات، وتوصلت الدراسة إلى أن ثورة تقنيات الإتصالات الرقمية ألقت مزيداً من الضغوط على العديد من مؤسسات القطاع العام لتحويل عملياتها إلى عالم الأعمال الإلكترونية فيما يعرف بالحكومة الالكترونية، وذلك لتسهيل العمليات الإدارية اليومية للقطاعات الحكومية.

- **دراسة (المطيرى واخرون، ٢٠١٢)**

هدفت الدراسة إلى التعرف على دور إستخدام البصمة العشرية مقارنة بقزحية العين فى مطار الملك خالد بالسعودية، وتكون مجتمع العينة من الضباط والأفراد والعامليين فى الجوازات وشرطة المطار وعددهم الإجمالي (٢٢٤) ضابط وفرد، وتم إختيار عينة عشوائية بإستخدام المعادلات الإحصائية بلغ حجمها (١٥١) استخدمت الدراسة المنهج الوصفي التحليلي، وتوصلت الدراسة الى وجود أوجة الشبه بين تقنية البصمة العشرية وتقنية الكشف عن قزحية العين.

- **دراسة (عبد الرحيم & جاه النبى، ٢٠١٧)**

هدفت الدراسة إلى التعرف على أهمية البصمات فى الأدلة الميدانية والجنائية فى

التعرف على مجهولى الهوية، كما هدفت الى إلقاء الضوء على تجارب بعض الدول العربية بإستخدام نظام (AFIS) (وهو نظام للتعرف على البصمات)، وتوصلت الدراسة إلى عدة نتائج منها: بصمة الأصابع دليلاً قاطعاً على تحدد هوية الأشخاص، الدقة والسرعة لنظام (AFIS) فى التعرف على مجهولى الهوية، واوصت الدراسة بضرورة التطويره فى جميع المجالات التى تستخدم قواعد البيانات تقليلاً للوقت والجهد.

ثانيا: دراسات تتعلق بمعالجة الصورة:

- **دراسة (عمار & السمان، ٢٠١١)**

هدفت الدراسة إلى تطوير طريقة لتنفيذ الكشف الآلي بمساعدة الحاسب عن المناطق المريبة في الكبد، تتألف الطريقة من مرحلتين، المرحلة الأولى إستخدام تقنية ترقيم المركبات المتصلة، وتقنيات العمليات المورفولوحية لكي يتم الإستخلاص الآلي لمنطقة الكبد في الصورة المقطعية المحوسبة لمنطقة البطن، والمرحلة الثانية إستخلاص المناطق المريبة من منطقة الكبد باستخدام خوارزمية تجميع البيانات، وتوصلت الدراسة إلى أن الطريقة المطورة أعطت نتائج واعدة، حيث تم كشف وإستخلاص كل المناطق المريبة آلياً.

- **دراسة (قريطم & ساعى، ٢٠١٣)**

هدفت الدراسة إلى إنتاج برمجية مقترحة لتحديد حجم اورام الدماغ ومكانها فى صورة الرنيين المغناطيسى من خلال تقنيات معالجة الصورة ، وفى سبيل تحقيق ذلك قامت الدراسة بمرحلتين : المرحلة الأولى تعتمد على المعالجة الأولية لتلك الصور بهدف تحسين جودتها ، في المرحلة الثانية تم تطبيق تقانة قطع الرسم البياني Graph-cutمن أجل إستخلاص منطقة الدماغ من صورة الرنين المغناطيسي، وتطبيق تقنية مستجمعات المياه Watershed لإستخلاص منطقة الورم من الصورة، وأخيراً تم حساب حجم الورم وتجميع الشرائح المحورية للدماغ ، وتوصلت الدراسة عند تطبيق البرنامج المقترح الى ان معدل نجاح النظام في كشف الأورام الدماغية كان بنسبة ٩٧.% .

- **دراسة (حنا & كيوان ٢٠١٥)**

هدفت الدراسة إلى إنتاج خوارزمية لتصميم نظام يقوم بتصنيف التعابير القياسية السبعة لوجه الإنسان (الخوف – الإشمئزاز – الحزن – التفاجؤ – الغضب – السعادة – التعبير الطبيعي) بإستخدام بعض تقنيات معالجة الصورة، وذلك بإستخدام لغة البرمجة Matlab ، وفى سبيل تحقيق ذلك قامت الدراسة بالمراحل التالية (مرحلة تجميع الصور، مرحلة المعالجة المسبقة للصورة، مرحلة إستخلاص السمات، مرحلة تدريب الشبكة العصبونية، مرحلة التصنيف والإختبار) وتوصلت الدراسة إلى تحقيق أعلى نسبة تصنيف عند تعبير الغضب حيث وصلت ١٠٠%، بينما أدنى نسبة تصنيف كانت عند تعبير الحزن وهي ٥٠.% .

- **دراسة عيد (٢٠١٦)**

هدفت الدراسة إلى تطوير طريقة جديدة لإستخراج وتحديد خصائص وسمات الأورام السرطانية في صور الرنين المغناطيسي للثدي بالإعتماد على خوارزميات العنقدة ومعالجة الصور الرقمية ، وتم في البداية الإعتماد على إحدى خوارزميات العنقدة في تجزئة الصورة وتجميع عناصرها وفق قيم المستويات الرمادية، وإستخدمت قاعدة بيانات مكونة من ٩٦ صورة من صور الرنين المغناطيسي للثدي وتم تطبيق الطريقة المقترحة عليها باستخدام برنامج الماتلاب Matlab ، وتوصلت الدراسة الى فعالية معالجة الصورة الرقمية فى إستخراج المناطق الورمية من هذه الصور ومقارنتها مع رأي الأطباء.

- **دراسة حاتم (٢٠١٩)**

هدفت الدراسة إلى إستخدام معالجة الصورة الرقمية فى عينات صور فوق صوتية وذلك لتحديد منطقة رأس الفخد عند اوراك الأطفال، وفى سبيل ذلك قامت الدراسة بمرحلتين المرحلة الأولى تتضمن عمليات معالجة إبتدائية للصور للوصول إلى تقطيع للصورة، وفي المرحلة الثانية تستخدم طريقة تحويل هاف التكراري العشوائي للتعرف على كائن منطقة الفخذ، وتوصلت الدراسة الى فعالية تقنيات معالجة الصور في تحديد منطقة رأس الفخذ في الصور فوق الصوتية مما يمهد

لإمكانية بناء نظام التشخيص المؤمن لحالة العسر التطوري للورك عند الأطفال.

ثالثاً: دراسات تتعلق بأمن المعلومات بالبنوك:

- **دراسة (قاسم & ردايدة، ٢٠١٠)**

هدفت الدراسة إلى معرفة مدى إعتماد البنوك الإردنية على إجراءات أمن المعلومات، من خلال التعرف على أهمية الأمن المادى لوسائط التخزين، وأمن المستخدمين للبيانات والنظم الألية، والبرمجيات والأجهزة والمعدات، وعمليات تخزين المعلومات وتبادلها، وتوصلت الدراسة إلى عدة نتائج منها استخدام البنوك الأردنية الأمن المادى سواء بإستخدام الهاتف، الخزائن المحمية لحفظ أقراص البيانات ووسائط التخزين المختلفة، كما أن هناك إهتمام كبير بالأمن البرمجي في البنوك الأردنية وهدفه تخزين البيانات.

- **دراسة (Altamimi ,2011)**

هدفت الدراسة إلى تقييم وتحديد مخاطر أمن المعلومات التى لها تأثير على الخدمات المصرفية عبر الإنترنت لعينة مكونه من ١٢ بنك بالمملكة العربية السعوديه، وتوصلت الدراسة إلى عدة نتائج منها وجود العديد من المخاطر المرتبطة بالخدمات المصرفية عبر الإنترنت، كما أن البنوك تركز على المخاطر الخارجية أكثر من الداخلية، وأوصت الدراسة بضرورة تطوير الوسائل التى تساعد على القضاء على التهديدات الخاصة بأمن المعلومات.

- **دراسة (Kumar &Puri ,2012)**

هدفت الدراسة إلى توفير حماية أفضل للمعلومات والبيانات وللنظام كما تناولت الدراسة إطار عام لتقييم سياسة أمن المعلومات ، وأوضحت الدراسة مجموعة من التهديدات التى تواجه المعلومات والإستراتجيات المتاحة من خلال إدارة المخاطر ، كما تم تحليل سياسات أمن المعلومات لتقييم نموذج جديد لأمن المعلومات من خلال مايلى : التحكم في الوصول إلى الخدمات ، إدارة أمن النظام ، التشفير ، وذلك لتحقيق المرونه والأمان ، والسرية ، وتوصلت الدراسة إلى إمكانية تطبيق سياسات أمن المعلومات التى تحتوى على الأنشطة السابقة لحماية المعلومات من المخاطر التى تواجهها .

- **دراسة (عوض الله &عثمان، ٢٠١٣)**

هدفت الدراسة إلى التعرف على قوة فاعلية الرقم السرى ، وقوة فاعلية التشفير بإستخدام خوارزميات التشفير ، وتوصلت الدراسة إلى عدة نتائج ومنها أنه يوجد توافر للجانب الأمنى في شبكة الصرف الآلى من خلال ثلاثة مراحل الأولى إجراء تعديلات على الرقم السرى ، المرحلة الثانية بدلاً عن التشفير المتماثل على مستوى البيانات المرسلة عبر الشبكة ، المرحلة الثالثة ، تطبيق RSA إستخدام تقنية التشفير اللامتماثل بإستخدام خوارزمية الوسائل الأمنية الخاصة بتأمين قواعد البيانات الموجودة على البنوك ، وأوصت الدراسة بإستخدام خوارزميات التشفير التى تعتبر أسرع لقوتها وأمانتها .

- **دراسة (نبيل & البير، ٢٠١٥)**

هدفت الدراسة إلى تقييم تأثير أمن المعلومات على البنوك المصرية فى عام ٢٠١٣ / ٢٠١٤، وتقييم مدى إستفادة البنوك من تطبيق معايير وإجراءات أمن المعلومات، وتوصلت الدراسة إلى عدة نتائج منها تتأثر ربحية البنوك بأمن المعلومات عن طريق وضع إطار لنظام إدارة أمن المعلومات، وتقييم مخاطر أمن المعلومات، وأوصت الدراسة بدراسة ومواكبة أحدث البرامج لتأمين بيانات العملاء داخل البنوك.

- **دراسة (الشمالى، ٢٠١٧)**

هدفت الدراسة إلى تعريف أمن المعلومات، وتسليط الضوء على كيفية تطبيق إجراءات أمن المعلومات فى البنوك العامة بالأردن، دراسة أثر أمن المعلومات على أداء البنوك العامة فى الأردن، مساعدة الإدارة العليا للبنوك لتحقيق كفاءتها عن طريق أمن وسرية المعلومات بها، وتوصلت الدراسة إلى عدة نتائج منها أهتمام عدد من البنوك بزيادة أمن وسرية المعلومات لديها وكان ذلك لثلاثة أسباب أولها الحماية المادية، وثانياً حماية العملاء، وثالثاً حماية البرامج وأوصت الدراسة بضرورة زيادة الإنفاق على برامج أمن المعلومات.

رابعاً: التعليق على الدراسات السابقة والفجوة البحثية:

تم تقسيم الدراسات السابقة إلى ثلاث مجموعات المجموعة الأولى دراسات

تتعلق بالقياسات الحيوية ، المجموعة الثانية دراسات تتعلق بمعالجة الصورة وبصمة العين ، المجموعة الثالثة دراسات تتعلق بأمن المعلومات فى البنوك ، وبعد الإطلاع على **المجموعة الأولى** من الدراسات السابقة الخاصة بالقياسات الحيوية تبين أن القياسات الحيوية يمكن تقسيمها إلى قسمين ، القسم الأول يتعلق بالخصائص الجسدية ، أما القسم الثانى يتعلق بالخصائص السلوكية ، كما أن للقياسات الحيوية العديد من العناصر مثل بصمة الأصابع ، بصمة الوجه ، بصمة شبكية العين ، بصمة قزحية العين ، بصمة اليدين ، بصمة الصوت ، بصمة الحمض النووى وغيرها ، وتوصلت الدراسات أن لبصمة العين الدور الأكبر فى أمن المعلومات وتستخدم فى كثير من المؤسسات لدقتها وصعوبة تزويرها وهذا ما يميزها عن الطرق المختلفة الأخرى ، ويوجد نوعين لبصمة العين وهما بصمة شبكية العين وبصمة قزحية العين ، وتبين أن للقياسات الحيوية تقنية للأمن وحماية المعلومات عن طريق التحقق من الأشخاص من خلال قراءتها وتخزينها فى نظام المعلومات ، كما توصلت الدراسات إلى أن القطاعات الحكومية إتجهت إلى إستخدام القياسات الحيوية نتيجة لتزايد الضغوط على العديد من المؤسسات بالقطاع العام لكى تقوم بتحويل العمليات إلى عالم الأعمال الإلكترونية ، وذلك لتسهيل العمليات الإدارية اليومية للقطاعات الحكومية والتى يمكن من خلالها التعرف على الأشخاص

أما **المجموعة الثانية** فهى الدراسات المتعلقة بمعالجة الصور ، وتقوم معالجة الصور بمجموعة من المراحل وهى مرحلة تجميع الصور ، ومرحلة المعالجة المستقبلية للصورة ، مرحلة إستخلاص السمات، مرحلة تدريب الشبكة العصبونية ، مرحلة التصنيف والإختبار، وتستخدم معالجة الصور العديد من لغات الحاسب ومنها لغة الفيجوال بيسك ولغة الماتلاب ، وتوصلت الدراسات أن لمعالجة الصور فعالية فى الإستخدامات الطبية وغيرها من المجالات المختلفة ، أما **المجموعة الثالثة** دراسات تتعلق بأمن المعلومات داخل البنوك ، وأكدت الدراسات إلى حاجة المنظمات بأخذ الإحتياطات اللازمه لمواجهة خطر حماية معلوماتها الثمينة فتقوم بالبحث عن طرق وأسالبيب فعالة لأمن المعلومات ألا وهى البرامج ، وتتعدد أنوع الأمن بالنسبة لكثير من

البنوك مثل أمن المكان و أمن الأنظمة الإلكترونية ، وأمن الشبكات وأمن الأفراد داخل المؤسسات وتدريبهم على البرامج للمحافظة على المعلومات الخاصة بالأفراد و الحسابات والأرصدة الخاصة بهم ، وتوصلت الدراسات إلى أن على الرغم من التقدم لأساليب أمن المعلومات داخل البنوك إلا أن هناك بعض التهديدات الموجودة داخل البنوك وتكون متطورة بشكل سريع ، ومن الصعب التخلص منها بالطرق التقليدية ، ومن أكثر هذه التهديدات خطورة هى التهديدات الداخلية فى البنوك ، وحماية المكونات المادية والبرمجية و أخذ الحيطة والحزر فى التعامل مع الأشخاص وهذا لضمان إستمرار المؤسسة ، لا التهديدات الخارجية لحماية وأمن المكان من أى هجوم خارجى.

كما أوصت الدراسات بضرورة الإهتمام بأمن المعلومات وتطويرة المستمر نظراً للتطورات الهائلة فى التهديدات والمخاطر التى تواجه العملاء داخل البنوك ، وبعد الإطلاع على هذه المجموعات تبين أن القياسات الحيوية من أهم التقنيات التى لها دوراً فعال فى مختلف الأنشطة فى حماية وأمن المعلومات وتحديد هوية الأشخاص الذين يتعاملون مع الأنظمة المختلفة ، لضمان عدم التلاعب والحذف و التغيير فى المعلومات بألانظمة ، لذلك فإن إدارة قواعد البيانات لدى البنوك فى حاجة إلى وجود تقنية دقيقة وفعالة مثل تقنية القياسات الحيوية للحفاظ على ممتلكات الأشخاص داخل البنوك ، ومن هنا جاءت الفجوة البحثية والتى تتمثل فى فعالية برنامج مقترح منتج بطريقة القياسات الحيوية بإستخدام معالجة الصور للتغلب على بعض التهديدات الأمنية فى البنوك .

٢- الإطار النظرى

يشتمل الإطار النظرى لهذة الدراسة على ثلاث محاور أساسية تتمثل في الاتى:

أولاً: القياسات الحيوية:

تعرف القياسات الحيوية بأنها تقنية لحماية وآمن المعلومات عن طريق التحقق من الأشخاص بناءاً على الخصائص الفسيولوجية للجسم البشرى من خلال قراءتها وتخزينها فى النظام، وللقياسات الحيوية مجموعة من العناصر تتمثل في الاتى: -

١-بصمة الأصابع:

وتعرف بصمة الأصابع بأنها عبارة عن نتوؤات بارزة فى بشرة جلد الأصابع

تجاورها منخفضات، تجعل عملية الإمساك بالأشياء أكثر سهولة وتختلف أشكال هذه النتوءات من شخص لأخر ولا يمكن أن تتطابق فى شخصين فى العالم (احمد، ٢٠١٠)

إستخدامات بصمة الأصابع:

تعتبر بصمة الأصابع ذات جدوى وفعالية فى أمن البيانات والمعلومات، وإستخدام هذا النظام بسيط حيث يتم تسجيل البصمة، ثم يتم تصنيف نماذج هذه البصمات وفقاً لأصابع اليد المأخوذ منها البصمات، وبإستخدام بطاقة بصمة الأصبع تؤخذ بعض النقاط الفريدة لتحديد بصمة الشخص، وتعرف بأنها علامات لبصمات الأصبع، ويمكن إستخدامها إذا تم إستخدام نظام إلكترونى للتحقق من البصمة، وتوجد ١٢٠ نقطة لتمييز بصمات الأصابع يمكن إدخالها للحاسب الألى ومطابقتها بالبصمات المخزنه داخل الحاسب الألى فى قاعدة البيانات (Early , 2006)

مميزات بصمة الأصبع:

ويرى (Muthukrishnan,2009) أن لبصمة الأصبع عدة مزايا كالتالى:

- معروفة لدى الأشخاص.
- سهلة الإستخدام بالنسبة للحاسب الألى.
- تعمل بشكل جيد.
- أقل ضرراً لدى المستخدم.

عيوب بصمة الأصبع:

وأوضح (أحمد، ٢٠١٠) عيوب تقنية الأصبع وهي ما يلي:

- التزوير: يمكن تزوير شكل بصمة الأصبع، ولكن يمكن للأجهزة إكتشاف هذا التزوير عن طريق التعرف على الجلد الميت من الحي لبصمة الشخص، وفحص تدفق الدم داخل الجلد أو انعكاسه.
- القبول الزائف: يحدث هذا القبول عندما يحدد نظام المعلومات خطأ المستخدم كمستخدم مختلف فى قاعدة البيانات، ويحدث عندما يقوم مستخدم لم يسبق تسجيله داخل النظام يتلقى إذن من التحقق من هويته.
- الرفض الزائف: ويحدث عند فشل النظام فى التعرف على مستخدم مسجل،

ويحدث إذا حدث إنجراف فى البصمة عند التسجيل داخل قاعدة البيانات، ولحل هذه المشكلة، يجب أن تكون نظم التحقق من الهوية مبرمجة.

- الإكراه: وتتم عن طريق إكراه مستخدم حقيقى للنظام للدخول من قبل شخص مهاجم، ويتم التغلب على هذه المشكلة عن طريق تسجيل بصمة إصبع سبابة اليد اليمنى كبصمة معتمدة، وتسجيل بصمة إصبع سبابة اليد اليسرى كبصمة إكراه، وعن طريق هذا يتم إعطاء إشارة للنظام أن هذا الشخص تم دخوله على النظام بفعل تهديد وإكراه.

٢- بصمة الشفاة:

تختلف بصمة الشفاه من شخص لأخر ولا يتفق إثنان فى العالم متفقين فى هذه البصمة وتؤخذ هذه البصمة بواسطة أجهزة يوجد بها حبر غير مرئى، ويتم الضغط على الجهاز بواسطة شفتى الشخص، ويتم وضع ورقة من النوع الحساس، فيتم طبع عليه بصمة الشفتين، وبلغت دقة هذه البصمة لدرجة إمكانية أخذ هذه البصمة من عقب السجارة، وتم إثبات أن هذه البصمة لا تتغير مع تقدم السن وإتضح أن بصمة الشفاه عند التوائم تكون دائماً قريبة التشابه إلى أقصى درجة، وتكون الخواص الموروثه من الأب والأم (عبد الفتاح، ٢٠١٤)

٣- بصمة الأذن:

ويقصد بها بصمة صوان الأذن، ويتم إلتقاط هذه البصمة بأساليب وطرق لا يفهمها إلا خبراء البصمات، وبعد إلتقاتها يتم مطابقتها مع بصمات صوان الأذن للشخص، ويمكن إستخدام هذه التقنية لحماية الأنظمة خاصة أن المجرمون يستخدمون القفازات لكنهم يستخدمون الأذن فى التجسس قبل فتح الأبواب والنوافذ ولا يوجد أذنان متشابهان (عبد العالى، ٢٠١٥).

٤ – بصمة اليد:

تستخدم تقنية بصمة اليد منذ ٣٠ عاماً وتستخدم فى التحكم فى دخول الأماكن ويتم إستخدام مجموعة من القياسات ومنها العرض والطول، والمسافات بين الأصابع وعقلها، وطول الأصابع، وأشكال المفاصل، ويتم إستخدام كاميرا ضوئية وضوء يطلق من صمام ثنائى، لتسجيل صورة متعامدة وثنائية الأبعاد لظهر اليد والجوانب، وبعد ذلك ترقيم هذه

القياسات المأخوذة ومقارنتها بالبيانات المخزنة من قبل لصور اليد، ولكن يوجد العديد من العوامل البيئية والطبيعية تسبب إختلافات طفيفة مع تقدم العمر (Rhodes,2003)

ويري (Giesing,2003) أن لهذه التقنية بعض المميزات والعيوب كتالى:

المميزات:

- نظام سهل الإستخدام.
- لا يتأثر بحالة الجلد.
- يتم التحقق بهذه الطريقة من أكبر عدد من الأشخاص.

العيوب:

- تحتاج إلى وجود الشخص نفسه فى المكان.
- تحتاج جهاز حجمه كبير.

٥ ـ بصمة الصوت:

هذه التقنية تعتمد على الخصائص المميزة مثل نغمة الصوت، ونبرته وإيقاعه، وتجويف الفم والأنف الذي يتحكم فى نبرات الصوت وهذا ما تعتمد عليه نظم التحقق من الأشخاص، ويتم الوصول إلى المعلومات المخزنه فى الحاسب بوسائل طبيعية للإتصالات مثل الحديث، ويتم تطبيق هذه التقنية عن طريق إستخدام نظم IVR (Interactive Voice Response) ، ويتم الإعتماد فى هذا النظام على إستخدام الهاتف للوصول إلى المعلومات الموجودة على الحاسب، وتعمل نظم IVR كحلقة وصل بين الأشخاص وقواعد البيانات من خلال إمداد المستخدمين بالمعلومات اللازمة(Nguyen ,2010)

٦ـ بصمة الحمض النووى:

تستخدم قياسات الحمض النووى DNA فى الحالات القضائية لتحديد مرتكبى الجرائم ويمكن إستخلاص الحمض النووى من الشعر أو العرق أو الإفرازات وأى سوائل جسدية أخرى، ويمكن إستخدام الحمض النووى فى تأمين شبكات المعلومات ويختلف عن القياسات الحيوية الأخرى فى عدة طرق (احمد، ٢٠١٠):

- يتطلب تحليل الحمض النووى وجود عينة مثل الدم أو الشعر.

- مضاهات الحمض النووى لا تستخدم القوالب أو إستخلاص الملامح ولكن تمثل مقارنة بين عينات حقيقية.
- لا يمكن مضاهاة الحمض النووى فى الوقت ذاته، ولا تتم جميع المراحل بشكل آلى، ومع ذلك فإن الحمض النووى عنصر من القياسات الحيوية التى تستخدم الخصائص الفسيولوجية للتحقق من الشخصية ومن أهم مزاياه أنه أكثر القياسات الحيوية دقة، لكنه من القياسات التى تأخذ أسابيع أو شهور فى معالجتها (احمد، ٢٠١٠).

٧ – بصمة الوجه:

يوجد بصمة أخرى ذات إستخدام واسع النطاق للقياسات الحيوية وهى بصمة الوجه عن طريق الصور ويستخدم هذا فى جميع أنحاء العالم مثل جوازات السفر الدولية ويعتمد هذا النظام على التعرف على هيكل الوجه ، فتوجد مسافات بين العين والأنف والفم مختلفة من شخص إلى أخر وفرصة تكرارها من شخص لأخر نادرة جداً ، وعند التعرف على بصمة الوجه ترسم خريطة لوجه الشخص وتظهر البيانات الأساسية عن محيط الوجه والمسافات بين مكونات الوجه ، ويتم البحث عن أخر صورة مماثلة ، كما توجد أكثر من ٨٠ نقطة لتحديد بنية الوجه ، وقد لا تستخدم النظم المختلفة هذه النقاط جميعاً ، ولكن تقوم بتحليل عدد صغير من النقط من خلال تحليل هذه المسافات (Caldera – serrana, 2008)

عيوب بصمة الوجه:

ويري (احمد، ٢٠١٠) أنه يوجد العديد من عيوب بصمة الوجه منها ما يلي:

- يمكن إجراء تغييرات جراحية بسهولة على الوجه.
- بصمة الوجه ليست أكثر دقة للتحقق من الشخصية بسبب التشابه الموجود فى هيكل الوجه وخاصة بين الأقارب والأخوات.
- وجود موانع تتعلق بكشف الوجه لأسباب دينية أو ثقافية.

٨ – بصمة العين:

تم إبتكار هذه البصمة من قبل إحدى الشركات الأمريكية لصناعة الأجهزة

الطبية ، كما أكدت الشركة أنه لا توجد عينان متشابهتان فى كل شئ ، وتؤخذ بصمة العين بواسطة عدسة الجهاز الذى يقوم بإلتقاط الصورة وعند الإشتباه فى شخص معين ، يتم الضغط على زر معين بالجهاز ، فتتم مقارنة صورته بالصورة المخزنة فى ذاكرة الجهاز، ولا يزيد وقت العملية عن ثانية ونصف ، وأكدت الدراسة عدم وجود حدقتين متشابهتين فى البشر حتى التوائم المتماثلة ، حيث أن حدقة العين اليمنى مختلفة عن اليسرى فى الشخص الواحد كما أن رسم حدقة العين ثابت مدى حياة الإنسان ، ويتكون هذا الرسم خلال ستة أشهر من ولادته ويثبت بعد سنه من العمر ، ويستمر فى الثبات حتى وفاة الشخص ، كما أن التعرف على بصمة العين للشخص يستغرق ثوان معدودة ، وتسجيل البصمة لأول مرة لا يزيد عن ثلاث دقائق ، ولا تؤثر النظارات الطبية والعدسات اللاصقة على عملية مسح البصمة (عبد الفتاح ، ٢٠١٤)

ويرى (christel et al , 2010) أنه يوجد نوعين لبصمة العين بصمة شبكية العين وبصمة قزحية العين:

أ – بصمة شبكية العين:

يتم أخذ هذه البصمة عن طريق تسليط شعاع من الضوء على قاع العين، وبهذا يتم تصوير خارطة الأوعية الدموية التى تخرج من العصب البصري إلى الشبكية، ويكون مسار الأوعية الدموية فى العين اليمنى مختلفة عن العين اليسرى، وينبغى أن يكون الشخص قريب جداً من جهاز مسح الشبكية، ويقوم بالتحديق مباشرة فى العدسات ويكون ساكناً أثناء مرور الضوء داخل العين، وأى حركة من العين تتطلب إعادة العملية من البداية (Daouk et al , 2012)

مميزات بصمة الشبكية:

وأوضح (ذكي، ٢٠١٢) أن هناك بعض المزايا للمسح الضوئى لبصمة شبكية العين كما يلي:

- عدم تأثرها بالعوامل البيئية.
- سهلة وسريعة الإستخدام.
- أمنة.

- تكلفتها منخفضة.
- يمكن ضغط ملف البيانات وبالتالى تقل مساحة الحفظ.
- أعلى دقة مقارنة بالسمات الحيوية المختلفة.

عيوب بصمة الشبكية

حدد (احمد، ٢٠١٠) بعض العيوب لبصمة الشبكية منها ما يلي:

- تلقى مقاومة شديدة من الأشخاص، لأنهم يخافون على أعينهم.
- توجد مخاوف من أن مصدر الضوء المستخدم قد يسبب ضرر للعين.
- تكلفة الأجهزة المستخدمة لمسح شبكة العين غالية الثمن.
- يمكن ان تتأثر شبكة العين بالعديد من الأمراض مثل المياه الزرقاء او البيضاء، وضغط الدم.
- صغر الشبكية داخل العين وصعوبة القياس يجعل من الصعب الحصول على صورة منها.

ب – بصمة قزحية العين

القزحية هى المنطقة الملونة فى العين وتقع خلف القرنية وتكون أمام العدسات، وتؤخذ البصمة عن طريق ضوء الأشعة تحت الحمراء غير المرئية، مما يعمل على إظهار تفاصيل أكثر غير مرئية للعين المجردة، ويتم إلتقاط صورة أبيض وإسود ذات درجة وضوح عالية للقزحية ثم يحدد هذا النظام حدود القزحية وينشئ نظام إحداثيات، ويتم تحديد مناطق التحليل فى النظام، وقد تم تطوير نظم بصمة قزحية العين كنظم متطورة عن نظم مسح الشبكية (زكى، ٢٠١٢)

مزايا بصمة قزحية العين (سواحل، ٢٠٠٩):

- دقة عالية مع سهولة فى الإستخدام.
- ثابته لا تتغير مدى حياة الشخص.
- يمكن إلتقاط الصورة بالنظر فقط إلى آلة التصوير على بعد ثلاثين سنتمتراً.
- التعرف على بصمة القزحية لا يستغرق أكثر من عدة ثوان.
- تسجيل البصمة لا يأخذ أكثر من ثلاث دقائق.

عيوب بصمة قزحية العين.

وهناك عدة عيوب لبصمة قزحية العين وهي:

- تكلفة شراء الأجهزة والتشغيل مرتفعة.
- إستخدام الأشعة تحت الحمراء قد يصيب العين ببعض الأمراض البصرية فى حالة التحقق أكتر من مرة فى اليوم.
- إذا تم مسح العين لشخص ميت جسدياً أو إكلينيكيا فإن العملية تتم بنجاح.
- يجب أن تكون جودة صورة القزحية مرتفعة حتى يقوم النظام بتحديد الشخص الصحيح.

فوائد إستخدام القياسات الحيوية:

يرى (Giesing,2003) و (أحمد، ٢٠١٠) أن هناك عدة فوائد للقياسات الحيوية على أمن المعلومات والبيانات منها ما يلي:

- توفير درجة أمان شبكات المعلومات لا توفرها الطرق الأخرى للتحقق من الشخصية.
- تتسم بالسرعة فى التحقق من الشخصية.
- عدم ضياعها، مما يعنى زيادة الأمن.
- غير قابلة للنسيان.
- غير قابلة للسرقة.
- موجودة دائماً مع الشخص فى أى وقت وأى مكان.
- عدم الحاجة إلى أرقام شخصية لتحديد الهوية.
- صعوبة التزوير.

ثانيا: معالجة الصورة

هي أحد فروع علوم الحاسب تهتم باجراء عمليات على الصور بهدف تحسينها طبقا لمعايير محددة او استخلاص بعض المعلومات منها Micki & (Tipton 2008)

١-المعالجة الرقمية للصورة:

الصورة الرقمية عبارة عن الآلف أو ملايين المربعات الصغيرة تسمى عناصر الصورة أو مايعرف بالبيكسل عندما يبدأ الحاسب برسم الصورة فإنه يقوم بتقسيم الشاشة أو الصفحة المطبوعة إلى شبكة من البيكسلات ثم يقوم بإستخدام القيم المخزنة للصورة الرقمية ليعطي لكل بيكسل لونة وسطوعة، وتسمى هذه الطريقة توضيع الخانات bit mapping وتسمى الصورة maps bit ، تعتمد جودة الصورة الرقمية على عدد البيكسل المكون لها فكلما إزداد عدد البيكسل كلما حصلنا على جودة أفضل إذا ماتم تكبير الصورة الرقمية إلى حد معين (يختلف من صورة لأخرى) نلاحظ ظهور تشوه معين ناتج عن كون الصورة مركبة من بيكسلات ، ويسمى هذا التشوة pixelization وكلما كان عدد البيكسلات كبيراً كلما تأخر ظهور هذا التشوه عند التكبير ، كما يحدد حجم الصورة بطريقتين إما بأبعادها بالبيكسل أو بعدد البيكسل المكون لها (المحمودى، ٢٠١٥)

كما يمكن تمييز الصورة الرقمية بانها صورة يسهل الوصول إليها، والتعامل معها ومعالجتها وتخزينها وتحميلها أو تنزيلها في الكمبيوتر أو على الإنترنت وبينما كان المصطلح يشير إلى معالجة الصورة عن طريق الماسح الضوئي وبرنامج الفوتوشوب، فقد تم التوسع في إستخدامه ليشير أيضاً إلى التقاط الصورة بإستخدام الكاميرات الرقمية، فضلاً عن معالجتها ببرامج معالجة الصورة، مروراً بإستخدام التقنيات الحديثة في حفظ وتنظيم الصورة وأرشفتها وإسترجاعها (شاكر عبد الحميد، ٢٠٠٥)

٢-التحولات الأساسية في انتاج الصورة الرقمية

يكشف التطور التاريخي للصورة على أنه بينما كان الأعتقاد السائد سابقاً بأن الكاميرا هي الطريقة الأكثر إستخداماً في الإشارة إلي المظاهر الخاصة بالأشياء والأشخاص والأدلة الخاصة بالوقائع، وأن التصوير الفوتوغرافى هو اكثر الوسائل شفافية ومباشرة في الأقتراب من الواقع، مع التحول للتصوير الرقمى ، بدا واضحاً أننا ندخل مرحلة جديدة، لم تعد فيها الصورة تمثل الحقيقة، وانها تنتقل بالمعرفة

لمستوى جديد ومختلف عما سبقه ، وأن ثمة تطورات كبيرة في طرق نقل الصور والمعلومات ومعالجتها وتخزينها ، وأن جودة الصورة في تحسن مستمر، وأن التصوير قد تحرر من قيود التركيز على جماليات الصورة إلى التركيز على أهمية جماليات الواقع ، وأن الكاميرا قد أصبحت الوسيط الجماهيرى الذى يمكن إستخدامة بطريقة ديمقراطية، كما يشير هذا التطور إلى أننا في بداية مرحلة جديدة في ثقافة أخلاقيات الصورة، وخاصة الإعلامية منها ، حيث أصبح من السهل التلاعب بالصور وتوظيفها فى خدمة أغراض عديدة (المحمودى، ٢٠١٥)

٣-مجالات معالجة الصورة

١-**التعرف**: أهم ميزة من مميزات معالجة الصورة مثل: التعرف على الوجوه التعرف على بصمة الإصبع التعرف على بصمة الكتابة التعرف على بصمة اليد ، وهو يعنى مقارنة بصمة شخص بشخص اخر ، وتحديد صورة من قاعدة البيانات و تحديد وجودها من عدمه ، بالإضافة الى التحري: البحث داخل قاعدة البيانات على أحدث صورة ، وللتعرف على شروط مثل : كمية الإضاءة والتي تقاس من حيث كونها هندسية:الحد الأدنى اللازم لإضاءة الموضوع المصور أو فنية: الإضاءة الجمالية التي تبرز أحد الأشكال الجمالية المعينة في وجه الشخص زاوية الكاميرا: مرتفعة – منخفضة – مستوى النظر.

٢-**استرجاع الصورة:** يتم إسترجاع البيانات عن طريق أحد الصور من أحد قواعد البيانات.

٣-**ترميم الصورة:** في حالة الصور التي يوجد بها عيوب ويصعب في حالة الصور التي لا يمكن التقاطها مرة أخرى.

٤-**نمذجة الصور:** عمل نموذج يحاكي الصورة الأصلية.

٥-**التتبع**: هي عملية تحديد مكان أو تعقب جسم متحرك باستخدام كامير (Gonzalez ,2018)

٤-أنواع الصورة الرقمية:

- **الصورة الثنائية Binary image**

هي صورة تتكون من رقمين (1,0) وتحتوي على اللونين الأبيض والإسود، تسمى one bit par bicsel، البكسل لو أصغر من ال bit أو العكس يحدث تشويش في الصورة .

- **الصورة متدرجة رمادي gray scale image**

هي الصورة التي تحتوي على الأبيض والإسود مع التدرجات الرمادية، تمثل شدتها بأرقام من ٠ إلى ٢٥٥ وتعتمد على كمية المستويات الرمادية، يوضح حجم الإضاءة على الصورة عن طريق أحد صورة أبيض وإسود ثم توضع عليها اضاءة ملونة تصبح الصورة بين الأبيض والإسود وبين الألوان.

- **الصورة الملونة color image**

يوجد بها ال balيتم تخصيص 3 bal لكل وحدة ضوئية لتحديد شدة الثلاثة ألوان الاساسية (أحمر-أخضر-أزرق) كل خانة تحتوي على 8bit (أوضح صورة).

- **الصورة المتحركة**

عبارة عن مجموعة من اللقطات الفلمية المتحركة تسجل بطريقة تماثلية أو رقمية وتعرض بنفس الطريقة التي سجلت بها ولها نوعين: صورة نقطية bit map وهي عبارة عن شبكة من البكسلات في الصورة فيها كل بكسل له موقع محدد على الشاشة وعند تكبير الصورة يحدث تشويش، صورة شعاعية victor وهي وصف هندسي يطرأ على الصورة بأي بعد، التكبير والتصغير لا يؤثر في حجم الصورة (شعبان، ٢٠١٠)

٥-تعلم الآلة

تعلم الآلة: هو أحد فروع علوم الحاسب المتفرع من علم الذكاء الاصطناعي يهدف إلى بناء نماذج من المدخلات للمساعدة في إتخاذ القرارات ويتدخل علم الآلة مع علم

الإحصاء حيث أن الإثنان يهدفان الي سرعة التنبؤ من خلال الحاسب Michael (Haenlein, 2019)

خوارزميات التعلم:

التعليم المراقب: فيه يتم إعطاء أمثلة لمدخلات الآله والمخرجات المرغوبة.

التصنيف: هذا النوع هو الأكثر استخداماً في تعلم الآله، يكون فيه الدخل مصنف إلى نوعين أو أكثر.

الانحدار: يقوم على تنبؤ قيم فيه يتم تصنيف أي دخل جديد، مثل: التنبؤ بأسعار البورصة _ التنبؤ بدرجة الحرارة.

التجميع: يتم فرز الدخل إلى مجموعات غير معروفة مسبقاً، تطبيقاته: تعلم حركة الشخص والمواقف الجديدة.

التعلم التعزيزى: الأقل إستخداماً من خلاله يتم إعطاء اشارات تشير الي مكافئة أو عقاب بناء على السلوك المعزز.

إستخلاص المميزات: عندما يكون دخل خوارزمية ما كبير جداً بحيث يصعب معالجتها بسهولة يتوقع إنتشار حجم البيانات قد يؤدي إلى إرتفاع التكلفة وكثرة الضغط على المعالج عندها يتم تحويل البيانات أي شكل أبسط يمثل البيانات الأصلية ويطلق على هذه العملية تحويل البيانات الي مميزات (الشذا & عناب ٢٠١٨)

٦-مكونات الشبكة العصبية وكيفية معالجة المعلومات:

تتم معالجة المعلومات في عناصر معالجة بسيطة تدعي العصبونات تمر الإشارات بين العصبونات عبر خطوط ربط، يرفق كل خط بوزن معين والذي يضرب مع الإشارات الداخلة الي العصبون، يطبق على كل عصبون تابع تنشيط غير خطي.

خصائص النظام العصبي:

- المعالجة المتوازية والموزعة.
- قابلية تعديل الاوزان.
- التعليم عملية مستمرة بلا إشراف.

- يعتمد فقط على المعلومات المحلية.

صفات الشبكات العصبية:

- الترابط.
- تحديد الأوزان.
- التنشيط للمستقبل.

مزايا الشبكات العصبية:

- قدرتها على حل العديد من المشاكل.
- إدارة فعالة لتكوين نماذج رياضية.
- لا تخزن المعلومات في مواقع محدده كما هو الحال في الحواسب الرقمية.

طرق تدريب الشبكات العصبية الاصطناعية:

- تدريب بإشراف معلم.
- تدريب بدون إشراف معلم.
- شبكات التوزيع الثابتة.
- خوارزمية تعيين الشبكة.
- خوارزمية الإنتشار العكسي (الحسينى، ٢٠١٥)

٧-الشبكات العصبية والقياسات الحيوية

يمكن تعريف الشبكات العصبية الاصطناعية (Artificial Neural Network) على أنها العلم الذي يهتم بدراسة أنظمة الضبط والإتصالات في الكائنات الحية، بهدف صنع نموذج شبيه بالعقل البشرى، وكذلك يمكن تعريفها على إنها تراكيب حسابية ثم صياغتها بالإعتماد على الخلايا الباثولوجية، وتعرف على إنها نظام معالجة للمعلومات له مميزات أداء معينة بإسلوب يحاكى الشبكات العصبية الحية ، الشبكات العصبية بنوعيها التى تعمل بإشراف والتى تعمل بدون إشراف طبقة واحدة أو من عدة طبقات إستطاعت وبنجاح تطبيق مختلف التصانيف ومسائل التمييز إذ أنها إستخدمت في تمييز أنواع كثيرة من الأشياء كالصور والصوت وغيرهما

(Al_Yaseen Sh., 2000)

كل شبكة عصبية قد تم تدريبها بإستخدام خوارزمية الإنتشار العكسي تدعي بالشبكة العصبية ذات الإنتشار العكسى ، وتعتبر الشبكة العصبية ذات الإنتشار العكسي نموذجاً مألوفاً جداً في الشبكات العصبية، وهي الأكثر إستخداماً في معمارية الشبكات العصبية، والسبب الرئيسى لهذا هو: أنها سهلة التنفيذ، إذ أن الشبكات المستخدمة لخوارزمية الإنتشار العكسي تتعلم المخططات المعقدة المتعددة الأبعاد بسهولة أكثر من استخدامها للخوارزميات الأخرى، والعديد من التطبيقات يمكن أن تصاغ بإستخدام شبكة الإنتشار العكسي إذ يكون لديها نموذج لأغلب الشبكات العصبية المتعددة الطبقات، ومن ثم يمكن القول إن أكثر طريقة تدريب شائعة الإستخدام في الشبكات العصبية المتعددة الطبقات هي خوارزمية الإنتشار العكسى، (النعيمى ،٢٠١١)

ثالثا: أنواع التهديدات على النظم داخل البنوك:

أولاً–التهديدات الناتجة عن الإعتداء:

تتعدد أنواع التهديدات الناتجة عن الإعتداء ومنها مايلى:

١-البرامج الضارة (الخبيثة):

ولهذه البرامج الضارة أشكال متعددة منها:

- الفيروسات : برامج خبيثة تم تصميمها من قبل المبرمجين لتحقيق بعض الأهداف ، وهذه الأهداف قد تكون غير مفيدة وقد تكون خطيرة ومدمرة كتعطيل وتدمير الأجهزة والبرامج ويكون للفيروسات القدرةعلى ربط نفسها بالبرامج ونسخ ماتحتويه البرامج دون علم .
- حصان طراودة : رمز خبيث يتخفى داخل البرامج يمكن أن يمرر الفيروسات أو أى رموز خبيثة أخرى تمكنه من الدخول إلى النظام المعلوماتى (Laudon&Laudon, 2006)
- الديدان وهي برامج تنتقل من حاسب لأخر داخل الشبكة دون تدخل بشرى وتنتشر

بسرعة فائقة عن الفيروسات وتخفي برامج وتعمل على إعاقة شبكة المعلومات فستطيع أن تنسخ نفسها بدون تدخلات خارجية أو داخلية (فيلالي & شليل، ٢٠١٨)

٢- القرصنة المعلوماتية:

تستخدم قرصنة الإنترنت والبرامج أساليب عديدة لإختراق الشبكات وقد يكون الضرر مقتصر على سرقة معلومات محددة، وقد يكون مدمراً يؤدى إلى تعطيل شبكة وأبرز أساليب القرصنة تعطيل شبكات الحاسب، وهذه الأساليب تستهدف البنوك وهدفها جعل جهاز أو الشبكة غير متاحه لدى المستخدمين وتتمثل طرق القرصنة في التصنت، سرقة الهوية عن طريق سرقة الممتلكات الخاصة لدى العملاء مثل بطاقة الإئتمان، بطاقة تعريف، كلمة السر (فيلالي، شليل، ٢٠١٨)

٣- التهديدات المادية:

وتتمثل هذه التهديدات مع الأجهزة المعلوماتية ومنها السرقة، وتستهدف كل مايتعلق بأنظمة المعلومات فالسرقة تكبد البنوك تكاليف جسيمة لما تحتوي من معلومات مهمة التى تخص العملاء كما أن الوصول والتدمير المادى للأجهزة قصداً من الأخطار الأمنية التى يمكن للمهاجم أن يدمرها إرادياً ويعمل على تخريبها (فيلالي & شليل، ٢٠١٨)

٤- سرقة كلمة السر اثناء التعامل مع الصراف الالى:

الان انتشرت بشكل كبير حوادث سرقة البطاقات الائتمانية وحصول السارق على مبالغ من حساب الضحية دون علم، وتتمثل في وضع جهاز مغناطيسى اثناء عملية السحب من الماكينة ليقوم بنسخ كلمة السر في الماكينة ثم يعاود السارق بعد انصراف العميل باستخدام الماكينة بكلمة السر المنسوخة للحصول على النقود المسروقة، لذا يجب على مستخدم ماكينة الصراف الالى فحص الماكينة جيدا قبل وضع كارت السحب في الماكينة (ملاحظة أحد الباحثين وتصويرة، ٢٠١٩).

ثانياً – التهديدات الناتجة عن ثغرات أمنية:

وتعرف التغيرات بأنها نقاط الضعف في تصميم البرامج أو قواعد التخزين، أو برامج التشغيل التى تمر بها المعلومات، ويتسلل المهاجم من هذه الثغرات لإحداث الضرر الذي يريده، ويجب فحص الشبكات والبرامج لتحديد هذه الثغرات وكيفية معالجتها، ويحاول المهاجمين إستغلال نقطة الضعف لشن هجمات، عن طريق تطوير برامج خبيثة تخترق النظام (الغثير وآخرون، ٢٠٠٩).

ومما سبق يتضح أن التهديدات السابقة سوف تؤثر على العمليات الداخلية والخارجية في البنوك الناتجة عن الهجمات وإختراق النظم الأمنية ونظم المعلومات، وتعدد صور ومصادر هذه التهديدات جعلت مشكلة التأمين واحدة من أكبر المشاكل التى تواجه البنوك نتيجة تزايد المعاملات اليومية داخل البنوك لدى العملاء، وقد تعمل هذه التهديدات على ضياع بعض أو كل المعلومات الخاصة بالعملاء.

ثالثاً: طرق مواجهة هذه التهديدات:

مع زيادة القيمة الإقتصادية والمالية للمعلومات ونمو فكرة رأس المال الفكرى

والإقتصاد الرقمى، تتطلب الأمر توفير الحماية لنظم المعلومات بإستخدام مجموعة من الوسائل التكنولوجية المختلفة، لحماية تبادل المعلومات ونظمها، وتعتبر إستراتيجية أمن المعلومات من الوسائل التكنولوجيه التى تتطبق داخل البنوك، وتتمكن من الحصول على المعلومات والعمل على إدارتها وتنظيمها (الطنملى، ٢٠٠٩)، وتتعدد أشكال الحماية لمواجهة التهديدات الخاصة بالبنوك كمايلى:

١- الحماية البرمجية للمعلومات وأنظمة المعلومات:

عملية تحديد صلاحيات الدخول وإستخدام أنظمة المعلومات التى تحتويها لتشمل الأطراف أوالأشخاص التى تستخدم هذه المعلومات وتقل البيانات بالطريقة التى تضمن الخصوصية، وتتعدد طرق الحماية البرمجية للمعلومات والأنظمة وتشمل: -

- **الجدار النارى:**

وعرف (عبد الحميد، ٢٠١٤) انها عبارة عن مجموعة مترابطة من البرامج تقع على شبكة الحاسب الخاصة بالبنك، وتقوم بحماية الموارد الخاصة بالشبكة من مستخدمى الشبكات، وفكرة الجدار النارى يشبه فكرة كانت تستخدمها القبائل فى العصور القديمة من وضع دوائر نيران لتمنع الإعداء من الوصول إليها.

- **برامج مكافحة الفيروسات:**

تقوم هذه البرامج بالتحقق من الأنظمة والأقراص من أجل تحديد أماكن الفيروسات، وتعمل على تنظيقها من أجل إبقاء البرامج فعالة، وتقوم بإستخدام مجموعة مفاتيح تشفير وفك الشفرة من قبل المسموح لهم بتسليمها. (حسين، ٢٠١٢)

- **أنظمة كشف التدخل ومراقبة الدخول:**

وتشمل أنظمة كشف التدخل أدوات مراقبة مستمرة موضوعة في أماكن الدخول لشبكات المؤسسة من أجل كشف التدخلات، ثم يطلق النظام إنذار في وقت حدوث حدث غير عادى وتعرف مراقبة الدخول بأنها الإجراءات المتخذه من قبل المؤسسات لإعاقة دخول الأنظمة من قبل الأشخاص الممنوعين (فيلالى & شليل، ٢٠١٨)

٢- الحماية المادية للممتلكات:

ويقصد بها كافة الوسائل التى تمنع الوصول إلى نظم المعلومات وقواعدها وجميع الوسائل التى تمنع الوصول إلى الأجهزة الحساسة وتأخذ صور الحماية المادية مايلى (النجار، ٢٠١٣): -

ا – أمن موقع النظام: - عن طريق تخصيص غرفة مغلقة لحفظ أجهزة الخادم المركزية.

ب – حماية المعلومات الحساسة عن طريق تركيب الكابلات في أماكن محمية.

ج – أمن تجهيزات نظم المعلومات عن طريق إستخدام كابلات مغلقة .

٣- الحماية الخاصة بالأفراد:

وهى الحماية الخاصة بالموظفين العاملين بالنظام والعملاء لأنها من العناصر الأساسية التى تؤدى إلى إلحاق الضرر بالمعلومات سواء بشكل غير مقصود بسبب ضعف مستوى التعامل مع النظام أو بشكل مقصود فى حالة رغبتهم الإساءة للمكان الذين يعملون فيه لأى سبب من الدوافع (ملل ، طمع ، إثبات ذات) ويأتى ذلك عن طريق ، حفظ كلمة السر الخاصة بالعميل ، إستخدام كلمة سر صعبة بحيث تحتوى على حروف وأرقام ويفضل تغيرها كل فترة ، عدم إفشاء كلمة السر لأحد موظفى البنك ، أخذ الحيطه والحذر عند إستخدام كلمة السر ، التأكد من هوية العميل وتأمين هذه الهوية عن طريق طلب معلومات إضافية عن العميل مثل تاريخ الميلاد وغيرها (عبد الحميد، ٢٠١٤).

٤- حماية حقوق الملكية الفكرية:

البرامج من أهم العناصر لنجاح النظام وذلك عن طريق حماية البرامج وطريقة إدارة النظام وأنظمة الإتصالات ويتطلب إتباع عدد من الإجراءات تمنع أى شخص من إمكانية التلاعب والدخول للنظام، ومن الإجراءات الخاصة بحماية البرامج عمل نسخ إحتياطية للملفات المهمة لتلاشى الفقدان، حماية قواعد البيانات وشبكات الإنترنت، وذلك عن طريق تدريب المستخدمين لنظام المعلومات فى مجال أمن الشبكات وقواعد البيانات وأمن نظم المعلومات (الشمالى، ٢٠١٧)

٥- حماية المعلومات الخاصة بالبنوك:

هناك الكثير من المعلومات التى تتطلب حماية حتى لا يستطيع الغير الحصول عليها، حيث لا تؤثر على سير العملية الإنتاجية للمنظمات كمايلى (داود، ٢٠٠٠)

- المعلومات المالية.
- الأسرار الداخلية.
- معلومات عن الموارد البشرية.
- الأداء المصرفى.
- معلومات العملاء.

٣-الدراسة الميدانية:

- **الهدف من الاستبيان:**

هدفت الدراسة الميدانية الوقوف على المتغيرات التالية: تحديد الوضع الأمني الحالي في البنوك المصرية، معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء في البنوك، معرفة اهم عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء.

- **تحديد محاور الاستبيان:**

في ضوء العديد من الدراسات التي اهتمت بدراسة الاستبيان تم تحديد المحاور التالية:
المحور الأول: تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.
المحور الثانى: معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.
المحور الثالث: معرفة عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.

- **صدق الاستبيان**

تم عرض الاستبيان على مجموعة من المحكميين من السادة أعضاء هيئة التدريس في جامعة كفرالشيخ وعددهم (٨) وبناء على مقترحات السادة المحكميين تم استبعاد بعض العبارات وإعادة صياغة بعض العبارات واخذ الباحثين العبارات التي اتفق عليها جميع السادة المحكميين، وقام الباحثين بإجراء صدق الاتساق الداخلي للأداة (المقياس) على عينة الدراسة وكانت النتيجة كما بالجدول (١) والذى يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الأول: تحديد الوضع الأمني الحالي في

البنوك المصرية للعملاء والموظفين ، وجدول (٢) والذى يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الثانى: اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين، والجدولب (٣) والذى يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الثالث: عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين، كما يوضح الجدول (٤) اتساق كل محورفى المقياس مع الدرجة الكلية للمقياس:

جدول (١)

يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الأول: تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.

رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة	رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة
١	٠.٤٥	٠.٠١	٩	٠.٥٤	٠.٠١
٢	٠.٤٨	٠.٠١	١٠	٠.٥٢	٠.٠١
٣	٠.٦١	٠.٠١	١١	٠.٣٨	٠.٠١
٤	٠.٥٤	٠.٠١	١٢	٠.٦١	٠.٠١
٥	٠.٣٦	٠.٠١	١٣	٠.٣٨	٠.٠١
٦	٠.٤٢	٠.٠١	١٤	٠.٥١	٠.٠١
٧	٠.٦٤	٠.٠١	١٥	٠.٣٧	٠.٠١
٨	٠.٤٥	٠.٠١			

جدول (٢)

يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الثانى: معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.

رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة	رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة
١	٠.٥٤	٠.٠١	٩	٠.٦٢	٠.٠١
٢	٠.٢٦	٠.٠١	١٠	٠.٤٦	٠.٠١
٣	٠.٤٧	٠.٠١	١١	٠.٤٧	٠.٠١
٤	٠.٤٦	٠.٠١	١٢	٠.٤٩	٠.٠١
٥	٠.٤٩	٠.٠١	١٣	٠.٣٨	٠.٠١
٦	٠.٦٤	٠.٠١	١٤	٠.٤٩	٠.٠١
٧	٠.٣٧	٠.٠١	١٥	٠.٥١	٠.٠١
٨	٠.٥٧	٠.٠١			

جدول (٣)

يوضح معامل ارتباط العبارة بالدرجة الكلية للمحور الثالث: معرفة عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.

رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة	رقم العبارة	ارتباط العبارة بالدرجة الكلية	دلالة معامل العبارة
١	٠.٦٤	٠.٠١	١٣	٠.٥٧	٠.٠١
٢	٠.٣٨	٠.٠١	١٤	٠.٣٩	٠.٠١

٣	٠.٤٩	٠.٠١	١٥	٠.٢٤	٠.٠١
٤	٠.٦٤	٠.٠١	١٦	٠.٦٧	٠.٠١
٥	٠.٤٢	٠.٠١	١٧	٠.٦١	٠.٠١
٦	٠.٤٩	٠.٠١	١٨	٠.٥٢	٠.٠١
٧	٠.٣٧	٠.٠١	١٩	٠.٦١	٠.٠١
٨	٠.٥٧	٠.٠١	٢٠	٠.٣٤	٠.٠١
٩	٠.٦٤	٠.٠١	٢١	٠.٦٣	٠.٠١
١٠	٠.٣٨	٠.٠١	٢٢	٠.٢٨	٠.٠١
١١	٠.٥٢	٠.٠١	٢٣	٠.٣٩	٠.٠١
١٢	٠.٤٥	٠.٠١			

جدول (٤)

اتساق كل محور مع الدرجة الكلية للمقياس:

رقم المحور	ابعاد المحور	معامل ارتباط المحور مع الدرجة الكلية للمحور	دلالة معامل الارتباط
الأول	- تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.	٠.٨٤٨	دال عند ٠.٠١
الثانى	- اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.	٠.٩١٠	دال عند ٠.٠١
الثالث	- عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.	٠.٧٩٢	دال عند ٠.٠١

- **حساب ثبات المقياس**

بطريقتين هما:

الطريقة الأولي: باستخدام التجزئة النصفية:

قام الباحثان بإجراء حساب معامل الثبات بطريقة التجزئة النصفية من خلال برنامج SPSS حيث كشف التحليل ان معامل الارتباط سبيرمان براون قدره (٠.٨٢٧) كما بالجدول (٥) وهو معامل مرتفع لثبات المقياس.

الطريقة الثانية باستخدام الفا كرونباخ

تم حساب ثبات المقياس بطريقة الفا كرونباخ وقد وجد أنه (٠.٨١٣) كما بالجدول (٥)، وبذلك يعتبر المقياس ثابت الى حد كبير.

جدول (٥)

حساب ثبات المقياس

المحور	البيان	عدد العناصر	الفا كرونباخ	التجزئة النصفية
الاول	- تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.	١٥	٠.٨٩٣	٠.٨٦١
الثانى	-اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.	١٥	٠.٧١٤	٠.٧٩٥
الثالث	-عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.	٢٣	٠.٨٣٢	٠.٨٢٦
جميع متغيرات استمارة الاستبيان معا			**٠.٨١٣**	**٠.٨٢٧**

- **عينة الدراسة:**

تتكون عينة الدراسة من (عملاء البنوك في محافظتى كفرالشيخ والدقهلية، االموظفين في البنوك في نفس المحافظتين)، وقد تم اختيار عينة الدراسة بطريقة حكمية ممن اتيح للباحث الاتصال بالخاضعيين للاستبيان، وبلغ حجم العينة ٥٥ فردا،

وكما هو موضح في الجدول (٦)، فقد بلغت نسبة الاستجابة ٦٣.٦٣ % حيث بلغ عدد الاستجابات ٣٥ استبيان، وهي نسبة مقبولة لإجراء التحليل الاحصائي.

جدول (٦)

بيان استمارات الاستقصاء الموزعة والمستلمة

المحور	الفئات	الاستمارات الموزعة			نسبة الاستجابة
		الموزعة	المستلمة الصحيحة	غير المرتدة	
الاول	- تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء والموظفين.	٥٥	٣٥	١٥	%٦٣.٦٣
الثانى	- معرفة اهمية القياسات الحيوية في تامين البيانات للعملاء والموظفين.	٥٥	٣٥	١٥	%٦٣.٦٣
الثالث	- معرفة عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء والموظفين.	٥٥	٣٥	١٥	%٦٣.٦٣
	الإجمالي	**١٦٥**	**١٠٥**	**٤٥**	**%٦٣.٦٣**

- **أساليب التحليل الاحصائي:**

بعد ترميز البيانات وادخالها للحاسب الالي، قام الباحث بتحليل البيانات الواردة بقائمة الاستقصاء من خلال برنامج (SPSS 19.0).

الاجابة على تساؤلات الدراسة:

السؤال الرئيسى:

ما الوضع الأمني الحالي ودور القياسات الحيوية وعناصرها الأهم في تامين البيانات للعملاء والموظفين في البنوك المصرية، ويتفرع من هذا السؤال مجموعة من الأسئلة الفرعية:

السؤال الأول: ما هو الوضع الأمني الحالي في البنوك المصرية للعملاء.

السؤال الثانى: ما هو الوضع الأمني الحالي في البنوك المصرية للموظفين.

السؤال الثالث: ما اهمية القياسات الحيوية في تامين بيانات العملاء.

السؤال الرابع: ما اهمية القياسات الحيوية في تامين البيانات للموظفين.

السؤال الخامس: ما عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات العملاء.

السؤال السادس: ما عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات الموظفين.

جدول (٧)

الميزان التقديرى وفقا لمقياس ليكرت الخماسي(Subedi ,2016)

م	الاستجابة	المتوسط المرجح	الاتجاة العام
١	لا اوافق بشدة	من ١ الى ١.٨٠	عدم الموافقة بشدة
٢	لا اوافق	من ١.٨١ الى ٢.٦٠	عدم الموافقة
٣	موافق الى حد ما	من ٢.٦١ الى ٣.٤٠	المحايدة
٤	اوافق	من ٣.٤١ الى ٤.٢٠	الموافقة
٥	اوافق بشدة	اكبر من ٤.٢٠	الموافقة بشدة

السوال الأول

ما هو الوضع الأمني الحالي في البنوك المصرية للعملاء.

جدول (٨)

المتوسط الترجيحى والانحراف المعيارى للمحور الأول الوضع الأمني الحالي في البنوك المصرية للعملاء.

م	الوضع الأمني الحالي في البنوك المصرية للعملاء.	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- نظام أمن المعلومات الحالى للبنوك يساعد على حماية حسابات العملاء	2.9	0.28	محايد
٢	- نظام أمن المعلومات الحالى للبنوك يساعد على عدم قدرة موظفى البنك من التلاعب بحسابات العملاء	2.9	0.55	محايد
٣	- نظام أمن المعلومات الحالى للبنوك يصعب اختراقه.	2.3	0.74	لا أوافق
٤	- نظام أمن المعلومات الحالى للبنوك يساعد على معرفة هوية الموظفين المتلاعبين بالحسابات.	2.5	0.98	لا أوافق
٥	- نظام أمن المعلومات الحالى للبنوك يسمح بتخمين الرقم السري للكارت عن طريق برامج التباديل والتوافيق .	2.7	0.99	محايد
٦	- نظام أمن المعلومات الحالى للبنوك يتبنى أحدث وسائل وطرق تأمين البيانات.	2.1	1.40	لا أوافق
٧	- نظام أمن المعلومات الحالى للبنوك يشعر العملاء بالطمأنينة والمصداقية.	2.9	0.45	محايد

٨	- نظـام أمـن المعلومـات الحـالى للبنـوك يعـرض المعلومـات الشخصـية والبطاقـات الذكية للعملاء للاختراق بسهولة	1.4	1.01	لا أوافق إطلاقا
٩	- نظـام أمـن المعلومـات الحـالى للبنـوك يعـرض المعلومـات الشخصـية والبطاقـات الذكية للنسيان مما يكلف صاحبها مادياً.	2.9	0.90	محايد
١٠	- نظام أمن المعلومات الحالى للبنوك توفير حمايـة مـن عمليـات الغـش المصـرفي مـن العمليات التي تتم على الانترنت.	2.7	1.01	محايد
١١	- نظام أمن المعلومات الحالى للبنوك يتحقق آليا من إبطال آليات الوصول لموظفى البنك السابقيين .	2.4	1.04	لا أوافق
١٢	- نظام أمن المعلومات الحالى للبنوك يوفر رقابـة امنيـة علـى عمليـة الوصـول الـى برمجيات الحاسوب.	2.5	1.07	لا أوافق
١٣	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة أمينة على المخرجات.	2.9	0.90	محايد
١٤	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة امنية على مستخدمي البرامج.	3	0.75	محايد
١٥	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة امنية عل فصل المهام والواجبات.	3.1	0.36	محايد
	القييم العام	**2.61**		**محايد**

من الجدول السابق (٨) يتضح ان المتوسط الترجيحى للمحور الأول: تحديد الوضع الأمني الحالي في البنوك المصرية للعملاء هو (٢.٦١)، وفى ضوء مقياس ليكرت عبر المتوسط الترجيحى " محايد "، ويتضح من ذلك من وجهة نظر العملاء

أن النظام الحالي للحماية بالبنك يحقق الغرض المطلوب ولكن ليس بالشكل الكافى الذي يحقق طمأنينه وثقة لتلك العملاء.

السوال الثانى:

ما هو الوضع الأمني الحالي في البنوك المصرية للموظفين.

جدول رقم (٩)

المتوسط الترجيحى والانحراف المعيارى للمحور الثانى الوضع الامنى الحالي في البنوك المصرية للموظفين

م	الوضع الأمني الحالي في البنوك المصرية للموظفين	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- نظام أمن المعلومات الحالى للبنوك يساعد على حماية حسابات العملاء	3.8	0.73	أوافق
٢	- نظام أمن المعلومات الحالى للبنوك يساعد على عدم قدرة موظفى البنك من التلاعب بحسابات العملاء	3.5	0.95	أوافق
٣	- نظام أمن المعلومات الحالى للبنوك يصعب اختراقه.	3.9	1.16	أوافق
٤	- نظام أمن المعلومات الحالى للبنوك يساعد على معرفة هوية الموظفين المتلاعبين بالحسابات.	3.4	0.85	أوافق
٥	- نظام أمن المعلومات الحالى للبنوك يسمح بتخمين الرقم السري للكارت عن طريق برامج التباديل والتوافيق .	3.2	1.25	محايد
٦	- نظام أمن المعلومات الحالى للبنوك يتبنى أحدث وسائل وطرق تأمين البيانات.	3.6	1.12	أوافق

٧	- نظـام أمـن المعلومـات الحـالى للبنـوك يشعر العملاء بالطمأنينة والمصداقية.	3.5	0.85	أوافق
٨	- نظـام أمـن المعلومـات الحـالى للبنـوك يعرض المعلومات الشخصية والبطاقات الذكية للعملاء للاختراق بسهولة	3.5	1.29	أوافق
٩	- نظـام أمـن المعلومـات الحـالى للبنـوك يعرض المعلومات الشخصية والبطاقات الذكية للنسيان مما يكلف صاحبها مادياً.	3.8	0.91	أوافق
١٠	- نظـام أمـن المعلومـات الحـالى للبنـوك توفير حماية من عمليات الغش المصرفي من العمليات التي تتم على الانترنت.	3.7	0.91	أوافق
١١	- نظـام أمـن المعلومـات الحـالى للبنـوك يتحقـق آليـا مـن إبطـال آليـات الوصـول لموظفى البنك السابقيين .	3.8	0.68	أوافق
١٢	- نظام أمن المعلومات الحالى للبنوك يوفر رقابـة امنيـة علـى عمليـة الوصـول الـى برمجيات الحاسوب.	3.6	1.37	أوافق
١٣	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة أمينة على المخرجات.	3.6	1.06	أوافق
١٤	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة امنية على مستخدمي البرامج.	3	0.75	محايد
١٥	- نظام أمن المعلومات الحالى للبنوك يوفر رقابة امنية عل فصل المهام والواجبات.	3.2	0.66	محايد
	القييم العام	**3.54**		**أوافق**

من الجدول السابق (٩) يتضح ان المتوسط الترجيحى المحور الأول: تحديد الوضع الأمني الحالي في البنوك المصرية للموظفين ككل هو (٣.٥٤) وفى ضوء مقياس ليكرت عبر المتوسط الترجيحى " أوافق"، ويتضح من ذلك من وجهة نظر الموظفين بالبنك أن النظام الحالي للحماية بالبنك يحقق الغرض المطلوب ولكنه لا يحقق الأمان الكامل والسرية الكاملة للمعلومات المرتبطة بحسابات العملاء.

السوال الثالث

ما اهمية القياسات الحيوية في تامين البيانات للعملاء..

جدول (١٠)

المتوسط الترجيحى والانحراف المعيارى للمحور الثانى

اهمية القياسات الحيوية في تامين البيانات للعملاء

م	اهمية القياسات الحيوية في تامين البيانات للعملاء	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- القياسات الحيوية تحقق الطمأنينة للعملاء .	4.7	0.89	أوافق تماما
٢	- القياسات الحيوية تتوافر أجهزتها بشكل كاف في البنوك.	3	0.82	محايد
٣	- القياسات الحيوية تعمل بشكل مرن.	4.7	0.90	أوافق تماما
٤	- القياسات الحيوية تتسم بالمرونة.	4.5	1.04	أوافق تماما
٥	- القياسات الحيوية أكثر دقة.	5	0.00	أوافق تماما
٦	- القياسات الحيوية تتسم بالسهولة والسرعة.	4.3	1.27	أوافق تماما

٧	- القياسات الحيوية وسيلة جيدة وهامة لجذب العملاء في البنوك.	4.8	0.49	أوافق تماما
٨	- القياسات الحيوية وسيلة لتقديم الخدمة أو المنتج في أماكن وأسواق مختلفة بشكل امن.	4.9	0.37	أوافق تماما
٩	- القياسات الحيوية وسيلة لا يقتصر تأثيرها على العملاء الذين يجدون التعامل مع الانترنت فقط.	4.3	1.09	أوافق تماما
١٠	- القياسات الحيوية تساهم في حل المشاكل التي تعيق استخدام الانترنت.	4.7	0.91	أوافق تماما
١١	- القياسات الحيوية تساهم في تقليل تكاليف التامين.	4.6	0.85	أوافق تماما
١٢	- القياسات الحيوية تعمل على تحسين خدمات العملاء.	4.6	0.91	أوافق تماما
١٣	- القياسات الحيوية توفر الوقت والجهد.	4.9	0.43	أوافق تماما
١٤	- القياسات الحيوية تعمل على زيادة كفاءة خدمات البنوك.	4.9	0.36	أوافق تماما
١٥	- القياسات الحيوية تحتاج الى بنية تحتية اضافية في البنوك.	4.7	0.89	أوافق تماما
	التقييم العام	**4.57**		**أوافق تماما**

من الجدول السابق رقم (١٠) يتضح ان المتوسط الترجيحى المحور الثانى: اهمية القياسات الحيوية في تامين البيانات في البنوك للعملاء ككل هو (٤.٥٧) وفى

ضوء مقياس ليكرت عبر المتوسط الترجيحى "أوافق تماما "، ويتضح من ذلك من وجهة نظر العملاء أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها في حماية وتأمين الحسابات الخاصة بهم من قبل البنوك.

السوال الرابع

ما اهمية القياسات الحيوية في تامين البيانات للموظفين.

جدول رقم (١١)

المتوسط الترجيحى والانحراف المعيارى المعيارى للمحور الثانى

اهمية القياسات الحيوية في تامين البيانات للموظفين

م	اهمية القياسات الحيوية في تامين البيانات للموظفين	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- القياسات الحيوية تحقق الطمأنينة للعملاء.	4.6	0.95	أوافق تماما
٢	- القياسات الحيوية تتوافر أجهزتها بشكل كاف في البنوك.	3.6	0.94	أوافق
٣	- القياسات الحيوية تعمل بشكل مرن.	4.5	1.04	أوافق تماما
٤	- القياسات الحيوية تتسم بالمرونة.	4.3	1.08	أوافق تماما
٥	- القياسات الحيوية أكثر دقة.	3.4	1.48	أوافق
٦	- القياسات الحيوية تتسم بالسهولة والسرعة.	3.4	1.48	أوافق
٧	- القياسات الحيوية وسيلة جيدة وهامة لجذب العملاء في البنوك.	4.4	0.98	أوافق تماما
٨	- القياسات الحيوية وسيلة لتقديم الخدمة أو المنتج في أماكن وأسواق مختلفة بشكل امن.	4.5	0.88	أوافق تماما
٩	- القياسات الحيوية وسيلة لا يقتصر تأثيرها على العملاء الذين يجدون التعامل مع الانترنت.	4.1	1.12	أوافق
١٠	- القياسات الحيوية تساهم في حل المشاكل التي تعيق استخدام الانترنت.	4.2	1.22	أوافق تماما
١١	- القياسات الحيوية تساهم في تقليل تكاليف التامين.	4.5	0.95	أوافق تماما
١٢	- القياسات الحيوية تعمل على تحسين خدمات العملاء.	4.5	0.98	أوافق تماما
١٣	- القياسات الحيوية توفر الوقت والجهد.	4.6	0.95	أوافق تماما

١٤	- القياسات الحيوية تعمل على زيادة كفاءة خدمات البنوك.	5	0.17	أوافق تماما
١٥	- القياسات الحيوية تحتاج الى بنية تحتية اضافية في البنوك.	4.9	0.37	أوافق تماما
	التقييم العام	**4.30**		**أوافق تماما**

من الجدول السابق رقم (١١) يتضح ان المتوسط الترجيحى المحور الثانى: اهمية القياسات الحيوية في تامين البيانات في البنوك للموظفين ككل هو (٤.٣٠) وفى ضوء مقياس ليكرت عبر المتوسط الترجيحى " أوافق" ويتضح من ذلك من وجهة نظر العاملين بالبنك أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها في حماية وتأمين البيانات الخاصة بالبنك وكذلك الحد من سهولة الوصول الى تلك البيانات إلا عن طريق من يصرح له بذلك.

السوال الخامس

ما عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات العملاء.

جدول رقم (١٢)

المتوسط الترجيحى والانحراف المعيارى للمحور الثالث

عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات العملاء.

م	عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات العملاء.	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- تمثل بصمة الاصبع أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	3.7	0.82	أوافق
٢	- استخدام بصمة الاصبع يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	2.9	0.84	محايد
٣	- يمكن تزوير شكل بصمة الاصبع.	3.1	0.66	محايد
٤	- بصمة الاصابع تتلاشى بالجروح.	3	0.00	محايد
٥	- تمثل بصمة الصوت أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	5	0.00	أوافق تماما

٦	- استخدام بصمة الصوت يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	4.1	0.53	أوافق
٧	- يمكن تزوير شكل بصمة الصوت.	2.9	0.81	محايد
٨	- بعض الامراض تؤثر على بصمة الصوت.	3.8	0.97	أوافق
٩	- تمثل بصمة اليد أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	4.1	0.50	أوافق
١٠	- استخدام بصمة اليد يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	2	0.17	لا أوافق
١١	- يمكن تزوير شكل بصمة اليد.	2.9	0.69	محايد
١٢	- تمثل بصمة الوجه أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	2.9	0.69	محايد
١٣	- يمكن تزوير شكل بصمة الوجه عن طريق بعض العمليات الجراحية	3	0.45	محايد
١٤	- بعض الأمراض تؤثر على بصمة الوجه.	3.9	0.51	أوافق
١٥	- تتشابه بصة الوجه بين الاخوات والاقارب.	2.5	0.95	لا أوافق
١٦	- تمثل بصمة العين أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	5	0.17	أوافق تماما
١٧	- استخدام بصمة العين يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	4.9	0.28	أوافق تماما
١٨	- بصمة العين تتميز بسهولة الاستخدام.	4.9	0.40	أوافق تماما
١٩	- لا تتشابه بصمة العين بين الاخوات والاقارب.	5	0.00	أوافق تماما
٢٠	- بصمة العين توفر درجة أمان مرتفعة.	5	0.00	أوافق تماما

٢١	- بصمة العين موجودة في أي وقت واي مكان ممكن يمكن إستخدامها بسهولة.	4.5	0.85	أوافق تماما
٢٢	- بصمة العين يصعب تزويرها.	4.9	0.50	أوافق تماما
٢٣	- بصمة العين اعلى دقة في تحديد الهوية.	5	0.00	أوافق تماما
	التقييم العام	**3.87**		**أوافق**

من الجدول السابق رقم (١٢) يتضح ان المتوسط الترجيحى المحور الثالث: عناصر القياسات الحيوية التي تساعد على حماية بيانات العملاء ككل هو (٣.٨٧) وفى ضوء مقياس ليكرت عبر المتوسط الترجيحى " أوافق "ويتضح من ذلك من وجهة نظر العملاء أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها، إلا أن أهم تلك القياسات من وجهة نظرهم التي يجب أن يعتمد عليها البرنامج المقترح لتأمين الحسابات الخاصة بهم هي بصمة العين، لما لها من مميزات تحقق الهدف من البرنامج.

السوال السادس

ما عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات الموظفين

جدول رقم (١٣)

المتوسط الترجيحى والانحراف المعيارى للمحور الثالث

عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات للموظفين

م	عناصر القياسات الحيوية الأفضل التي تساعد على حماية بيانات الموظفين	المتوسط الترجيحي	الانحراف المعياري	تعليق على المتوسط
١	- تمثل بصمة الاصبع أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	3.1	1.18	محايد

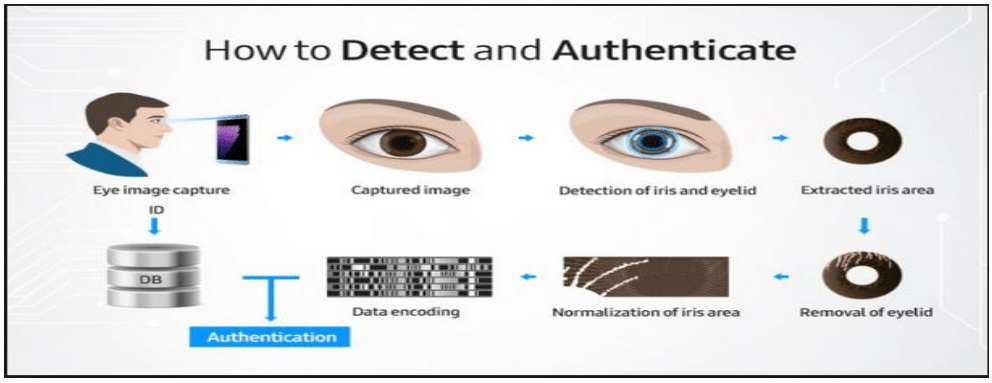
٢	- استخدام بصمة الاصبع يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	2.1	0.24	لا أوافق
٣	- يمكن تزوير شكل بصمة الاصبع.	3.9	0.56	أوافق
٤	- بصمة الاصابع تتلاشى بالجروح.	2.9	0.24	محايد
٥	- تمثل بصمة الصوت أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	4.9	0.43	أوافق تماما
٦	- استخدام بصمة الصوت يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	3.9	0.68	أوافق
٧	- يمكن تزوير شكل بصمة الصوت.	3.1	0.51	محايد
٨	- بعض الامراض تؤثر على بصمة الصوت.	3.9	0.42	أوافق
٩	- تمثل بصمة اليد أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	3.6	1.00	أوافق
١٠	- استخدام بصمة اليد يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	3.9	0.37	أوافق
١١	- يمكن تزوير شكل بصمة اليد.	3	0.17	محايد
١٢	- تمثل بصمة الوجه أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	3.3	0.77	محايد
١٣	- يمكن تزوير شكل بصمة الوجه عن طريق بعض العمليات الجراحية	3.7	0.56	أوافق
١٤	- بعض الأمراض تؤثر على بصمة الوجه.	4.1	0.88	أوافق
١٥	- تتشابه بصة الوجه بين الاخوات والاقارب.	3.8	0.77	أوافق
١٦	- تمثل بصمة العين أحد أساليب القياسات الحيوية التي تساعد على حماية هوية العملاء.	4.8	0.63	أوافق تماما
١٧	- استخدام بصمة العين يحتاج الى تجهيزات إضافية تؤدى الى زيادة التكاليف.	4.9	0.24	أوافق تماما

١٨	- بصمة العين تتميز بسهولة الاستخدام.	5	0.00	أوافق تماما
١٩	- لا تتشابه بصمة العين بين الاخوات والاقارب.	5	0.17	أوافق تماما
٢٠	- بصمة العين توفر درجة أمان مرتفعة.	5	0.00	أوافق تماما
٢١	- بصمة العين موجودة في أي وقت واي مكان ممكن يمكن إستخدامها بسهولة.	4.7	0.66	أوافق تماما
٢٢	- بصمة العين يصعب تزويرها.	5	0.00	أوافق تماما
٢٣	- بصمة العين اعلى دقة في تحديد الهوية.	4.9	0.37	أوافق تماما
	التقييم العام	**4.02**		**أوافق**

من الجدول السابق رقم (١٣) يتضح ان المتوسط الترجيحى المحور الثالث: عناصر القياسات الحيوية التي تساعد على حماية بيانات الموظفين ككل هو (٤.٠٢) وفى ضوء مقياس ليكرت عبر المتوسط الترجيحى "أوافق"، ويتضح من ذلك من وجهة نظر العاملين بالبنك أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها، إلا أن أهم تلك القياسات من وجهة نظرهم التي يجب أن يعتمد عليها البرنامج المقترح لتأمين الحسابات الخاصة بهم هي بصمة العين، لما لها من مميزات تحقق الهدف من البرنامج.

٤-انتاج البرنامج

كيفية عمل أنظمة القياسات الحيوية بمعالجة الصورة الرقمية



تعمل أجهزة البصمة بغض النظر عن نوعها وفقاً لثلاثة خطوات رئيسية، وهذه الخطوات هي كما يلي:

- التسجيل: وذلك من خلال أخذ المعلومات الأساسية للمستخدمين كالإسم أو رقم التعريف وأخذ صور للمستخدمين.
- التخزين: حيث تُخزَن كل معلومة خاصة بمستخدم معين على شكل رموز أو رسوم بيانية، وقد توضع بعض هذه الرموز على بطاقة تعريفية يحملها المستخدم.
- المقارنة: وذلك من خلال مطابقة الصفات التي يقدمها المستخدم لجهاز البصمة مع ما هو مُخزن به من بيانات، وتحديد فيما إذا كان هناك تطابق أم لا.

متطلبات البرنامج:

- تم تنفيذه بواسطة MATLAB
- كمبيوتر ذات معالج Core I5
- الذاكرة العشوائية ٨ جيجا
- كارت VGA ٤ جيجا

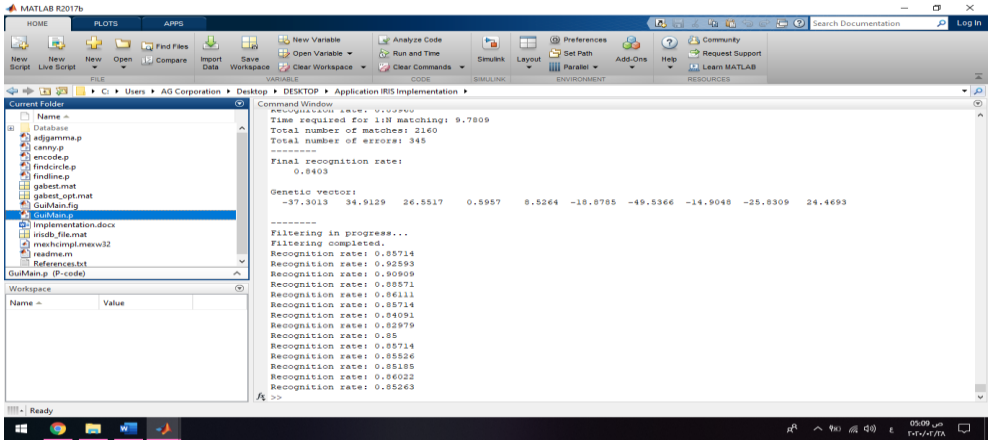
كيف يعمل البرنامج:

- فى البداية يقوم بإلتقاط صورة طبيعية للعين بالنقر على (فتح القاعدة)
- يمكن إضافة الصورة إلى قاعدة البيانات وربطها بالمستخدم بالنقر على (إضافة إلى قاعدة البيانات).
- يقوم بقص قزحية العين وهي الجزء الملون من العين.
- يمكن رفع أى صورة أخرى والنقر على (التعرف على بصمة العين) لتحديد المستخدم الخاص بها.

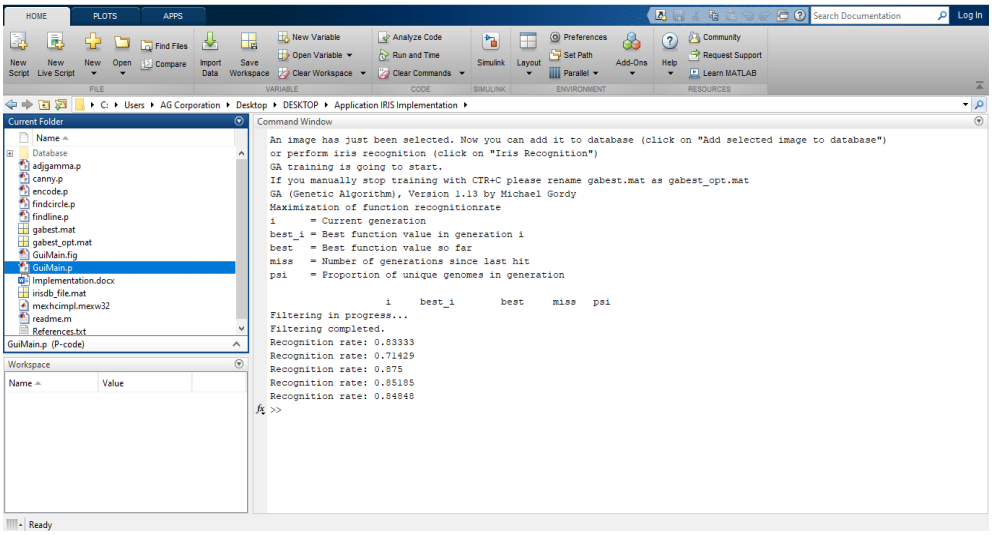
- **فى البداية يقوم بإلتقاط صورة طبيعية للعين بالنقر على (فتح القاعدة)**

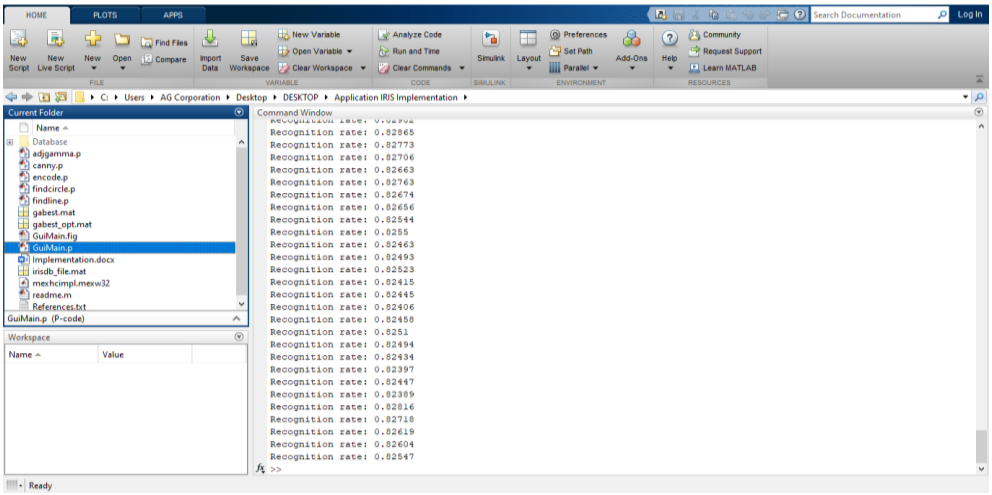
يمكن إضافة الصورة إلى قاعدة البيانات وربطها بالمستخدم بالنقر على (إضافة إلى قاعدة البيانات).

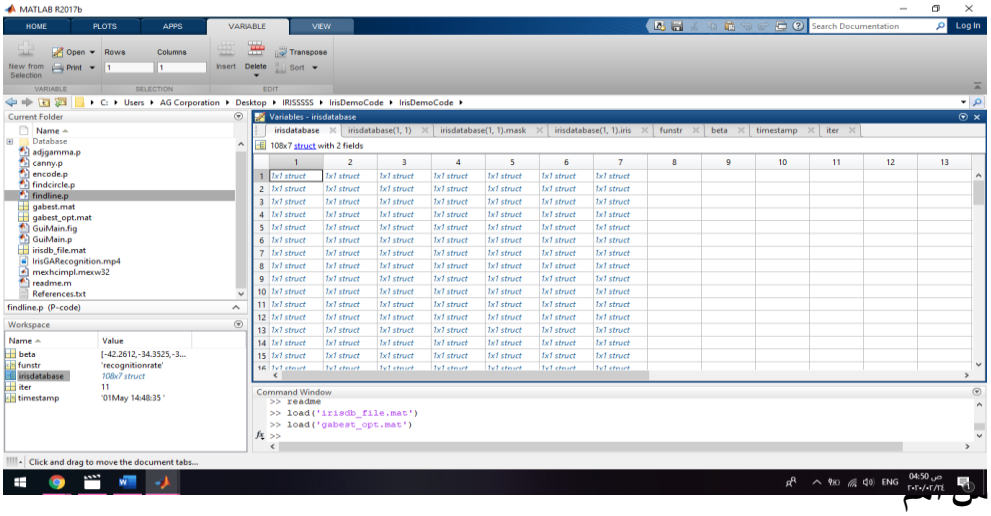
- **يقوم بقص قزحية العين وهي الجزء الملون من العين بعد إضافة الصورة إلى قاعدة البيانات**



يمكن رفع أى صورة أخرى والنقر على (التعرف على بصمة العين) لتحديد المستخدم وإظهار بياناته الخاصة


HOME
PLOTS
APPS
Search Documentation
Log In
New Script
New Live Script
New
Open
Find Files
Compare
Import Data
Save Workspace
New Variable
Open Variable
Clear Workspace
Analyze Code
Run and Time
Clear Commands
Simulink
Layout
Preferences
Set Path
Parallel
Add-Ons
Help
Community
Request Support
Learn MATLAB
FILE
VARIABLE
CODE
SIMULINK
ENVIRONMENT
RESOURCES
C: ▸ Users ▸ AG Corporation ▸ Desktop ▸ DESKTOP ▸ Application IRIS Implementation ▸
Current Folder
Name
Database
adjgamma.p
canny.p
encode.p
findcircle.p
findline.p
gabest.mat
gabest_opt.mat
GuiMain.fig
GuiMain.p
Implementation.docx
irisdb_file.mat
mexhcimpl.mexw32
readme.m
References.txt
GuiMain.p (P-code)
Workspace
Name
Value
Command Window
An image has just been selected. Now you can add it to database (click on "Add selected image to database")
or perform iris recognition (click on "Iris Recognition")
GA training is going to start.
If you manually stop training with CTR+C please rename gabest.mat as gabest_opt.mat
GA (Genetic Algorithm), Version 1.13 by Michael Gordy
Maximization of function recognitionrate
i = Current generation
best_i = Best function value in generation i
best = Best function value so far
miss = Number of generations since last hit
psi = Proportion of unique genomes in generation
i best_i best miss psi
Filtering in progress...
Filtering completed.
Recognition rate: 0.83333
Recognition rate: 0.71429
Recognition rate: 0.875
Recognition rate: 0.85185
Recognition rate: 0.84848
>>
Ready


HOME
PLOTS
APPS
Search Documentation
Log In
C: ▸ Users ▸ AG Corporation ▸ Desktop ▸ DESKTOP ▸ Application IRIS Implementation ▸
Current Folder
Command Window
Recognition rate: 0.82865
Recognition rate: 0.82773
Recognition rate: 0.82706
Recognition rate: 0.82663
Recognition rate: 0.82763
Recognition rate: 0.82674
Recognition rate: 0.82656
Recognition rate: 0.82544
Recognition rate: 0.8255
Recognition rate: 0.82463
Recognition rate: 0.82493
Recognition rate: 0.82523
Recognition rate: 0.82415
Recognition rate: 0.82445
Recognition rate: 0.82406
Recognition rate: 0.82458
Recognition rate: 0.8251
Recognition rate: 0.82494
Recognition rate: 0.82434
Recognition rate: 0.82397
Recognition rate: 0.82447
Recognition rate: 0.82389
Recognition rate: 0.82816
Recognition rate: 0.82718
Recognition rate: 0.82619
Recognition rate: 0.82604
Recognition rate: 0.82547
>>
Ready



النتائج التي توصل اليها الباحثان هي: -

- **من وجهة نظر ال**
- **عملاء:**

✓ أن النظام الحالي لحماية بياناتهم الشخصية يحقق الغرض المطلوب ولكن ليس بالشكل الكافى الذي يحقق لهم الطمأنينه.

✓ أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها في حماية وتأمين البيانات الخاصة بهم.

✓ أن أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها لتأمين الحسابات الخاصة بهم هي بصمة العين، لما لها من مميزات تحقق الهدف من البرنامج.

- **من وجهة نظر العاملين بالبنك:**

✓ النظام الحالي للحماية بالبنك يحقق الغرض المطلوب ولكنه لا يحقق الأمان الكامل والسرية الكاملة للمعلومات المرتبطة بحسابات العملاء، ولا

يستطيع عمل رقابة على المتعاملين مع حسابات العملاء.

- ✓ أن القياسات الحيوية أحد أهم أساليب التأمين الهامة التي يجب الأعتماد عليها في حماية وتأمين البيانات الخاصة بالبنك وكذلك للحد من سهولة الوصول الى تلك البيانات إلا عن طريق من يصرح له بذلك.
- ✓ أن أهم أساليب التأمين الهامة التي يجب الأعتماد عليها، لتأمين الحسابات الخاصة بالعملاء داخل البنك هي بصمة العين، لما لها من مميزات تحقق الهدف من البرنامج.

- تعرف القياسات الحيوية بأنها أساليب آلية يمكن من خلالها التعرف على الأشخاص بناءاً على خصائص فسيولوجية وسلوكية يمكن إستخدامها فى الأنظمة الأمنية للمساعدة على حماية الأشياء المهمة.
- تعد تقنية القياسات الحيوية فرع من الفروع المتميزة فى مجال معالجة الصور والذكاء الإصطناعى وتعلم الاله تعمل على إيجاد وتطوير التقنيات للتعرف على أنماط أو أشكال معينة.
- التطورات المتزايدة فى مجال معالجة الصور أدى إلى وجود طرق حديثة يمكن إستخدامها فى عملية تميز الأنماط.
- تستخدم تقنية القياسات الحيوية فى كثير من المؤسسات الحكومية والخاصة لضبط الحضور والإنصراف ونظم أمن المعلومات.
- توجد ثلاث فئات رئيسية تستخدم للتغلب على بعض التهديدات الامنية فى البنوك **الفئة الأولى** البطاقات الذكية، والطاقات المعتمدة، والمفاتيح، **والفئة الثانية** كلمات السر، **والفئة الثالثة** هي القياسات الحيوية.
- تختلف أساليب القياسات الحيوية التي يمكن استخدامها للتحقق من الهوية، ومن أهمها: بصمات الأصابع، وشبكية العين، والقزحية، والوجه، وهندسة اليد، والتوقيع، وطريقة استخدام لوحة المفاتيح، والصوت، والحمض النووي
- تحليل الصور وإستخلاص الخواص من الخطوات الرئيسية لتمييز الأنماط فى القياسات الحيوية بسرعة ودقة عالية.

٦-التوصيات.

للحصول على فعالية للقياسات الحيوية يمكن العمل على تطبيق التالى:

- كل القياسات الحيوية فاعلة وخصوصا بصمة العين الأكثر فاعلية ولكن يجب ان تكون الوسيلة مناسبة لتحقيق الأمان الكافى ولتحقيق ذلك يجب الاخذ في الاعتبار الاتى: -

١. الدقة.
٢. انجاز مستوى الأمان المطلوب.
٣. يمكن استخدام القياسات الحيوية بفاعلية مع البطاقات الذكية.

- يمكن زيادة امان القياسات الحيوية بعدة طرق من بينها: -

١- استخدام أكثر من نموذج للقياسات الحيوية وأكثر من طريقة وأكثر من صورة بالإضافة الى تشفير الصور المستخدمة في عملية المضاهاة.
٢- تفعيل القياسات الحيوية فى مختلف المؤسسات للتحقق من الهوية وحماية نظم وآمن المعلومات.
٣- إستخدام القياسات الحيوية مع التقنيات الأخرى مثل البطاقات الذكية فى البنوك.
٤- تطوير البرامج الخاصة بمعالجة الصور لإستخدامها فى أمن المعلومات داخل البنوك.
٥- تدريب وتأهيل العاملين داخل البنوك على البرامج الخاصة بالقياسات الحيوية لحماية وأمن المعلومات بما ينعكس إجاباً على مصلحة العمل.
٦- استخدام القياسات الحيوية فى المجالات المختلفة مثل الأمنية الوطنية، الصحية، التعليمية، الإجتماعية، والتطبيقات المالية.

٧- مقترحات الأبحاث المستقبلية:

- اجراء مزيد من الدراسات للمقارنة بين أنواع متعددة من القياسات الحيوية وذلك لوضع مواصفات فنية يمكن الارتكاز عليها عند اتخاذ قرار بشأن تامين البنوك في السنوات القادمة.
- انتاج برامج باستخدام معالجة الصور يستخدم فيها أكثر من نوع من أنواع القياسات الحيوية.
- عمل استطلاعات راى متعددة للعملاء داخل البنوك المصرية للوقوف على أفضل الطرق لتامين البنوك فى الأيام القادمة.

المراجع

اولا: المراجع باللغة العربية:

أبو حجيلة، محمد رشيد & القواعدة، محمد نواف (٢٠٠٧)، " الحماية الجزائية للمعلومات الشخصية للأفراد فى مواجهة أخطار بنوك المعلومات: دراسة مقارنة "، رسالة ماجستيرغير منشورة، كلية الدراسات الفقهية والقانونية- جامعة آل البيت، الأردن.

ابوالعز، محمد زهير محمد (٢٠١٠) " جرائم الكمبيوتر فى مجال البنوك" مجلة البحوث القانونية والإقتصاد، جامعة المنصورة – كلية الحقوق، العدد ٤٨، ص ص ٧٣٠ – ٧٩٧.

احمد، فايزة دسوقى (٢٠١٠):" القياسات الحيوية وامن المعلومات " جمعية المكتبات والمعلومات السعودية، مؤتمر البيئة المعلوماتية الامنة، الرياض، الفترة من ٦ الى ٧ ابريل ٢٠١٠.

احمد، فايزة دسوقى، (٢٠١٠) " البيئة المعلومات الأمنية: المفاهيم والتشريعات والتطبيقات " المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض ٦ – ٧ إبريل.

بنى خالد، طارق عودة& الرحاحلة، محمد ياسين، (٢٠٠٩) " مدى توفير أساليب الرقابة الداخلية لضمان أمن المعلومات المحاسبية المحوسبة فى البنوك التجارية الأردنية "رسالة ماجستير، كلية إدارة المال والأعمال، جامعة آل البت الأردن.

التمامى، شذى بنت حمد بن حسن (٢٠١٨):" مقال علمي (التحقق من الهوية باستخدام المقايس الحيوية) مركز أمن المعلومات.

حاتم، اياد (٢٠١٩):" اكتشاف منطقة راس الفخد فى الصورة فوق الصوتية للورك باستخدام تقنيات معالجة الصور الرقمية " مجلة جامعة تشرين للبحوث والدراسات العلمية –، سلسلة العلوم الهندسية، اللازقية، الجمهورية العربية السورية، المجلد ٢٣، العدد ٥.

الحاج، أم أيمن محجوب عمر& زين العابدين، جعفر (٢٠١٣) " التعرف على الأفراد من خلال بصمة الأذن بإستخدام خورزمية LDA، رسالة ماجستير كلية الدراسات العليا، جامعة النيلين – السودان.

حسين، رجب عبد الحميد (٢٠١٢) " أمن شبكات المعلومات الإلكترونية: المخاطر والحلول " عدد ٣٠، ص ١ – ١٢.

الحسينى ، هدى خليل إبراهيم & المعمورى ، على محمد نجيل (٢٠١٥) :" استخدام الشبكات العصبية الاصطناعية في تطوير دور مراقب الحسابات في اكتشاف الاخطاء الجوهرية : بحث تطبيقي في الشركة العامة للصناعات الكهربائية وشركة نصر

العامة للصناعات الميكانيكية ، مجلة دراسات محاسبية ومالية ، مجلد ١٠ ، عدد ٣١.

حنا، جبر & كيوان، رنيم (٢٠١٥):" التصنيف الآلي لتعابير الوجه باستخدام تقنيات معالجة الصورة (الخوف – الاشمئزاز – الحزن – التفاجؤ – الغضب – السعادة – التعبير الطبيعي) " مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الهندسية، اللازقية، الجمهورية العربية السورية، المجلد٣٦، العدد ٣.

خير، بشرى خير الحاج، (٢٠٠٩)، " رصد ومتابعة لندوة حول سياسة أمن المعلومات"، مجلة المصرفى، السودان، العدد ٥٤.

داود، حسن طاهر، (٢٠٠٠)، " جرائم نظم المعلومات "مركز الدراسات والبحوث، المملكة العربية السعودية، الرياض.

ذكي، عزة حازم (٢٠١٢):" نمذجة نظام برمجي للتحقق من الهوية عن طريق بصمة العين" المجلة العراقية للعلوم الاحصائية، كلية علوم الحاسوب والرياضيات، الموصل، العدد ٢٢، ص ص ١٥٠ -١٦٦.

زين العابدين، جعفر، الملحانى، بسام حسن (٢٠١٣) " التعرف على الوجه الثابت بإستخدام خورزمية الإنتشار الخلفى بالشبكة العصبية " مجلة الدراسات العليا، جامعة النيلين، كلية الدراسات العليا، مجلد ٢، ص ص ٢٧٩- ٢٩٤.

سليمان، مودة على (٢٠١١): " تمييز قزحية العين باستخدام شبكة ايلمان العصبية الاصطناعية " مجلة التربية والعلم، كلية العلوم، جامع الموصل، العراق، المجلد ٢٥، العدد ٤.

سواحل، وجدي عبد الفتاح (٢٠٠٩) " إستخدام الهندسة الوراثية فى مجال التحقق الجنائى: أساليب وتطبيقات" المركز القومى للبحوث، القاهرة.

شاكر عبد الحميد (٢٠٠٥):" عصر الصورة: الإيجابيات والسلبيات" عالم المعرفة، المجلس الوطنى للثقافة والفنون والأداب، الكويت، العدد ٣١١، يناير ٢٠٠٥، ص ص٢٢-٢٣

الشدي، لمياء فهد علي & عناب، نسرين محمد (مشرف) (٢٠١٨): "إطار امن محسن لانظمة المعلومات الكبيرة باستخدام نموزج الكشف الغامض " رسالة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية أمن الحاسب والمعلومات، قسم أمن المعلومات، تخصص أمن المعلومات.

شعبان، هند رستم (٢٠١٨): " أساسيات معالجة الصورة الرقمية في السي بلس بلس " العراق، المكتبة الإسلامية، ص ص ١-١٨.

http://solutionsproj.net/software/mo3lajasora43p.pdf

الشمالى، حسين على قاسم (٢٠١٧): " أمن وسرية المعلومات وأثرها فى الأداء المصرفى:

دراسة تطبيقية على البنوك العامة فى الأردن "، مجلة جامعة القدس المفتوحة للبحوث الإدارية والإقتصادية، جامعة القدس المفتوحة، المجلة ٢، العدد ٧، ص ص ١٨٧ – ٢٠٠.

الطمنلى، سهير فتحى (٢٠٠٩): " دور الرقابة الداخلية فى دعم وتفعيل أمن وسلامة المعلومات في البنوك الإلكترونية والخلوية "، مجالة المال والتجارة، نادى التجارة، العدد ٤٧٨، ص ص ٢٧ – ٤٨.

العابدين، جعفر زين (٢٠١٣):" التعرف على الوجة الثابت باستخدام خوارزمية الانتشار العكسى بالشبكية العصبية " مجلة الدراسات العليا – جامعة النيلين – كلية علوم الحاسبات وتقانة المعلومات، المجلد ٢، ص ص ٢٧٩-٢٩٤.

عبد الحميد، صلاح الدين محمد (٢٠١٤): " كيفية تأمين مقار معلومات المصارف على شبكة الإنترنت ضد جرائم المعلوماتية المال والإقتصاد "، بنك فيصل الإسلامى السودانى، العدد ٧٦، ص ص ١٦ – ٢٠.

عبد الرحيم، أميمة عثمان& جاه النبى، محمد عبد الرحيم (٢٠١٧): "دور نظام البصمة الآلى (ولاية الخرطوم، رسالة ماجستير فى علوم الأدلة الجنائية، جامعة الرباط الوطنى، كلية الدراسات العليا والبحث العلمى.

عبد العالى، أحمد (٢٠١٥): " البصمات البشرية المعتمدة فى البحث الجنائى " المجلة المغربية للقانون الجنائى والعلوم الجنائية، مركز الدراسات والبحوث الإنسانية والإجتماعية، العدد ٢، ص ص ١٧٥-١٨١.

عبد العزيز، سعد محمد (٢٠٠٧): " محاور إستخدام المقاييس الإحصائية فى إسناد جودة النظم البرمجية "، المؤتمر الإحصائى العربى الأول، عمان، الأردن.

عبد الفتاح، محمد لطفي (٢٠١٤): " البصمة الوراثية فرع من التكنولوجية الحيوية ودورها فى الإثبات الجنائى: دراسة علمية قانونية "مجلة جامعة ابن يوسف، جمعية إحياء جامعة إبن يوسف، العدد ١٤ -١٥، ص ص ١٠٧-١٣٠.

عمار، بعن & السمان، باسل (٢٠١١): " استخدام تقنيات معالجة الصورة في الاستخلاص الآلي للمناطق المريبة من الكبد في صور الأشعة السينية المقطعية المحوسبة "، مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الهندسية المجلد، اللازقية، الجمهورية العربية السورية، المجلد ٣٣، العدد ٣.

عوض الله، طارق أحمد& عثمان، سيف الدينم (٢٠١٣): "تأمين ماكينة الصرف الآلى: دراسة حالة لبعض البنوك التجارية السودانية "، رسالة ماجستير، معهد بحوث ودراسات

العالم الإسلامى، جامعة أم درمان الإسلامية السودان.
عيد، باسم (٢٠١٦):" استخراج الأورام السرطانية وتحديد واصفاتها في صور الرنين المغناطيسي للثدي باستخدام خوارزميات العنقدة ومعالجة الصورة " مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الهندسية، اللازقية، الجمهورية العربية السورية، المجلد ٣٨، العدد ٢.
الغثير، خالد بن سليمان& القحطافى، محمد بن عبد الله (٢٠٠٩): " أمن المعلومات بلغة ميسرة "، الرياض: جامعة الملك سعود، مركز التميز لأمن المعلومات ص ٢٤ – ٢٩.
فيلا، أسماء & شليل، عبد اللطيف (٢٠١٨): "تهديدات أمن المعلومات وسبل التصدى لها، مجلة البشائر الإقتصادية "، جامعة طاهرى محمد بشار – كلية العلوم الإقتصادية والعلوم التجارية، وعلوم التيسير، المجلد ٤، العدد ٣ ص ص ١٦٣ – ١٧٧.
قاسم، عبد الرازق محمد & الردايدة، مداد خالد (٢٠١٠): "أمن البيانات ونظم المعلومات المحاسبية فى بيئة تكنولوجيا المعلومات فى البنوك الأردنية: دراسة ميدانية "المجلة العربية للعلوم الإقتصادية والإدارية، جامعة الروح القدس – الكسليك – إتحات الجامعات العربية – جمعية كليات إدراة الأعمال والعلوم التجارية فى الجامعات المصرية، العدد ٥، ص ص ٩٠ – ١١١.
قريطم، زيد & ساعى، مريم (٢٠١٣):" تحديدُ حجمِ الورمِ ومكانِه في صور الرنين المغناطيس آلياً باستخدام تقانات معالجة الصورة " مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الهندسية، اللازقية، الجمهورية العربية السورية، المجلد ٥٣، العدد ٦.
المحمودى، فوزي محمد سالم (٢٠١٥): " أثر معالجة الصورة الرقمية على إختلاف العمل الإعلامى " مجلة الجامعى الالثقافية العامة لأعضاء هيئة التدريس، مج ٢٢ ص ص ٣٢٤ – ٢٤٣
المطيري، عادل بن ركيان & السراء، محمد بن حسن (مشرف) & السعيد، حمد بن عبد الله (مناقش) & الدعيج، علي بن عبد الرحمن (مناقش) (٢٠١٢):" استخدام تقنية البصمة العشرية مقارنة بقزحية العين في مطار الملك خالد الدولي بالرياض ودوره في دعم الأمن من وجهة نظر المبحوثين " أطروحة (ماجستير)-جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، تخصص القيادة الأمنية.
نبيل، مايكل & ألبير نادر (٢٠١٥): " أثر أمن المعلومات على أداء البنوك المصرية "، المجلة العلمية للإقتصاد والتجارة، كلية التجارة، جامعة عين شمس، العدد الرابع، ص ص

٢٥٧ – ٢٨٥.

النجـار، فـايز جمعـة (٢٠١٣):" نظـم المعلومـات الإداريـة مـدخل معاصـر مـن منظـور إدارى، الأردن، عمان دار الحامد للنشر والتوزيع.

النعيمـى، ميسـون خضـر حسـين (٢٠١١):" تتميـز بصـمة الأصـبع بإسـتخلاص الخـواص وبإعتمـاد الشبكات العصبية المحلية العراقية للعلوم الإحصائية ٢٠٤ ص ص ٦٧٥ - ٧٩٠.

ثانيا: المراجع باللغة الاجنبية:

Aitamimi, T. (2011) "Information security Risks for internet banking in Saudi Arabia ", a study submitted inpartial fulfillment of the requirements for the degree of master of scieuce in information systems at the university of Sheffield.

Al_Yaseen Sh., 2000 face Recognition using Neocognitron Neural Network, M.Sc. Thesis, Department of computer Engineering, University of Mosul.

Abod L.K., (1998), Classification of satellite image using neural network, Ph.D. Thesis, Department of physics, collage of science, university of Baghdad.

Andreas Kaplan; Michael Haenlein (2019) Siri, Siri in my Hand, who is the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence, Business

Caldera-Serrano, J. (2008). Changes in the management of information in audio-visual archives following digitization: Current and outlook. Journal of librarianship and information science, 40(1), 13-20.

christel - loic tisse، lionel mart in، lionel torres، michel robert, (2010) " person identification technique using human iris recognition, universite de montpellier، France.

Daouk, c. h, el - esber, l.a, kammoun .f .d and at ataoui .m.a. (2002) irtsrecognition electrical and computer engineering department, American university of Beirut.

EARLEY, W. (2006). Are biometrics the key to data security? EContent

(Wilton, Conn.), 29(7).

Giesing, i1se (compiler). (2003). Biometrics. - University of pretoria -pp.49-76.

Gonzalez, Rafael (2018). Digital image processing. New York, NY: Pearson. ISBN 978-0-13-335672-4.

Khalid, k.&Abdallah , R.&Elrafa , E. Elbaset , E. (2006), " Customer satisfaction with internet banking website case study on the arab bank ", The arab academy for banking and financial sciences, Jordan.

Khan, M&Barue, S. (2009) "The status and threats of information security in the Banking sector of Banglades: Polices required ", Bangladesh journal of MIS 1 (2).

Knapp, Kenneth Joseph (2005), A model of managerial effectiveness in information security: from groundad theory to empirical test, Phd dissertation, Auburn university.

Kumar, s. &pari, A. (2012), "A framework for evaluation and validation of information security policy ", International journal of computers and distributed systems 1 (3). Retrieved from .

Laroche, Gregg (2006), information and physical security: can they live together?
Information systems security.

Laudon. K &laudon, J. (2006) management des yestemesd'information .ge'me edition, edition Pearson, France.

Lim, Jee – Hae (2006), three essays on information technology and firm performance, PhD dissertation, the University of Kansas.

Micki Krause, Harold F. Tipton (2008). Information security management hand. (6-thed).USA: Mc Grow. Hill.

Muthukrishnan, arvind. Bioment rick - fingerprint, retina and pupil recognition - available at: http//:// knol .google. Com /k/ arvind - muthukrishnan/biometrics - finger - print - iris - retina - and /3ktp6efifn11p17#.-accessed at 14- /8/2009.

Nguyen. P (2010). "Automatic classification of speaker characteristics". International Conference on Communications and Electronics 2010. pp. 147–152.

Raab, C., & Mason, D. (2003). Privacy, Surveillance, Trust and Regulation The interception of communication: two studies. Information Communication & Society, 6(3), 377-379.

Rhodes, K. A. (2003). Information Security: Challenges in Using Biometrics. General Accounting Office.

Solomon, C.J.; Breckon, T.P. (2010). Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab. Wiley-Blackwell.

Subedi, P, B. (2016)," Using Likert type data in social science research: confusion, issues and challenges", International Journal of Contemporary Applied Sciences, Vol. 3, No. 2, PP 36-49.

Ula, M, Ismail, Z. &sidek, z. (2011) "A framework for the governance of information security in banking system ", journal of information assurance & cyber security, article ID 726196.

Whitman .M. &mattod .H. (2011). Principles of information security, 4th edition, Boston: cengage learning / course technology.