نظام التشفير الرقمي لحماية سرية البطاقات

إعداد

ديالا رشيد صبحي إبراهيم

المشرف

أ.د. عبد الفتاح التميمي

المشرف المشارك

د. أيمن عارف عبد الله

الملخص

هذه الأطروحة تقدم نظرة عامة شاملة لمشكلة حفظ المعلومات الإلكترونية من خطر قراصنة المعلوماتية خاصة أولئك الذين لديهم معرفة تامة واسعة في علم القرصنة الإلكترونية، وذلك من خلال المعلومات الموجودة في الصور وبناء نظام أمني من أجل إثبات هوية الشخص الذي يقوم باستعمال الحاسب الآلي لمعرفة إذا كان يملك صلاحية للحصول على المعلومات الموجودة في هذه الصور. إن طريقتنا المنهجية تعتبر حل قوي وفعال لحل هذه المشكلة وذلك لكونها تعتمد على مستويين اثنين من الأمان أولاهما التشفير المرئي (Visual Cryptography: VC) حيث يعتبر نظام تقاسم السرية البصري أحد أنواع أنظمة تقاسم السرية المتبعة والذي يتميز بخاصية استعادة الصورة السرية مرئياً بالعين البشرية دون الحاجة لإجراء أي عمليات حسابية بواسطة الحاسب الآلي. وبالإضافة إلى هذه الطريقة استعملنا المستوى الثاني من الأمان والذي يعتبر تقنية حيوية وهي برنامج

التعرف على الوجوه (Face Recognition) وبالأخص الجزء المهم الخاص بتمييز الوجوه (Face Detection) والتي تعتبر الخطوة الأولى في برنامج التعرف على الوجوه مع أنه لا يعتبر أسلوب مباشر ودقيق لتمييز الوجوه وذلك لوجود متغيرات تؤثر في مظهر الصورة والتي قد تكون ناتجه من عدة عوامل نذكر منها على سبيل المثال تعدد الوضعيات التي تؤخذ فيها الصورة، إخفاء الوجه أو جزء منه، التغيير في مستوى الإنارة، الزاوية التي أخذت منها الصورة وكذلك تعابير الوجه عند التقاط الصورة. هذه التقنية استعملناها لفحص الصور المستعادة الناتجة عن تكدس وتراكم الصور المجزأة من الصورة الأصلية فوق بعضها البعض لتكون صورة مطابقة للأصل.

النظام الأمني المقترح بنا أحرز نتائج هامة، ففي المقام الأول أخذنا حالتين وعند إيجاد المعدل النسبي (Ratio Rate: RR) لعدد الصور التي تم التعرف عليها من الصور التي تم فحصها والزمن اللازم للتعرف عليها. فعند مقارنة نسبة الصور المجزأة مع الصور المستعادة فقد حققنا معدل نسبي يعادل 0.98 في زمن قدره 23 ثانية. هذا يعني أننا تمكنا بسهولة من كشف الصور المستعادة وذلك بعد تكدس أو تراكم الصور المجزأة من الصورة الأصلية فوق بعضها البعض. من جهة أخرى أجرينا مقارنة بين الصور المجزأة والصور الأصلية وذلك باستعمال خوارزمية (Eigenfaces) حيث أن هذه الخوارزمية تستطيع أن تكشف وتتعرف على الوجوه بسهولة وسرعة مرضية وذلك بتقسيم الوجوه إلى مجموعات صغيرة من الملامح والمميزات وحيث أن (Eigenfaces) تشكل المكونات الرئيسية لصور تعليمية تسمى مجموعة التدريب. التعرف على الوجوه يحصل بعمل صورة جديدة تسمى مجموعة الاختبار. وباستعمال هذه الخوارزمية حصلنا على معدل نسبي (RR) 0.41 في 8 ثواني. كذلك استعملنا خوارزمية أخرى للتعرف على الوجوه لنرى مدى التأثير على نظامنا الأمني وهي خوارزمية تحليل المكونات الرئيسية (PCA) والتي تعتمد على مفهوم نظرية المعلومات حيث أنها استراتيجية ملائمة للتعرف على الوجوه وذلك لقدرتها على تمييز التباين في الوجوه البشرية. وجدنا باستعمال هذه الإستراتيجية لإستعادة الصورة الأصل من الصور المجزأة أن المعدل النسبي (RR) يعادل 0.53 في زمن مقداره 8 ثواني. وبناءاً على ذلك فإن خوارزمية تحليل المكونات الرئيسية (PCA) قد أعطت نتائج أفضل مما يجعل استخدامها أفضل من خوارزمية (Eigenfaces) لإستعادة الصورة الأصل من الصور المجزأة.

معظم العمل الذي تم إنجازه في التشفير المرئي يمثل نظام تقاسم السرية الملونة لبناء نموذج الألوان (RGB) حيث أن الصور السرية الأصلية تتجزأ إلى جزئين وللحصول على الصورة المستعادة والتي تطابق الصورة السرية يجب تكدس أو تراكم الصور المجزأة فوق بعضها البعض بعد ذلك قمنا

بإستعمال خوارزمية التعرف على الوجوه لفحص الصورة المخزنة المتكونة للتأكد من أن المستخدم الذي سيحصل على الصورة قانوني ومصرح له بذلك أو لا وذلك بمقارنة الصور المستعادة أو المجزأة مع الصور الأصل. وبهذا تمكنا من رفع كفاءة وفعالية ودقة نظامنا مما يجعله صالحاً للتطبيق في مجالات تتطلب مستوى عالي من السرية والأمان مثل المجالات العسكرية والصناعة المصرفية أو البنكية ومجال المجوهرات وغيرها من المجالات الأخرى.