توليد مفاتيح التشفير لخوارزمية تشفير باستخدام المعلومات الأكثر أهمية من الواصفات البيومترية

د. محمد مصطفى حجازية*

مزيا مازن شموط**

(تاريخ الإيداع 31 / 8 / 2020. قُبِل للنشر في 18/ 11 / 2020)

□ ملخّص □

تتعرض خوارزميات التشفير للهجوم بشكل دائم بسبب ضعف مفاتيح التشفير، يقدم البحث خوارزميتين جديدتين لتوليد مفاتيح التشفير بالاعتماد على الواصفات البيومترية مطورتين عن خوارزمية أصلية تعتمد على صور لبصمة اصبع fingerprint وعلى خوارزمية التشفير AES. يقترح البحث استخلاص معلومات البصمة باستخدام طريقة mintuae ثم توليد مفاتيح التشفير اعتماداً على هذه المعلومات. تتضمن عمليات توليد المفاتيح العديد من الخطوات التي تزيد قوة التشفير مثل عمليات التبديل والخلط، تم تفادي مشاكل صور البصمة من خلال عمليات المعالجة المسبقة، كما تم استخلاص معلومات مستقلة للصور عن الشكل والاتجاه والدوران. تمكنت الخوارزميتان المعدلتان من تشفير وفك تشفير النصوص بنجاح وبأزمنة تنفيذ أقل من الخوارزمية الأصلية وبأداء أعلى كما أنها زادت رصانة الخوارزمية تجاه الهجمات حيث تم اختبار الخوارزميتين الجديدتين على صور بصمة لأشخاص مختلفين وتبين قدرة الخوارزمية على التصدي لها، ومنع كشف النص الأصلي في حال لم تكن البصمة صحيحة. تفوقت الخوارزمية الأولى المعدلة على الخوارزمية الثانية المعدلة وعلى الخوارزمية الأصلية من ناحية الزمن والأداء والتصدي للهجمات كما أنها تمكنت من فك تشفير النصوص باستخدام صور بصمة مقلوبة ومدورة ومقتطعة وصور بصمة لليد اليسرى.

الكلمات المفتاحية: التشفير، فك التشفير، خوارزمية AES، مفتاح التشفير البيومتري، خوارزمية mintuae.

* **أستاذ مساعد– قسم هندسة الحاسبات والتحكم الآلي– مدير معهد الحاسبات– جامعة تشرين– اللاذقية– سورية.**

** **طالب دراسات عليا (ماجستير)– قسم هندسة الحاسبات والتحكم الآلي– كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين– اللاذقية– سورية.**

Generation of Encryption Keys Related to Encryption Algorithm Using The Most Important Features of Biometrics

Dr. Mohamad Mostafa Hijaziah*
Mozaya Mazen Shammout**

(Received 31 / 8 / 2020. Accepted 18 / 11 / 2020)

□ ABSTRACT □

Cryptographic algorithms are under regular attacks due to poor cryptographic keys. The research introduces two new algorithms for generating cryptographic keys based on biometric descriptions developed from an original algorithm. The algorithms rely on fingerprint images and AES encryption algorithm. The research suggests extracting fingerprint features using the mintuae method and then generating cryptographic keys based on these features. Key generation operations include several steps that increase cipher strength such as switching and mixing operations, fingerprint image problems were avoided through pre-processing operations. The Extracted features from images were independent of shape, direction and rotation. The two modified algorithms were able to successfully encode and decode the texts with less implementation times than the original algorithm and with higher performance. They also increased the sobriety of the algorithm towards attacks as the algorithms were tested on fingerprint images of different people and show the algorithm's ability to address it. They prevented the decryption of the original text in case the fingerprint is not correct. The modified first algorithm outperformed the second modified one and the original algorithm in terms of time, performance, and attack. It also managed to decode the texts using inverted, rounded, partial and left-hand fingerprint images.

Keywords: Encryption, Decryption, AES Algorithm, Biometric Encryption Key, Mintuae Algorithm.

* **Associate Professor, Department of Computer and Automatic Control Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.**
** **Master Student - Computer Engineering, Department of Computer and Automatic Control Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.**

مقدمة:

يستغرق البشر وقتا طويلا لتذكر مفاتيح التشفير الخاصة بهم، كما أن خوارزميات التشفير تتعرض بشكل دائم للهجوم وبطرق مختلفة. وهذا ما دعا بالباحثين إلى استخدام الواصفات البيومترية الموجودة في جسم الإنسان والتي تعتبر مميزة وفريدة وتسخيرها في توليد مفاتيح التشفير لخوارزميات التشفير وهذا يوفر على المستخدمين عناء تذكر وحفظ مفاتيح التشفير أو حمايتها [1].

هناك العديد من الأسباب التي أدت لظهور هذه التقنية مؤخراً وهي: [3] , [2] , [1]

- عدم الحاجة إلى تذكر الكم الكبير والعشوائي من كلمات المرور والمفاتيح المستخدمة في عمليات التشفير.
- أكثر أمانا من ناحية السرقة.
- صعوبة المشاركة وإعادة التشكيل.

يقصد بتشفير البيانات عملية تحويل المعلومات من نص بسيط إلى نص غير مقروء (مشفر) بواسطة مفتاح يدعى مفتاح التشفير Encryption Key. هناك نوعان من خوارزميات التشفير حسب نوع المفتاح وهما التعمية المتناظرة symmetric encryption والتعمية غير المتناظرة Asymmetric encryption وتختلفان في كون التعمية المتناظرة تستخدم نفس المفتاح في التشفير وفك التشفير في حين أن التعمية غير المتناظرة تستخدم مفتاحين مختلفين.

هناك العديد من خوارزميات التشفير التي استخدمت في تاريخ عمليات التشفير منها خوارزميات التشفير العادية والتربيعية والأسية ولكل واحدة من هذه الخوارزميات أنواع كثيرة من الخوارزميات وفي البحث الحالي تم استخدام خوارزمية Advanced Encryption Standard (AES) وهي خوارزمية متناظرة تعتمد على البيانات الكتلية في عملية التشفير. أما من ناحية الواصفات البيومترية التي تم استخدامها فقد تم اختيار بصمة الإصبع لما لها من معلومات فريدة تميز حتى بين التوائم ولما تتمتع به من دقة تمييز عالية.

ومن الجدير بالذكر أن الواصفات البيومترية التي تستخدم في هذا المجال هي بصمة الإصبع والقزحية والبصمة الوراثية DNA والشبكية، وهناك واصفات أخرى يمكن استخدامها لكنها أقل موثوقية وأمانا وأكثر تعرضا للسرقة والانتحال مثل الوجه والأذن واليد والتوقيع. [3]

تم عرض عدد من الأبحاث في مجال التشفير بالاعتماد على الواصفات البيومترية وفيما يلي أهم هذه الأبحاث:

الدراسة الأولى:

[4] **Secured cryptographic key generation from multimodal biometrics**

تقدم الدراسة طريقة فعالة تعتمد على الواصفات البيومترية المتعددة والتي هي البصمة finger print والقزحية Iris من أجل توليد مفتاح خاص بعملية التشفير. تتألف الطريقة المقترحة من ثلاث مراحل أساسية هي استخلاص المعلومات، وتوليد القالب البيومتري الهجين المؤلف من معلومات القزحية والبصمة، وتوليد مفتاح التشفير. قام الباحثون بداية باستخلاص معلومات صور البصمة التي تمثل خطوط البصمة المميزة ونهايات البصمة المميزة والتي تختلف من شخص لآخر وتسمىminutiae ،أما بالنسبة لصورة القزحية فقد خضعت لعمليات تجزيء واستخلاص معلومات باستخدام معلومات جابور اللوغاريتمي. بعد استخلاص معلومات القزحية والبصمة تم دمجهما معا ضمن شعاع معلومات موحد وتعتمد طريقة الدمج على مبدأ العشوائية ثم التسلل أي إلحاق الشعاع الثاني في نهاية الشعاع الأول. أما المرحلة الأخيرة كانت توليد المفتاح المستخدم في عملية التشفير ذو k–bit من شعاع المعلومات المدمج للقزحية والبصمة، حيث ثم أخذ شعاع المعلومات القالب BT والمؤلف من عدة قيم [bTn ..... bT2 bT1]=BT وحيث

أن هناك مجموعة من المكونات المميزة في كل قالب BT معرفة ومخزنة ضمن الشعاع UBT، ثم بعدها يتم تحجيم الشعاع UBT الى حجم ثابت بطول المفتاح المراد توليده أي بطول .K واستخدمت هذه القيم المتبقية في الشعاع لتوليد المفتاح KB حيث: KB<< Bi mod 2 ; i=1,2,3,...k. طبقت الخوارزمية المقترحة على بيئة الماتلاب 2010 على عينات أخذت من قاعدة بيانات CASIA العالمية وتمكنت الخوارزمية من توليد مفتاح 256 بت من معلومات القزحية والبصمة المدمجة. لم يوضح الباحث مقارنة بين المفاتيح الناتجة عن أشكال مختلفة أو صور مختلفة لبصمة الشخص ذاته بحيث يوضح درجة اختلاف المفاتيح المولدة، ففي حال كان الاختلاف كبير فالطريقة تكون غير دقيقة. لم يحدد الباحث طبيعة قاعدة البيانات والحالات المختلفة لصور البصمة والتي يمكن أن تؤثر على نتيجة وقيم المفاتيح المولدة.

الدراسة الثانية:

Cryptographic key generation using fingerprint biometrics Huda Zaki [5]

استخدمت الدراسة صورة البصمة من أجل توليد مفتاح تشفير لخوارزميات التشفير من أجل زيادة الأمان وإلغاء الحاجة لحفظ مفتاح التشفير. تتألف الدراسة من جزأين أساسيين يتضمن الأول ذاكرة تملأ بالمعلومات من صورة البصمة بعد تطبيق عدد من عمليات التحسين ثم استخلاص المعلومات والتي هي عبارة عن 512 قيمة رقمية. أما الجزء الثاني فيتضمن مجموعة من مسجلات إزاحة خطية تمثل كل حركة لمنظومة مسجلات الإزاحة فيها عنوان في الذاكرة والتي أبعادها 64*8، تعطي المسجلات الثلاثة الأولى عنوان الصف في الذاكرة أما المسجلات الستة الثانية فتعطي عنوان العمود في الذاكرة والتي تخزن قيمة رقمية للبصمة. تم استخلاص معلومات البصمة التي تمثل نقاط التأثير ونهايات البصمة وخطوط البصمة. في مرحلة توليد المفتاح تم اعتماد نظام توليد عشوائي يتألف من مرحلتين تتضمن المرحلة الأولى تخزين المعلومات المستخلصة من البصمة ضمن الذاكرة EPROM ذات 256 بت وحيث تم تمثيل الذاكرة بثمانية مسجلات إزاحة حجم كل منها 64 بت ثم تم استخدام المسجلات الثمانية ذات الأطوال (11,13,9,13,11,17,13,17) وتم ملئ هذه المسجلات الثمانية بمفتاح من 8 أحرف وتم توزيع ترميز الآسكي لكل حرف على المسجلات الثمانية بحيث تم توليد مفتاح ذو 100 رقم من خلال أرقام مصفوفة EPROM المشار اليها برقم السطر والعمود الناتجين من المرحلة 3 و 4. طبقت الخوارزمية المقترحة على قاعدة بيانات FVC 2004 ضمن بيئة الماتلاب وتمكنت من توليد مفاتيح التشفير لصور البصمة. لم يوضح الباحث مقارنة بين المفاتيح الناتجة عن أشكال مختلفة أو صور مختلفة لبصمة الشخص ذاته بحيث يوضح درجة اختلاف المفاتيح المولدة، ففي حال كان الاختلاف كبير فالطريقة تكون غير دقيقة. لم يحدد الباحث طبيعة قاعدة البيانات والحالات المختلفة لصور البصمة والتي يمكن أن تؤثر على نتيجة وقيم المفاتيح المولدة.

الدراسة الثالثة:

Performance management of cryptographic key using biometric images Mohammad [6] c.nadinni 2016 ،tajuddin

استخدمت الدراسة صور شبكية العين من أجل توليد شجرة الأوعية الدموية لصورة شبكية العين والتي استخدمت لاحقا لتوليد مفتاح التشفير. أدت عملية استخدام صورة الشبكية الى توليد مفاتيح تشفير أكثر تعقيدا على المهاجمين لاكتشافها وفكها. تم بدايةً الحصول على مناطق الأوعية الدموية في صورة شبكية العين والتي تسمى شجرة الأوعية الدموية vascular tree.ثم الحصول على معلومات الشبكية وهي ثلاث أنوعا من أشعة المعلومات :K1 عدد النقاط التي تمثل نهاية الأوعية الدموية، K2 عدد نقاط التشعب (التفرع) وهي الأماكن التي يتفرع فيها الشريان الى شريانين، K3 عدد الجزر المتشكلة نتيجة تقاطع الأوعية مع بعضها البعض. تم توليد مفتاح التشفير وهو عبارة عن جداء القيم الثلاثة

للمعلومات أي: k=k1 * k2 * k3 .طبقت الخوارزمية ضمن بيئة الماتلاب وتم استخراج مفاتيح تشفير بطول 128 بت من سمات الأوعية الدموية واستخدمت هذه المفاتيح من أجل التشفير باستخدام خوارزمية.AES أظهرت النتائج قدرة المفاتيح المولدة على التشفير وفك التشفير بنجاح. أظهرت النتائج أيضا تحسن في الأداء بمقدار 3% الى 5% عن النتائج الحالية المستخدمة لتقنيات التشفير باستخدام ذات الطريقة. استخدم الباحث صور من قاعدة بيانات DRIVE و STAREالعالميتان. خوارزمية استخلاص المعلومات وتوليد المفتاح تعتمد على معلومات قد تتأثر بوجود محددات مثل تغيرات الإضاءة أو تعرض العين لأمراض تغير في طبيعة الأوعية الدموية مثل حالات النزف، إجهاد العين، التحسس وغيرها والتي تؤدي بدورها لاختلاف قيم المفتاح بشكل كبير للشخص ذاته.

الدراسة الرابعة:

[7] T.Trivedi ،R.Seshadri Efficient cryptographic key generation using biometrics

استخدم البحث في هذه الدراسة صور بصمة الإصبع finger print لتوليد مفتاح خاص بعملية التشفير، وتتضمن الطريقة المقترحة استخلاص المنطقة المهمة ROI من صورة البصمة ثم استخلاص معلومات البصمة باستخدام طريقة استخلاص نقاط التأثير ونهايات البصمة ونقاط الانفراج فيها. وفي المرحلة الأخيرة تم توليد مفتاح التشفير اعتمادا على إحداثيات نقاط التأثير المهمة في صورة البصمة. تمكنت الخوارزمية المصممة من توليد المفتاح من البصمة بخوارزمية بسيطة وسريعة لكن هناك العديد من الملاحظات على البحث حيث لم يحدد البحث طبيعة قاعدة البيانات المستخدمة، كما لم يورد أمثلة عن المفاتيح المولدة وطبيعة هذه المفاتيح.

الدراسة الخامسة:

RSA cryptographic key generation using finger print minutia Mofeed Rasheed ،Huda Zaki 2014[8]

قدمت الدراسة طريقة لتوليد مفتاح حيوي قوي معتمد على تفاصيل صورة البصمة .finger print وقامت الدراسة بتوليد مفاتيح بطول 1024 بت يمكن استخدامها في خوارزمية التشفير RSA لتوليد مفاتيح بطول 2048 بت. تعتمد الخوارزمية على تحسين تباين الصورة من أجل توضيح تفاصيل البصمة (التقاطعات والتفرعات والنهايات) وتقليل الضجيج الذي هو عبارة عن نقاط بيضاء صغيرة في البصمة. ثم استخلاص معلومات البصمة (نقاط التأثير) :Minutiaeثم تمثيل المعلومات حيث يمثل كل بيكسل نتج من المرحلة السابقة بإحداثيات x,y وقيمة سوية رمادية وتخزن كل منها في شعاع مستقل ونحصل بذلك على شعاعين F1 و F2 واحد يمثل الإحداثيات والثاني يمثل السويات الرمادية. وفي المرحلة الأخيرة يتم توليد المفتاح ويتم من خلال الشعاعين F1 و F2 لتوليد رقم أولي فريد يعتمد على ثلاث عمليات هي دمج الشعاعين F1 و F2 بشعاع واحد.S ، وتحجيم الشعاع S إلى 1024 بت فقط من خلال إهمال قيم بعض المعلومات منه والاحتفاظ بال 1024 قيمة والعملية هنا عشوائية، وعملية البعثرة أو الخلط shuffelingويتم من خلالها تطبيق خوارزمية Mongean لإضافة فكرة العشوائية لخلط قيم الشعاع الناتج. طبيعة قاعدة البيانات غير موضحة حيث لم يحدد الباحث مدى فعالية الطريقة المستخدمة في حال تغير موقع صور البصمة أو شكلها أو حجمها كون أن الطريقة تتضمن إحداثيات نقاط البصمة وهذه الإحداثيات تتغير بتغير شكل وحجم ودقة الصورة. لم يطبق الباحث أي عملية تطبيع normalization لضبط قيم أبعاد البصمة لتثبيت الإحداثيات وبالتالي ستتغير قيم المفتاح بتغير دقة الصورة أو حجمها.

الدراسة السادسة:

Generation of biometric key for use in DES Rupam Sharma[9]

قدم البحث طريقة لاستخدام صورة البصمة لتوليد مفتاح تشفير لخوارزميات التشفير يحل محل المفاتيح المولدة والمخزنة. تتضمن الطريقة المقترحة المعالجة المسبقة لصورة البصمة ثم التحويل للصيغة الثنائية يلي ذلك عملية الترقيق المورفولوجية، ثم بعد ذلك يتم استخلاص معلومات البصمة التي تمثل نقاط التأثير المهمة في الصورة وهي نقاط نهايات خطوط البصمة ونقاط الانفراجات ونقاط التقاطعات ثم يتم بعد ذلك إزالة النقاط غير المهمة والتي هي بالأصل ضجيج أو معلومات غير مهمة، لتبدأ بعد ذلك عملية توليد مفتاح التشفير المؤلف من 64 بت. في النهاية تم استخدام المفتاح المولد كمفتاح لخوارزمية DES وأظهرت النتائج العملية قدرة المفتاح المولد من البصمة على تشفير وفك تشفير عدد من الرسائل بنجاح. لم يحدد الباحث طبيعة صور البصمة المستخدمة، لم يحدد دقة النتائج التي توصل إليها، لم يوضح الباحث أي إحصائيات تدل على تغير عملية التشفير بتغير طول المفتاح وتغير قيم المفتاح بتغير البصمة.

أهمية البحث وأهدافه:

يهدف البحث إلى توليد مفاتيح تشفير لخوارزمية تشفير اعتمادا على معلومات الواصفات البيومترية (البصمة أو القزحية أو كليهما). حيث تتعرض خوارزميات التشفير للهجوم من قبل أطراف خارجية، إضافة لصعوبة تذكر مفاتيح التشفير، لذا كان من المفيد استخدام الواصفات البيومترية في بناء مفاتيح التشفير بدلاً من الطرق التقليدية الأمر الذي يجعل إمكانية كسرها أصعب وسهولة التعامل معها أكبر كون أن الشخص يحملها معه دوماً.

أهمية البحث:

إنَّ استخدام معلومات الواصفات البيومترية الفريدة من نوعها والمختلفة من شخص لآخر لتوليد مفتاح تشفير يزيد من قوة خوارزميات التشفير التي تعتبر أكثر المجالات أهمية في أمن المعلومات.

أهداف البحث:

- توليد مفاتيح تشفير لخوارزميات التشفير اعتماداً على الواصفات البيومترية ودراسة العوامل التي تلعب دوراً هاماً في تغيير قيم المفتاح مثل الضجيج وتغيرات الإضاءة والموقع واختلاف طبيعة الصور.
- تقوية خوارزمية التشفير باستخدام المعلومات المميزة في البصمة أو القزحية كمفتاح أساسي لعملية التشفير.

طرائق البحث ومواده:

يقترح البحث تطوير وتعديل الخوارزمية المقدمة من قبل البحث [7] حيث تم تطوير وتعديل طريقتين جديدتين من الخوارزمية الأصلية، بالتالي تم الحصول على 3 خوارزميات (أصلية واثنتان معدلتان) في مجال توليد مفاتيح التشفير باستخدام الواصفات البيومترية.

1 –خوارزميتا التشفير المعدلتان الأولى والثانية:

تم تعديل هذه الخوارزمية عن الخوارزمية الأصلية المقدمة من قبل البحث [7] حيث تم تعديل مراحل المعالجة المسبقة لصورة البصمة. أما التعديل الأساسي فكان في خوارزمية توليد المفتاح. يوضح المخطط (1) خوارزمية توليد مفتاح التشفير لخوارزمية التشفير AES المعدلة المقترحة.

المخطط (1) خوارزمية توليد مفتاح التشفير الأولى المعدلة المقترحة

في حين يوضح المخطط (2) التعديل الثاني المقترح للخوارزمية المقدمة في البحث [7].

المخطط (2) خوارزمية توليد مفتاح التشفير الثانية المعدلة المقترحة

1-1- العمليات ضمن مرحلة التقييس:

تهدف عملية التقييس إلى الحصول على عناصر سمات (معلومات) موحدة بحيث لا يطغى أحدها على الآخر. تتضمن عملية التقييس المقترحة المراحل التالية:

1. ضرب قيم السمات (المعلومات) المعبرة عن الانحراف المعياري والقيم المتوسطة والوسيط والقيم الصغرى والعظمى بقيمة 100 لتكبيرها لتصبح من مجال السمة الأولى التي تمثل عدد عناصر نقاط التفرع والنهايات. حيث أنها من رتبة المئات.
2. ضبط مجال الشعاع الناتج ليصبح بين 0 و 1 وذلك بتطبيق العملية الرياضية المشهورة (1):

$$X_{new}= (X-X_{min})/ (X_{max}-X_{min}) \qquad (1)$$

فبفرض لدينا شعاع المعلومات الهامة الناتج من استخلاص معلومات البصمة الأكثر أهمية:

593.0000 1.6819 9.0000 9.0000 1.00 1.6819 8.4394 8.4394 56.0000 593.0000

ناتج المرحلة الأولى هو:

1) 593.0000 168.1945 900.00 900.000 100.00 168.19 84.394 84.394 56.0000 593.000

وناتج المرحلة الثانية هو:

2) 0.6445 0.1329 1.0000 1.0000 0.0521 0.1329 0.0336 0.0336 0 0.6363

2 - مرحلة تشفير النصوص باستخدام مفتاح التشفير المولد من قبل البصمة:

يتم في هذه المرحلة تقديم مفتاح التشفير الذي حصلنا عليه من مرحلة توليد المفتاح لخوارزمية التشفير وذلك لتتمكن الخوارزمية من عملية تشفير النص الأصلي. طبعاً الخوارزمية المستخدمة للتشفير هي خوارزمية AES (Advanced Encryption Standard). دخل خوارزمية AES هو أمرين أساسيين: النص الأصلي original text ومفتاح التشفير وفي بحثنا هو المفتاح المولد من قبل بصمة الإصبع. أما الخرج فهو النص المشفر. تخضع عملية التشفير لمرحلتين أساسيتين هما مرحلة التشفير للنص الأصلي، ومرحلة جدولة المفتاح. تتضمن عملية التشفير وفق خوارزمية AES المراحل التالية [10،11،12]:

2-1 مرحلة تشفير النص:

تمر مرحلة التشفير بعشر دورات أساسية في كل منها يوجد 4 مراحل أساسية لعملية التشفير، والدخل هنا هو النص الأصلي+ المفتاح القادم من مرحلة round key أو جدولة المفتاح. أما المراحل الأساسية الأربعة هي مرحلة تعويض البايتات حيث يتم استبدال قيم البايت من النص الأصلي بقيم من جداول s-box وتعتمد عملية التبديل على قيمة البايت فالخانات الأربعة الأدنى من البايت تشكل رقما ست عشرياً يمثل رقم السطر في جدول s-box أما الخانات الأربعة الأعلى من البايت تشكل رقماً ست عشرياً يمثل رقم العمود في جدول s-box. وبمطابقة الرقمين مع جدول s-box نحصل على بايت يتم استبدال البايت الأصلي بقيمة هذا البايت القادم من جدول s-box وتكرر العملية حتى ننتهي من كامل مصفوفة النص الأصلي.

2-2 إزاحة الأسطر:

يزاح كل سطر عدد من المرات توافق رقمه فالسطر 0 لا يزاح (السطر الأول) أما السطر الثاني أو السطر رقم 1 يزاح مرة واحدة والثالث مرتين والرابع ثلاث مرات، وطبعاً عملية الإزاحة تتم من اليسار إلى اليمين.

2-3 مرحلة خلط الأعمدة:

الدخل هو المصفوفة الناتجة من مرحلة إزاحة الأسطر، حيث يتم جداء كل عمود بمصفوفة الخلط الموضحة في الشكل التالي واستبدال قيم العمود الأصلية بناتج الضرب.

2-4 إضافة دورة للمفتاح add round key:

في هذه الخطوة يلزمنا دخل مهم هو مصفوفة round key وهذه المصفوفة يتم حسابها من عملية جدولة المفتاح والتي سنتكلم عنها لاحقاً، أما الدخل الثاني لهذه المرحلة هو مصفوفة النص الأصلي الناتجة من مرحلة خلط الأعمدة. نجمع الأعمدة المتقابلة من المصفوفتين معاً ونستبدل قيمة العمود في النص الأصلي بالعمود الناتج من عملية الجمع. تكرر العملية 9 مرات أخرى فنحصل على النتيجة النهائية للنص المشفر.

2-5 key schedule:

تتضمن هذه المرحلة 10 دورات في كل منها تطبق عدة عمليات من أجل الحصول على قيمة المفتاح لدورة واحدة وتستخدم قيمة المفتاح الناتجة عن كل دورة في عملية تشفير النص ضمن مرحلة واحدة كما ذكرنا سابقاً. تتم عملية جدولة المفتاح وفق مايلي: نأخذ قيمة المفتاح الناتج من خوارزمية توليد المفتاح من بصمة الإصبع، ولدينا دخل آخر هو مصفوفة Rcon التي سنستخدمها في عملية الجدولة. حيث نبدأ الجولة الأولى للمفتاح round key1 حيث نأخذ العمود الأخير من المصفوفة W_{i-1}، ثم نجري له إزاحة من الأسفل للأعلى مرة واحدة فقط. ثم نقوم باستخدام جدول s-box من لأجل عملية تبديل قيم المفتاح الناتجة بقيم الجدول s-box. بعد ذلك نجمع قيمة العمود W_i مع العمود W_{i-4} مع العمود الرابع من مصفوفة Rcon ونضع نتيجة الجمع مكان العمود W_i وهو أول عمود من Round key 1. الآن ننتقل للعمود التالي من round key1 ويصبح العمود السابق الذي أنجزناه هو Wi-1 أما العمود الجديد يصبح هو Wi هنا فقط ننجز عملية جمع بين Wi-1 مع Wi-4 ونضع الناتج في العمود Wi، تكرر العملية السابقة للحصول على العمود الثالث ثم الرابع من Round key 1، وبذلك تنتهي الجولة الأولى round1 ويتم إرسالها لمرحلة التشفير الأولى ونبدأ الجولة الجديدة round2 نعيد الخطوات السابقة ذاتها للحصول على النتيجة الأخيرة للمفتاح.

3- أدوات البحث:

تم الاستعانة بالأدوات التالية لإنجاز البحث:

- جهاز حاسب بالمواصفات التالية:Windows 7 ultimate service pack 1, 64 bit OS, 4GB RAM
- برنامج MATLAB 2015
- قاعدة بيانات صور القزحية FCV2002 التي تم تحميلها من الموقع [13].

النتائج والمناقشة:

تم تطبيق الاختبارات العملية على قاعدة بيانات FCV2002 التي تتضمن 80 صورة للقزحية بمعدل 8 صور لكل شخص. تتضمن قاعدة البيانات بعض التحديات مثل تغيرات في الإضاءة وفي الموقع والشكل للشخص الواحد.

تم تطبيق الاختبارات على الخوارزميات الثلاثة (الأصلية والمعدلة) لتبيان الأفضل من بينها ومقارنة أداء هذه الخوارزميات سواء من ناحية الزمن أو القدرة على التشفير وفك التشفير والأمان من حيث عدم قابلية كسر الخوارزمية بوجود صور بصمة لأشخاص مخالفين.

بالنسبة للقسم البرمجي من البحث تم الاعتماد على كود خوارزمية AES [14] لكنه يتضمن عملية التشفير وفك التشفير بنفس التابع، لذا تم فصلها على تابعين مختلفين لنتمكن من اختبار إمكانية الحصول على مفتاحين متشابهين لدى طرف الإرسال والاستقبال بمجرد تواجد البصمة لدى المرسل والمستقبل. تم كذلك الاستعانة بكود خاص بعملية توليد معلومات البصمة وهي نقاط التفرع والنهايات [15]، وعدلنا عليه بحيث أضفنا مرحلة المعالجة المسبقة.

تم كتابة برنامج لعملية توليد المفتاح، وبرمجة 3 طرق مختلفة اعتماداً على بعض الدراسات المرجعية إضافة لتعديلات في بنية كل طريقة. حفظنا المفتاح الناتج عن صورة البصمة للشخص الموجود بطرف الإرسال بمصفوفة feature1 وللمفتاح الناتج عن صورة البصمة للشخص الموجود بطرف الاستقبال بمصفوفة feature2. وضمن خوارزمية التشفير لم يتم إدخال قيمة للمفتاح وإنما تم تحميلها من المصفوفة Feature1 وكذلك في خوارزمية فك التشفير لم يتم إدخال قيمة مفتاح مباشرة وإنما تم تحميلها من المصفوفة Feature2. تم تصميم واجهة رسومية يمكن من خلالها إدخال النص الأصلي والضغط على زر تشفير للحصول على النص المشفر ثم الضغط على زر فك التشفير للحصول على النص الأصلي.

1- نتائج مرحلة تحضير البصمة لتوليد مفاتيح التشفير:

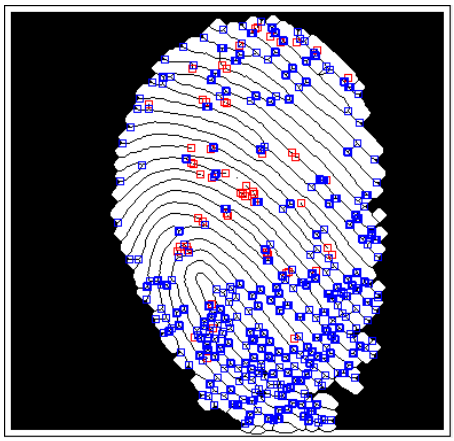
من أجل توليد مفاتيح التشفير من صور البصمة لا بد أولاً من الحصول على المعلومات الهامة من صورة البصمة. من أجل استخلاص المعلومات أو المعلومات المهمة تم تحسين الصورة أو ضبط التباين، تطبيق عملية تآكل لتوضيح خطوط البصمة وزيادة سماكتها، وفي المرحلة الأخيرة نطبق عملية الترقيق Thinning للحصول على خطوط البصمة الناعمة بعد أن تم ترميمها من قبل عملية التآكل. توضح الصورة (1) شكل البصمة قبل استخلاص معلوماتها.

الصورة (1) شكل البصمة قبل مرحلة أخذ المعلومات المهمة

تبين النتائج الموضحة في الصورة (1) أنَّ خطوط البصمة أصبحت أكثر وضوحاً مما يجعل عملية أخذ المعلومات أفضل وأدق.

2 - الحصول على المعلومات الهامة من البصمة لاستخدامها في توليد المفتاح:

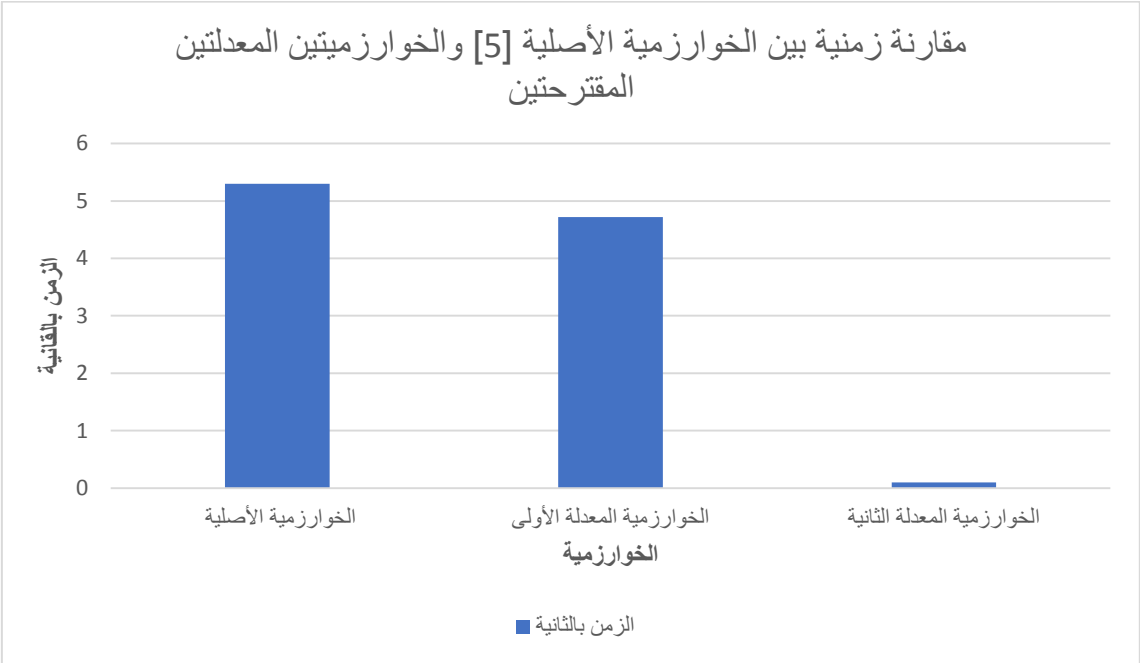
تم استخدام خوارزمية جاهزة لاستخلاص معلومات البصمة المهمة وهي طريقة استخلاص نقاط mintuae. توضح الصورة (2) ناتج تطبيق هذه العملية على صورة البصمة، حيث نقاط النهاية ending ridge باللون الأحمر ونقاط التفرع branch باللون الأزرق.



الصورة (2) ناتج الحصول على المعلومات الهامة من البصمة لتوليد مفتاح التشفير

3- نتائج خوارزميات توليد المفتاح المقترحة:

يوضح المخطط (1) مقارنة زمنية بين الخوارزميتين الأولى والثانية المعدلتين مع الخوارزمية الأصلية.



المخطط (1) مقارنة زمنية بين الخوارزميتين الأولى والثانية المعدلتين مع الخوارزمية الأصلية

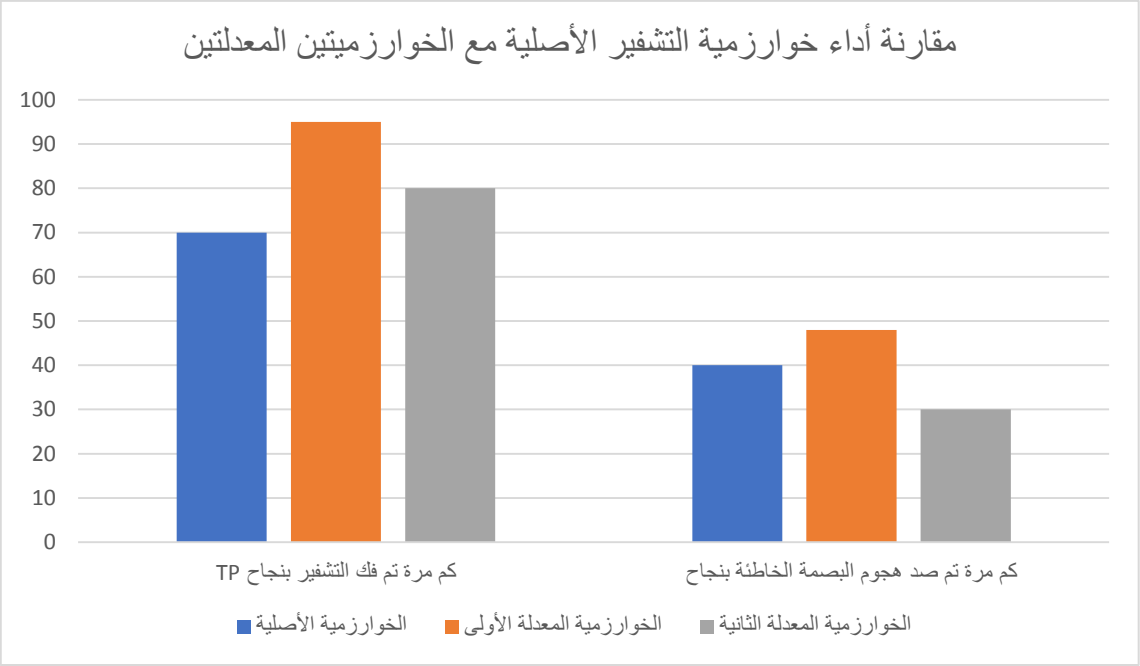
حيث يوضح المخطط (1) أنَّ الخوارزمية المعدلة الثانية هي الأقل زمناً وذلك لأنها تعتمد مراحل أقل من الخوارزمية المعدلة الأولى، كما يمكن أن نلاحظ أن الخوارزمية المعدلة الأولى استغرقت زمناً أقل من الخوارزمية الأصلية والسبب يعود لوجود حلقات تكرارية في الطريقة الأصلية تجعل زمن توليد المفتاح أكبر.

توضح الصورة (3) مقارنة بين الخوارزميتين المعدلتين الأولى والثانية والأصلية من ناحية الأداء.

البصمة المستخدمة في التشفير	البصمة المستخدمة في فك التشفير	النتيجة في الخوارزمية الأولى المعدلة	النتيجة في الخوارزمية الثانية المعدلة	النتيجة في الخوارزمية الأولى الأصلية
	 بصمة أخرى لنفس الشخص (مقلوبة)	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	لم يتمكن البرنامج من فك التشفير لأن الخوارزمية تتأثر بتغيرات الاتجاه
	 بصمة أخرى مدورة	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	لم يتمكن البرنامج من فك التشفير لأن الخوارزمية تتأثر بتغيرات التدوير
	 بصمة لشخص آخر	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم
	 بصمة أخرى لنفس الشخص	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح
	 بصمة لشخص آخر	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم	تم فك التشفير ولم تنجح الخوارزمية في التصدي للهجوم	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم

	 بصمة أخرى لنفس الشخص	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح
	 بصمة أخرى لنفس الشخص	لم يتمكن البرنامج من فك تشفير النص المشفر.	تمكن البرنامج من فك تشفير النص المشفر بنجاح	لم يتمكن البرنامج من فك تشفير النص المشفر.
	 بصمة أخرى لنفس الشخص غير كاملة	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	لم يتمكن البرنامج من فك تشفير النص
	 بصمة أخرى لنفس الشخص غير كاملة	لم يتم فك التشفير ونجحت الخوارزمية في التصدي للهجوم	تم فك التشفير ولم تنجح الخوارزمية في التصدي للهجوم	تم فك التشفير ولم تنجح الخوارزمية في التصدي للهجوم
	 بصمة اليد اليسرى	تمكن البرنامج من فك تشفير النص المشفر بنجاح	تمكن البرنامج من فك تشفير النص المشفر بنجاح	لم يتمكن البرنامج من فك تشفير النص

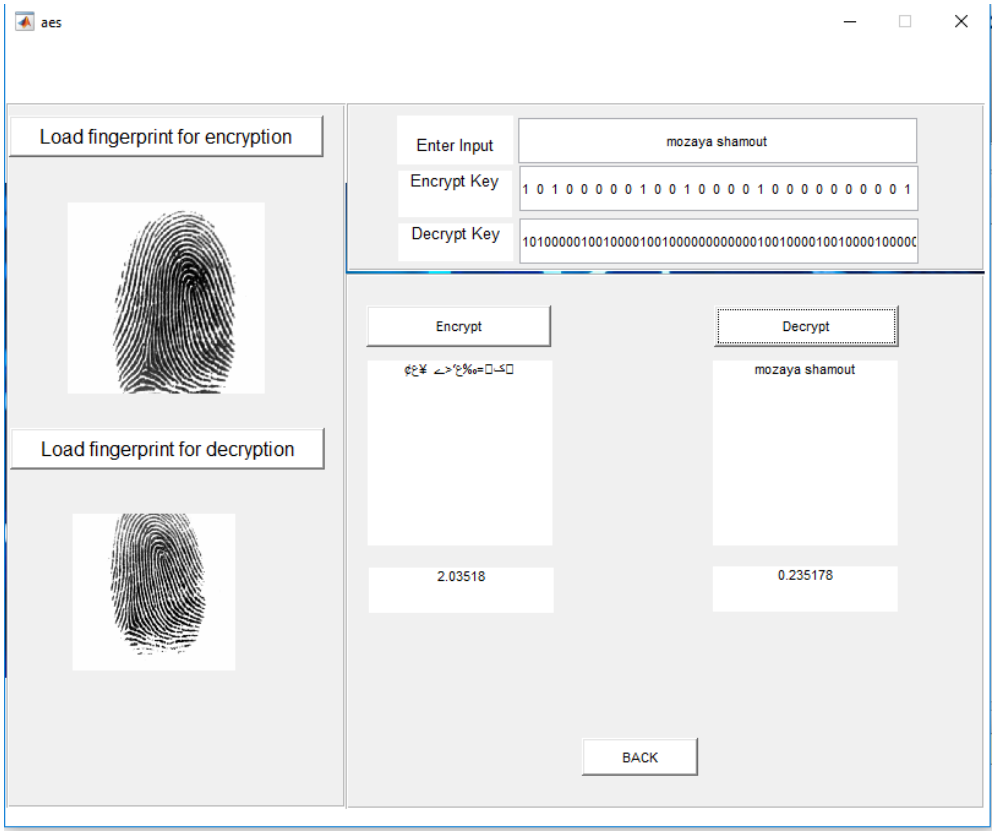
الصورة (3) مقارنة الأداء بين الخوارزميتين الأولى والثانية المعدلتين مع الخوارزمية الأصلية



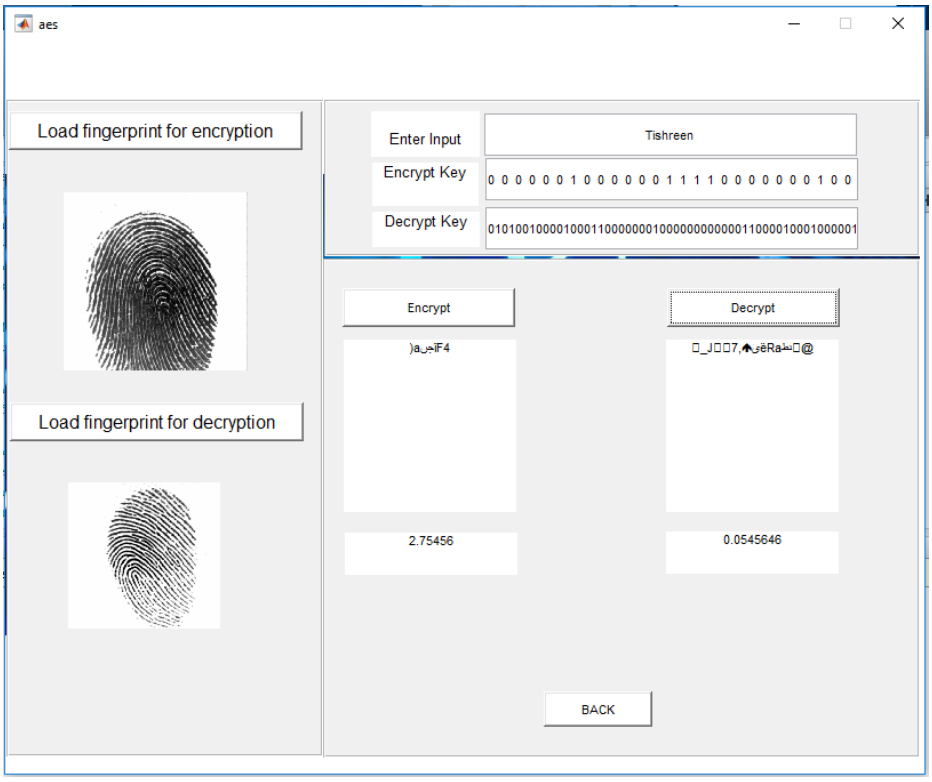
المخطط (2) مقارنة الأداء بين الخوارزميتين الأولى والثانية المعدلتين مع الخوارزمية الأصلية

يوضح المخطط (2) تفوق الخوارزمية الأولى المعدلة من حيث الأداء (فك تشفير النصوص لدى تقديم بصمة لنفس الشخص بنجاح، أو التصدي للهجوم وكشف البصمات المزورة عند تقديم بصمة لشخص مختلف)، أما بالنسبة للخوارزمية الثانية المعدلة فهي أفضل من حيث الأداء لكنها سيئة من ناحية التصدي للهجوم. مقارنة بالخوارزمية الأصلية تتفوق الخوارزمية المعدلة الأولى من حيث الأداء ومن حيث الزمن ومن حيث التصدي للهجمات كما أنها تعمل في ظل ظروف التغيرات مثل الاتجاه والدوران والإضاءة على عكس الخوارزمية الأصلية.

توضح الصورتان (4,5) مثالان عن اختبار تشفير وفك التشفير باستخدام الخوارزمية الثانية المعدلة بصمتين لنفس الشخص على الواجهة الرسومية (الصورة (4)) وباستخدام بصمتين لشخصين مختلفين للتحقق من إمكانية التصدي للهجوم (الصورة (5))، حيث تم تصميم الواجهة من أجل تسهيل التعامل مع عمليات التشفير وفك التشفير.



الصورة (4) ناتج فك تشفير نص أصلي باستخدام بصمة تعود لنفس الشخص



الصورة (5) ناتج فك تشفير نص باستخدام بصمة لشخص آخر

الاستنتاجات والتوصيات:

يقدم البحث خوارزميتين جديدتين لتوليد مفاتيح التشفير مطورة من خوارزميتين أصليتين تعتمد الخوارزميات على صور البصمة fingerprint حيث يتم الحصول على معلومات البصمة باستخدام طريقة mintuae ثم توليد مفاتيح التشفير اعتماداً على هذه المعلومات. تتضمن عمليات توليد المفاتيح العديد من الخطوات التي تزيد قوة التشفير مثل عمليات التبديل والخلط، ولتفادي مشاكل صور البصمة من خلال عمليات المعالجة المسبقة، ولحل مشاكل استخدام صور مختلفة لبصمات الشخص نفسه من خلال استخلاص معلومات مستقلة عن الشكل والاتجاه والدوران.

تمكنت الخوارزميات المصممة من تشفير وفك تشفير النصوص بنجاح وبأزمنة تنفيذ أقل من الخوارزمية الأصلية وبأداء أعلى كما أنها زادت رصانة الخوارزمية تجاه الهجمات حيث تم اختبار الخوارزميات على صور بصمة لأشخاص مختلفين وتبين قدرة الخوارزمية على التصدي لذلك ومنع كشف النص الأصلي في حال لم تكن البصمة صحيحة. تفوقت الخوارزمية الأولى المعدلة على الخوارزمية الثانية المعدلة وعلى الخوارزمية الأصلية من ناحية الأداء والتصدي للهجمات كما أنها تمكنت من فك تشفير النصوص باستخدام صور بصمة مقلوبة ومدورة ومقتطعة وصور بصمة لليد اليسرى.

يوصي الباحث بما يلي:

1- إضافة فكرة لكل الخوارزميات تتضمن استخدام رقم سري يضاف للخوارزمية ويتم استخدام هذا الرقم في فك التشفير بحيث حتى لو تمكن المهاجم من الحصول على بصمة الشخص لن يستطيع فك تشفير النص إلا في حال تمكن من معرفة الرقم المستخدم في عملية فك التشفير.

2- إضافة واصفات بيومترية أخرى واستخلاص معلومات هجينة مركبة من كلا الواصفتين لزيادة قوة الخورازميات.

References:

[1] Umut Uludge, Sharath Pankanti, Salil Parbhakar and Anil K.jain, "Biometric Cryptosystems: Issues and Challenges", IEEE, 18 May 2004.

[2] Rashi Bais, K.K.Mehta," Biometric Parameter Based Cryptographic Key Ganeration", International Journal of Engineering & Advanced Technology, (IJEAT) ISSN: 2249-8958, Vol (1), Issue (5), June 2012.

[3] Seif Aldin Abdulkarim, "Building an Information Security system with Network Application Based on Generating Biometric Key (from fingerprint)", Tishreen University, 2016.

[4] Jagadeesan A, Duraiswamy K," Secured cryptographic key generation from multimodal biometrics" , International Journal of Computer Science and Information Security , Vol. 7, No. 2, 2010, pp:28-37.

[5] Zaki H," Cryptographic key Generation Using Fingerprint Biometrics ". J.Thi-Qar Sci, Vol.5 (2),2015, pp:75:79.

[6] Tajuddin M, Nandini C," Performance Measurement of Cryptographic Key using Biometric Images ", International Journal of Electrical Sciences & Engineering, 2016, pp:13-18.

[7] Seshadri R, Trivedi T," Efficient Cryptographic Key Generation using Biometrics , Int. J. Comp. Tech. Appl., Vol 2 (1),2011, pp:183-187.

[8] Rashid M, ZaKi H, "RSA Cryptographic Key Generation Using Fingerprint Minutiae , Iraqi Commission for Computers & Informatics", Vol (1) Issue (1), 2014.

[9] Sharma R, "Generation of Biometric Key for Use in DES ", international journal of science issues,Vol (9)Issue (6), 2012, pp:312-315.

[10] Jawahar Thakur, Nagesh Kumar, " DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis", International Journal of Emerging Technology and Advanced Engineering, Vol(1) Issue(2), 2011.
[11] Sunil V. K. Gaddam and Manohar Lal," Efficient Cancellable Biometric Key Ganaration Scheme foe Cryptography". International Journal of Network Security, Vol.11, No (2),2010.
[12] Dorothy Elizabith, Robling Denning," Cryptography and Data Security", ISBN 0-201-10150-5, Addison-Wesley, 1982.