الفصل الحادي عشر

أمن البيانات وحمايتها للصور الطبية

Data security and for medical

د. ايجيني لم — Dr. Eugene Y. S. Lim

مستشفى الأمير ألفريد الملكية — Royal Prince Alfred Hospital and

جامعة سيدني — University of Sydney

(١١،١) مقدمة

(١١،١،١) الخلفية

هناك التزامات أخلاقية قانونية على موفري الرعاية الصحية وهي أن يحافظوا على خصوصية وسرية معلومات المرضى، التي قد تحتوي على بعض من أكثر المعلومات أهمية عن هؤلاء الأشخاص [1]. بصرف النظر عن مميزات السجل الإلكتروني الطبي electronic medical record, EMR، فإن هناك فرصة أعلى لإفشاء هذه المعلومات على العامة بالمقارنة بالأشكال الأخرى مثل السجلات المدونة في الأوراق [2]. إن الشبكات السريعة وأدوات المعالجة للبيانات تسمح بالبحث في البيانات الكبيرة الحجم واسترجاع وتفعيل نقل البيانات المعلنة. إن الاتصال السهل بأنظمة الشبكات يزيد من مخاطر إفشاء المعلومات سواء كان متعمداً أو غير متعمد. إن المستوى الحقيقي لانتهاكات الأمان في أنظمة الرعاية الصحية الحالية ليس ذو أهمية عالية حتى الآن ولكنه قوي بحيث ترفع معه درجة الأهمية [3, 4].

في مثل هذا الوسط، فإن الخطورة الأساسية المصاحبة للمعلومات الطبية هي الإفشاء بالمعلومات لأي طرف غير مسموح له بذلك مما قد ينتج عنه سوء استخدام لهذه المعلومات. إن التغير غير المصرح به لهذه المحتويات سواء كان مقصوداً أو غير مقصود قد يؤدي إلى التشخيص الخاطئ وبعض النتائج الأخرى الخطيرة. إن أمان المعلومات الطبية يكون محميا بالقانون والأخلاق العالية، كما أن قانون حسابات واعتمادية التأمين الصحي Health insurance portability and accountability act, HIPAA الذي قدم أخيراً عن طريق الحكومة الأمريكية قد أدى إلى تطوير قانون قومي للأمان، ومعايير الأمان، ومعايير المعاملات الإلكترونية لتقليل الانتهاكات والإفشاء الخاطئ للمعلومات الطبية. هناك ثلاثة جوانب للأمان يُمكن أن تتضح عند التعامل مع الصور الطبية: السرية، والاعتمادية (السلامة، التوثيق)، والإتاحية أو التوافر [6] وكلها يُمكن تحديدها كما يلي:

السرية confidentiality تهدف إلى التأكد من أن الأشخاص المخولين فقط هم الذين يتصلون بهذه المعلومات.

الاعتمادية ولها جانبان: السلامة Integrity والمقصود منها أن المعلومات لم يتم عليها أي تغيير عن طريق الخطأ سواء بالتراسل أو المستخدمين غير المصرح لهم، والتوثيق authentication ويقصد به التأكد من أن البيانات أو المعلومات يتم تحديدها بطريقة صحيحة (بمعنى أنها من المصدر الصحيح وأنها تتبع المريض الصحيح). الإتاحية availability تعني أن المعلومات يتم استخدام ها عن طريق المستخدمين المخولين بذلك في ظروف الاتصال والممارسة.

إن التوزيع الفعال والاتصالات للصور الطبية خلال موفري الخدمة الصحية أصبحت على درجة كبيرة من الأهمية، كما أن شبكات الرعاية الصحية تعتبر مكوناً أساسياً في توفير الرعاية العلاجية بالتكلفة المناسبة. لتوفير

التبادل والاتصالات الفعالة للبيانات، فإن استخدام قنوات الشبكات العامة مثل الإنترنت يكون أمراً لا مفر منه. أخيراً، تم اقتراح العديد من أنظمة توزيع الصور التي تستخدم الإنترنت في المؤلفات، مثل نظام توزيع الصور الطبية المعتمد على الإنترنت وعن بعد [11-7]. هذه الأنظمة سيكون لها فرصاً عظيمة نتيجة كفاءتها التكليفية وسهولة الاتصال بها.

واحد من الاعتبارات المهمة عند تنفيذ أي نظام تصويري شبكي يستخدم شبكة الإنترنت هو أن بيانات الصور من الممكن أن تكون عرضة للاتصال غير المصرح به، والإفشاء، والتغيير. معظم أنظمة أرشيف الصور والاتصالات الإكلينيكية picture archive and communication system, PACS [12] تستخدم معيار التصوير الرقمي والاتصالات في الطب digital imaging and communication in medicine, DICOM كنظام قياسي للصور الطبية. يوجد هناك الآن عدد من مقاييس الأمان في الـ PACS والـ DICOM، مثل التراسل المشفر، والحائط الناري firewall، وكلمات المرور passwords، والمفاتيح العامة والخاصة، وكلها توفر الحماية المعقولة للتخزين والتراسل. وعلى الرغم من ذلك، فإن سرعة الشبكات والحاسبات تزداد بسرعة مما يمثل مخاطر تأمينية للوسط الطبي. إن السرعات العالية لمعالجة البيانات تزيد من فرص التعرض لهجوم القوي الغاشمة ومختلف الشفرات المحللة [14]، كما أن الشبكات الممتدة الواسعة المساحة تولد إمكانية للوصلات غير المصرحة على شبكات الرعاية الصحية مما ينتج عنه هجوم مثل التنصت. إن معظم أدوات الأمان يكون لها حدود أيضاً، كما أن ربط الطرق المختلفة من الممكن أن يزيد من أمان البيانات [15]. في هذا الفصل سنعرض باختصار لبعض طرق الأمان المستخدمة حالياً في الحياة العملية وبعض الطرق الجديدة أيضاً لحماية الصور الطبية.

(١١،١،٢) نظام التشفير والعلامة المائية الرقمية

نظام التشفير أو السايفر cipher يكون عبارة عن دالة حسابية تستخدم في عملية التشفير وفك التشفير. في الوقت الحالي يعتبر التشفير هو الحماية أو الأمان لأنظمة المعلومات الطبية مثل الـ DICOM، وذلك باستخدام التوقيع الإلكتروني والترميز لتحسين الأمان [13]. أنظمة التشفيرتكون قادرة على توفير السرية باستخدام التشفير وأما حماية المحتويات فيضمن السلامة والخصوصية باستخدام التوقيع أو البصمة الإلكترونية. على الرغم من ذلك، فما زالت هناك بعض جوانب الضعف في أنظمة التشفير، فمثلاً، ليست هناك حماية مضمونة بعد فك التشفير باستخدام المفتاح الشرعي (وهي الطريقة الأكثر شيوعاً في التوزيع غير القانوني لمحتويات الوسائط المتعددة) [6]. لذلك؛ فإن طريقة التوقيع الإلكتروني تعتبر حلاً جيداً للكشف عن التعديلات المقصودة أو غير المقصودة للمحتويات الرقمية.

تعتبر العلامة المائية الرقمية طريقة لإخفاء معلومات مشفرة في بيانات رقمية بحيث تكون المعلومات غير مرئية أو غير محسوسة، ولكنها يُمكن فك شفرتها وإظهارها عن طريق الشخص المخول لذلك [16]. من المفروض أنه من

الصعب على الشخص غير المخول أن يزيل المعلومات المخبأة بدون الخلاص من البيانات الأساسية. تشتمل تطبيقات العلامة المائية الرقمية على حماية حقوق الطبع، والتوثيق، والتزييل، والتتبع للتوزيع غير الشرعي، والاتصالات الآمنة، وكل واحد من هذه التطبيقات له متطلبات مختلفة [18]. فمثلا، حماية الملكية الفكرية تتطلب علامة مائية قوية [17]، بينما يتطلب التوثيق لعلامة مائية هشة أو شبه هشة أو ضعيفة [18]. العلامة المائية القوية هي الطريقة التي تكون فيها العلامة المائية المخفية يجب أن تبقى كما هي بعد أي عملية معالجة يتم تطبيقها على البيانات الأساسية بما في ذلك عمليات الضغط والتحويلات الهندسية. هذه القوة تكون مفيدة في الحماية الفكرية حتى يُمكن الحفاظ على ملكية المحتويات. العلامات المائية الهشة أو شبه الهشة هي طريقة لإخفاء العلامات المائية القابلة للكسر على محتويات الصورة بحيث أن أي معالجة للصورة من الممكن أن تدمر العلامة المائية. إن العلامة المائية المكسرة تكون مازالت قابلة للاستخدام للتوثيق مع تحديد مكان التغيير.

الشكل رقم (١١.١) يبين الفرق بين أنظمة التشفير والعلامة المائية الرقمية. من الفروق المهمة أن أنظمة التشفير تخفي الصورة الأساسية من الاتصال غير المخول عن طريق تشفيرها بينما العلامة المائية الرقمية تخفي معلومات سرية في خلال محتويات الصورة الأصلية نفسها والتي يُمكن استخلاصها من الصورة للتحقق منها.

(١١،٢) نظرة عامة على أنظمة التشفير Cryptography

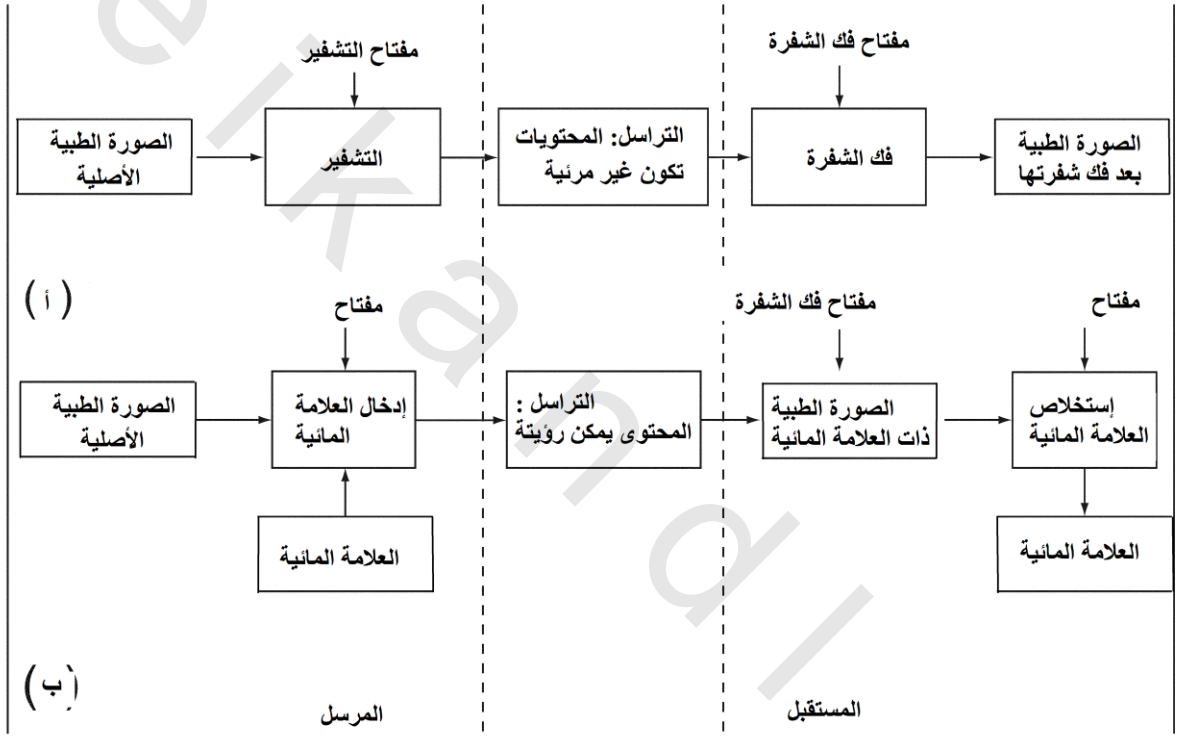
التشفير cryptography مأخوذة من الكلمة اليونانية crypto والتي تعني الإخفاء و graphein والتي تعني الكتابة، والكلمة كلها يقصد بها الكتابة السرية. تقوم عملية التشفير بتحويل الرسالة النصية إلى شفرات نصية باستخدام خوارزم معين للتشفير. العملية العكسية وهي فك الشفرة أو decryption هي عملية استخلاص و الحصول على النص الأصلي. على العموم هناك نوعان من خوارزمات التشفير، التشفير بالمفتاح المتماثل symmetric (الخاص)، والتشفير الغير متماثل asymmetric (العام).

(١١،٢،١) التشفير بالمفتاح المتماثل

يعتمد التشفير بالمفتاح المتماثل (ويسمى أيضاً المفتاح الخاص) على مفتاح مشترك معروف فقط لدى طرفي الاتصال. من خوارزمات التشفير المتماثلة الشهيرة، خوارزم تشفير البيانات القياسي، وخوارزم تشفير البيانات الدولي [19]، والـ RC5 [20]، وخوارزم تشفير البيانات القياسي المتقدم.

إن مستوى السرية التي تحققها الخوارزمات يعتمد على سرية المفتاح. كل من طرفي الاتصال لابد أن يتوافقا على المفتاح السري قبل إرسال الرسالة. هذا النوع من الخوارزمات يحقق الخصوصية في الرسالة، ولكن عيب أساسي في هذا النوع من الخوارزمات هو أن أي رسالة يُمكن مقارنتها عند الكشف عن المفتاح أو اعتراضه، كما أن هناك موضوعاً آخر وهو استخدام المفتاح السري في أي وسط شبكي. عندما يكون هناك أكثر من قناتي اتصالات أو

أكثر من عقدة فإنه يفترض أن كل اثنين من المتراسلين سيستخدم مفتاحاً منفصلاً، وهذا سيتسبب في تكلفة حسابية عالية عندما يكون هناك عدد كبير من أزواج المتراسلين، وهذا يكون طبيعياً في الوسط الطبي. وعلى الجانب الآخر، فمن مميزات هذا الخواريزم على خواريزم المفتاح العام أن خواريزم المفتاح الخاص يتطلب حجماً صغيراً للمفتاح لنفس مستوى السرية المطلوب. وبالتالي فإن الحسابات من الممكن أن تكون سريعة، ومتطلبات الذاكرة تكون أصغر، وهذا بالطبع يكون مفيدا في الاتصالات التي بها أعداد صغيرة من المستخدمين.



الشكل رقم (١١،١) (أ) نظام تشفير للصور الطبية، يتم إخفاء محتويات الصورة أثناء التراسل. (ب) العلامة المائية المخفية، يتم التعامل مع الصورة أثناء التراسل، ولكن هناك معلومات سرية غير مرئية أو مخفية داخل الصورة.

(١١،٢،٢) التشفير بالمفتاح الغير متماثل

يستخدم التشفير بالمفتاح غير المتماثل (يسمى أيضاً العام) مفتاحين مختلفين: مفتاحاً عاماً ومفتاحاً خاصاً. المفتاحاً العام يكون متاحاً لأي شخص، وأما المفتاح الخاص فيكون معروفاً فقط لمالك هذا المفتاح. يُمكن للمرسل أن يشفر الرسالة باستخدام المفتاح العام للمستقبل، حيث يُمكن فك تشفير هذه الرسالة باستخدام المفتاح الخاص للمستقبل فقط. إن التشفير بالمفتاح العام لا يتطلب مفتاحاً مشتركاً بين كل من المتراسلين؛ ولذلك فإنه يحل مشكلة

توزيع المفتاح على شبكات الاتصال، ولكن عملية التشفير وفك الشفرة تكون في العموم أبطأ بكثير عن التشفير بالمفتاح المتماثل. إن حجم المفتاح في التشفير بالمفتاح العام ينمو ليصبح كبيراً جداً؛ مما يتطلب معالجة حسابية أكبر وحجم أكبر من الذاكرة.

عندما نبحث عن الأداء الأفضل، فإن استخدام المفتاح المتماثل يكون أفضل من المفتاح غير المتماثل. لكي نحصل على التوازن بين الأداء وفعالية التوزيع، فإنه يجب استخدام خليط من التشفير بالمفتاح المتماثل والمفتاح غير المتماثل. هناك مفتاح عشوائي مؤقت يسمى مفتاح الجلسة أو الدورة session key يُمكن استخدامه. يتم استخدام مفتاح الدورة لتشفير الرسالة، وبعد ذلك يتم تشفير مفتاح الدورة باستخدام مفتاح المستقبل العام. يتم إرسال مفتاح الدورة المشفر بالمفتاح العام مع الرسالة المشفرة إلى المستقبل، حيث يُمكن استخلاص مفتاح الدورة باستخدام المفتاح الخاص بالمستخدم، وبعد ذلك يتم فك الرسالة باستخدام مفتاح الدورة. في الصور الطبية، ونتيجة لكبر حجمها، فإن هذه الطريقة المركبة يُمكن أن تحسن من الأداء والأمان في إدارة المفاتيح.

(١١،٢،٣) دالة البعثرة Hash للتشفير

تأخذ دوال البعثرة أي طول من البيانات المدخلة (مثل محتويات الصور) وتولد سلاسل أحرف ثابتة الطول. يُمكن لهذه السلسلة المولدة أن تلحق مع البيانات المدخلة أثناء التراسل للكشف عن الأخطاء. هذه السلسلة تسمى أيضاً ببتات التكافؤ أو التساوي parity عندما تكون سلسلة ثنائية. بمقارنة سلسلة الباريتي (أو الحصيلة) الموجودة في البيانات المرسلة مع محصلة الرسالة الملحقة (يسمى أيضاً المجموع الاختباري) فإنه يُمكن اختبار الخطأ. تستخدم هذه الطريقة على العموم في اختبار الأخطاء العشوائية المضافة بسبب الضوضاء على الرسالة أثناء التراسل. على الرغم من ذلك فهناك تهديدات لهذه الطرق مثلاًعندما يعترض مهاجم ماكر البيانات المرسلة، ويعدلها، ويعيد إرسالها بحصيلة يعاد حسابها للرسالة المعدلة.

في العادة يتم استخدام دوال البعثرة هاش التشفيرية التي تستخدم التشفير بالمفتاح المتماثل أو التي تستخدم التشفير بالمفتاح غير المتماثل في عمليات التوثيق authentication. عمليات التوثيق تشبه عمليات اختبار الأخطاء، ولكنها تتأكد من أن مصدر البيانات تم التعرف عليه بدقة. في العادة يتم عمل التوثيق في نفس الوقت كاختبار سلامة. إن الناتج لقيمة البعثرة هاش التشفيرية (بمعنى السلسلة الثنائية) يعرف على أنه التوقيع الرقمي.

لإنتاج أي توقيع رقمي، يتم حساب خلاصة أي رسالة دخل M باستخدام دالة البعثرة هاش H(x). بعد ذلك يتم تشفير الرسالة الملخصة 'M باستخدام مفتاح المرسل، وهذا التشفير من الممكن أن يكون خاصاً أو عاماً. هذا التشفير للبعثرة يمنع المهاجمين الخبثاء من تعديل بيانات الدخل وإعادة حساب مجموعها الاختباري. من أشهر دالتي البعثرة هاش المستخدمة في التشفير بكثرة، خوارزم خلاصة الرسالة ٥، وخوارزم البعثرة الآمن، على الرغم من وجود عيوب أمن في كل من الخوارزمين تم تقريرها [21, 22].

شفرة توثيق الرسالة message authentication code, MAC وتعرف أيضاً بالمجموع الاختباري للتشفير، هي دالة عامة في بيانات الدخل ومفتاح سري يعطي قيمة ثابتة الطول تستخدم في التوثيق. تعتبر خوارزميات الـ MAC طرق تشفير بالمفاتيح المتماثلة تعطي توثيقا لمصدر البيانات وسلامتها. لقد استخدمت هذه الخوارزميات في قطاع عريض من التطبيقات مثل التجارة الإلكترونية e-Commerce. إن أي دالة بعثرة h لها مفتاح K له مفتاح سري مكون من k من البتات كدخل ثانوي يستخدم لتوثيق الرسالة.

(١١،٣) العلامة المائية الرقمية

يُمكن تصنيف طرق العلامة المائية الرقمية [16, 23-25] تبعا لإدراكيتها أو فهمها، أو قوتها، أو نطاق المعالجة، أو أنواع المفاتيح كما في الجدول رقم (١١.١).

إن العلامات المائية الهشة لا تتحمل طرق المعالجة المعقدة. هذا الهششان يساعد في الكشف عن أي تعديل [18]. إن وضع العلامة المائية الهشة في الأجزاء غير المهمة الإدراك من البيانات يؤكد على عدم مدروكية هذه الأجزاء. إن العلامة المائية القوية يُمكنها أن تتحمل أو تعبر من خلال طرق المعالجة التي يتم تطبيقها على المحتويات [26]. هذه العلامات المائية القوية يُمكنها أن تتحمل عمليات المعالجة العادية مثل الترشيح، أو التحجيم، أو الاقتصاص [27] وتستخدم أساسا للتأمين والحماية، كما إنه من الصعب الوصول إلى علامة مائية واحدة تستطيع أن تتحمل كل عمليات معالجة الصور. يتم إخفاء أكثر من علامة مائية في الصورة المضيفة بحيث تستطيع واحدة من هذه العلامات على الأقل أن تمر عبر العمليات المختلفة لمعالجة الصورة وتسمى هذه الطريقة بالإخفاء المختلط [28] ولقد ظهرت هذه الطريقة في العديد من المنشورات.

في العادة يستخدم التشفير في توليد أو الحصول على العلامات المائية، في هذه الحالة يُمكن استخدام إما المفتاح العام وإما المفتاح الخاص. لقد اقترح Wong [29] علامة مائية باستخدام المفتاح العام تقوم بتقسيم الصورة إلى بلوكات ثم يتم حساب التوقيع لكل بلوك باستخدام دالة بعثرة للمفتاح العام، ثم يتم إخفاء هذا التوقيع في البلوكات المقابلة لها. يُمكن لهذه التوقيعات أن تحدد موضع أي تعديلات حتى مستوى البلوك الأساسي. بصرف النظر عن مقدرتها على تحديد الموضع وقوة مفتاح التشفير، إلا أنه قد تم الإعلان عن طرق ممكنة للهجوم على هذه الطريقة [26]. تعتمد هذه التوقيعات المنفردة على البلوك فقط بحيث لا توجد علاقة بينية بين هذه التوقيعات. يطلق على هذه الطريقة الاستقلالية على مستوى البلوك. إحدى الطرق الممكنة لتزوير العلامة المائية المستقلة على مستوى البلوك تسمى تكميم المتجه vector quantization, VQ للهجوم على التزوير [26]. إذا كان المهاجم لديه عدد كافٍ من عينات الصور التي بها علامات مائية، فإنه من الممكن للمهاجم أن يولد صورة توثيقية جديدة عن طريق إضافة قطع من عينات الصور الموثقة المختلفة، مثلما يحدث في الترقيع. منذ ظهور

مهاجمات التكميم الاتجاهي VQ، فقد ظهر عدد من التحسينات للطرق الموجودة [30]: (١) زيادة أبعاد البلوك، (٢) تضمين فهارس البلوك في التوقيع، (٣) تضمين فهارس الصورة في التوقيع، (٤) تكسير الاستقلالية على مستوى البلوك.

الجدول رقم (١١،١) تصنيف التعليم المائي.

التصنيف	نوع العلامة المائية
الإدراكية	مرئي، غير مرئي
القوة	قوي، شبه هش، هش
نطاق معالجة الإشارة	النطاق المساحي، النطاق التحويلي
أنواع المفاتيح	المفتاح الخاص، المفتاح العام

بالنسبة لنطاق معالجة الإشارة الموضح في الجدول رقم (١١.١)، فإن طرق العلامة المائية الموجودة يُمكن تصنيفها إلى طرق في النطاق التحويلي، وطرق في النطاق المساحي [31]. الفكرة الأساسية في طرق النطاق المساحي هي إخفاء العلامات المائية واستخلاصها من الصور في النطاق المساحي بدون أي تحويل. يتم تشكيل العلامات المائية في النطاق المساحي ويتم إخفاؤها مباشرة في بيانات بكسلات الصورة. من أكثر الطرق شيوعاً لإخفاء المعلومات غير المرئية هي طريقة التعويض في البت ذات القيمة الصغرى LSB [23, 32, 33]. الفكرة الأساسية هي إدخال بتات الرسالة المطلوب إخفاؤها في البتات ذات القيمة الصغرى للبكسلات. لقد قامت طرق التعليم المائي الهشة الأولية بإخفاء المجموع الاختباري checksum [34] أو تتابع شبه عشوائي في مستوى البتات ذات القيمة الصغرى للصورة. لقد طبقت الأنظمة الأكثر حداثة آليات إخفاء أكثر تطوراً، بما في ذلك استخدام دوال البعثرة كما ذكرنا في طريقة وانج Wong [35]، للمساعدة في الكشف عن التغيرات في الصور ذات العلامة المائية. في عملية الاستخلاص، فإن البتات ذات القيمة الصغرى للصورة ذات العلامة المائية يتم استخلاصها ورصها بجوار بعضها لتشكيل الرسالة السرية، وبعد ذلك يتم تطبيق معكوس دالة التحكم. يُمكن لطريقة البتات ذات القيمة الصغرى أن تمتد للعديد من الأنواع المختلفة للتطبيقات عن طريق استخدام أنواع مختلفة لدالة التحكم، اعتماداً على تطبيقاتها.

بالمقارنة بطرق النطاق المساحي، فإن الفكرة الأساسية لطرق نطاق التحويل تتم باستخدام تحويلات مثل تحويل فورير، التحويل الجيبي المقطع DCT، والتحويل المويجي لإخفاء واسترجاع العلامات المائية في النطاق التحويلي. تقوم طرق النطاق التحويلي بإخفاء الرسالة في مساحة معتبرة من الصورة، مما يجعله أكثر قوة ضد الهجوم.

(١١،٤) العلامة المائية للصور الطبية

إن تقنيات العلامة المائية تعزز مقاييس السرية الموجودة حالياً لتوزيع البيانات من شتى الأنواع بما في ذلك الصور الطبية. على الرغم من ذلك، فإن هناك حدوداً على تطبيق هذه الطرق مباشرة على الصور الطبية من حيث

أن العلامة المائية يُمكن أن تغير من الصورة الأصلية إلى الدرجة التي قد تكون عندها الصورة غير مقبولة للتشخيص أو التحليل الكمي. إن تأثير العلامات المائية المخفية في الصور على تشخيص وتحليل هذه الصور يعتبر من المواضيع الأساسية.

تطبيق العلامات المائية [36] في الصور الطبية يكون في الأساس عمليات توثيق [6]، واختبار السلامة [37-42] وإخفاء البيانات الفوقية [43, 44]. عدد من طرق العلامات المائية المقترحة موجهة أساسا لتوزيع وإدارة الصور الطبية لأغراض بعيدة التشخيص [40, 42, 43]. تعتمد طرق العلامات المائية المقبولة للتشخيص أساسا إما على طرق العلامات المائية المنعكسة [39, 41]، وإما على الطرق المعتمدة على المنطقة [5, 37, 38] والتي سيتم شرحها في الأجزاء التالية. هناك عدد من طرق العلامات المائية المناسبة للصور الطبية المضغوطة في النطاق التحويلي. سنركز في هذا الفصل على طرق العلامات المائية للصور الغير مضغوطة، حيث الصور غير المضغوطة تكون مقبولة للاستخدام في أغراض التشخيص.

(١،٤،١١) العلامات المائية المنعكسة

يقال عن العلامة المائية أنها منعكسة إذا اعتبرت الصورة موثقة والضوضاء المضافة نتيجة هذا التوثيق يُمكن إزالتها بالكامل للحصول على بيانات الصورة الأصلية. لقد تم تقديم طريقتين أساسيتين للعلامة المائية المنعكسة في المؤلفات. تعتمد إحدى هاتين الطريقتين على العلامة المائية القوية المضافة مساحياً بالارتباط مع الإضافة الوحدوية modulo addition [45]، وتعتمد الطريقة الثانية على الضغط بدون خسارة lossless والتشفير لمستويات البتات [46-48]. كل من الطريقتين تحقق قوة تشفيرية في التحقق من سلامة الصورة نتيجة تعلق سرية النظام بتشفير سري أساسي مثل دالة البعثرة، هاش.

واحدة من طرق العلامة المائية المنعكسة المبكرة تم اقتراحها عن طريق بارتون Barton [46] حيث قام بضغط البتات التي تتأثر بعملية الإخفاء. إن الضغط يحافظ على البيانات الأصلية بينما يولد مساحة لإخفاء المعلومات السرية، كما أن البيانات المضغوطة والحمل المضاف يتم إخفاؤها بعد ذلك في الصورة المضيفة. تستخدم هذه الطريقة لإخفاء العلامات المائية المنعكسة [47, 48].

طرقة أخرى من طرق إخفاء البيانات المنعكسة [45] تستخدم طريقة إضافة علامة مائية قوية مساحيا [49] لإخفاء نموذج علامة مائية W في صورة أصلية من ٨ بتات، حيث يتم حساب W من دالة البعثرة H (للصورة الأصلية). يُمكن استخدام دالة بعثرة بمفتاح سري K كما يلي:

$$W=H(p,K)$$ المعادلة رقم (١١،١)

حيث P هي بتات الحمل الإضافي. يتم إضافة نموذج العلامة المائية W للصورة كما يلي:

$$I_w=I+W \bmod 256$$ المعادلة رقم (١١،٢)

حيث I_w هي الصورة المحتوية على العلامة المائية. لاسترجاع الصورة الأصلية، فإن الحمل الإضافي p يتم استخلاصه أولا من الصورة المحتوية على العلامة المائية، وبعد ذلك يتم حساب نموذج العلامة المائية W كما سبق. البيانات الخبيئة يُمكن إزالتها باستخدام الطرح الوحدوي modulo 256 للحصول على الصورة الأصلية I كما يلي:

$$I=I_w - W \text{ modulo} 256$$ المعادلة رقم (١١.٣)

إمكانية أن الطريقة السابقة سينتج عنها ضوضاء الملح والفلفل salt and pepper في الصورة ذات العلامة المائية عندما يتم عكس البكسلات القريبة من الصفر إلى قيم قريبة من ٢٥٥ قد تم شرحها في المرجع [50]. إمكانية استخلاص الحمل الإضافي صحيحاً تقل عندما يكون عدد البكسلات التي يتم عكسها كبيراً جداً. هذه الضوضاء التي في صورة الملح والفلفل في الصورة ذات العلامة المائية قد تكون غير مرغوبة في تطبيقات الصور الطبية.

لقد اقترح Fridrich et al [51] طريقة إخفاء للبيانات بدون خسارة لشكل الصور الطبية غير المضغوطة. يتم فرض الصورة الأصلية في الشكل الرمادي بالأبعاد MxN بكسل بما في ذلك قيم البكسلات من المجموعة P حيث، $P=\{0, \ldots, 255\}$. يتم تجميع البكسلات في أي صورة في بلوكات غير متقاطعة، يتكون كل منها من عدد من البكسلات المتجاورة. يتم تقسيم الصورة إلى مجموعات غير متجاورة من عدد n من البكسلات المتجاورة $(x_1, \ldots, x_n)$. يتم إنشاء دالة تمييز F لتصنيف البلوكات إلى ثلاثة أنواع مختلفة من المجموعات: العادية R، والوحيدة S، وغير القابلة للاستخدام U. يتم تحديد أي عملية منعكسة F على الـ P، وهي عبارة عن تبديل للمستويات الرمادية التي تتكون كلها من دورتين. الفكرة الأساسية لهذه الطريقة هي أنها تفحص الصورة في مجموعات وتقوم بالضغط بدون خسارة للتدفقين R و S. يتم عكس المجموعات R و S كل منها مع الآخر باستخدام عملية العكس F، بينما لا تغير المجموعات U حالتها. بوضع واحد في R وصفر في S، يتم إخفاء أحد بتات الرسالة في كل من مجموعة الـ R أو الـ S. إذا كانت بت الرسالة ونوع المجموعة غير متوافقين، يتم تطبيق عملية العكس F على المجموعة للحصول على التوافق. تتكون البيانات المطلوب إخفاؤها من الحمل الزائد وإشارة العلامة المائية. على الرغم من أن هذه الطريقة جديدة وناجحة في إخفاء البيانات المنعكسة، إلا أن كمية البيانات التي يُمكن إخفاؤها تكون محدودة. أحد المشاكل التي يُمكن أن تظهر مع تطبيق هذه الطريقة على الصور الطبية هي أنه مع زيادة السعة، فإن جودة الرؤية تنخفض بدرجة كبيرة.

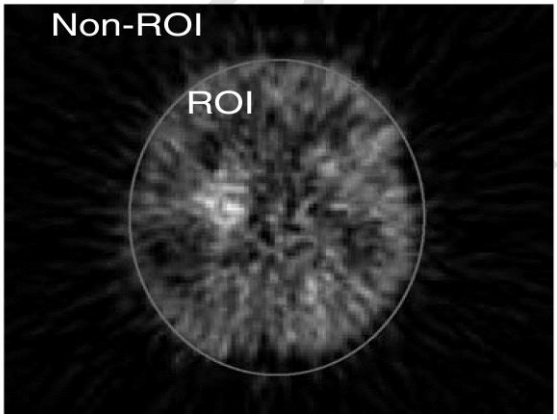
لقد قدم Celik et al [52] طريقة لإخفاء البيانات ذات سعة عالية، وأقل ضوضاء، وقابلة للعكس. في هذه الطريقة يتم تكميم الإشارة المضيفة، ويتم الحصول على المتبقيات في مرحلة الإخفاء. يتم استخدام خوارزم الضغط المعتمد على السياق، والمهايئة، والتشفير للصورة بدون خسارة context based, adaptive, lossless image coding, CALIC، مع اعتبار قيم التكميم كمعلومات جانبية. يتكون هذا الخوارزم من ثلاثة مكونات: التوقع، ونمذجة

السياق، والتشفير الإنتروبي المشروط. يعمل التشفير التوقعي على تقليل التكرار المساحي في الصورة. يقوم النموذج السياقي بفحص العلاقة المساحية مع مستويات الصورة المختلفة. ثم يقوم التشفير الإنتروبي المشروط بتوليد شفرة أصغر عن طريق تحويل العلاقة. إن هذا يفعل توليد السعة العالية لبيانات الحمل عن طريق ضغط المتبقيات التكميمية. ثم يتم تركيز المتبقيات المضغوطة وبيانات الحمل وإخفاؤها في الإشارة المضيفة باستخدام طريقة التعويض عن البت ذات القيمة الصغرى LSB. لقد تم تقرير أن السعة العالية للإخفاء يُمكن الحصول عليها مع ضوضاء أقل نسبياً.

إن الاعتبارات الأساسية في تطوير كل خوارزميات الإخفاء بدون خسارة هي زيادة السعة وتقليل المشاكل البصرية المتولدة بسبب إخفاء الحمل.

(٢،٤،١١) العلامة المائية المعتمدة على المنطقة

تستخدم الطرق المعتمدة على المنطقة التكرار المساحي في الصورة. يوجد في معظم الصور الطبية تكرار مساحي مثل الخلفية، التي لا يكون لها أهمية كبيرة في التشخيص. لقد اقترح Coatrieux [37] طريقة علامة مائية معتمدة على المنطقة للتحقق من سلامة الصورة. لكي يتم حماية الصورة الطبية يتم تقسيمها إلى مناطق: مناطق اهتمام ROI، ومناطق غير مناطق الاهتمام NROI كما هو موضح في الشكل رقم (١١.٢).



الشكل رقم (٢،١١) طريقة إخفاء تعتمد على المنطقة، التوقيع عن منطقة الاهتمام ROI يتم إخفاؤها في منطقة عدم الاهتمام NROI.

إن منطقة الاهتمام هي المنطقة المطلوبة للتشخيص، وسلامتها تكون مهمة. المنطقة غير المهمة NROI هي المنطقة المحيطة (خارج منطقة الاهتمام ROI) والتي لا تستخدم في التشخيص. يُمكن تحديد منطقة الاهتمام آلياً أو رسمها بطريقة شبه آلية عن طريق المشغل أو العامل. المعلومات عن حدود منطقة الاهتمام ROI تكون مطلوبة لعملية التحقق. يتم حساب التوقيع المتولد من دالة بعثرة التشفير من منطقة الاهتمام وإخفاؤه في منطقة الإدخال. أي

صورة يتم استخلاص التوقيع منها من منطقة الاهتمام والذي لا يتوافق مع التوقيع الموجود في منطقة الإدخال تكون صورة محتملة التعديل. ولذلك؛ فإن أي تغيير سواء كان نتيجة تزوير خبيث، أو نتيجة عبث، أو معالجة سببية أو أخطاء ضوضائية، يُمكن الكشف عنه. يعتبر استخدام منطقة الاهتمام ومنطقة غير الاهتمام في عملية الإخفاء والتحقق شرطاً مبدئياً مهماً لهذه الطرق.

يُمكن اعتبار منطقة اهتمام الصورة كرسالة ثنائية M، حيث |M| هي طول الرسالة، ويتم التحقق من صحتها عن طريق التوقيع Sr المحسوب من دالة البعثرة للتشفير f. يُمكن تقسيم M إلى N من المقاطع m_i كل منها طوله μ_i من البتات: $M=m_1,\ldots, m_N$. يتم إنتاج التوقيع S_R من تجاور كلمات التحكم Si التي عددها N وهي $\eta_1, \ldots, \eta_N$ لتحديد أي تغيير. كل Si يحمي المقطع المقابل له m_i استقلاليا. دالة استخلاص التوقيع f (تسمى دالة التحكم أيضاً) يُمكن تحديدها كما يلي:

$$S_R=f(M)=f(m_1,\ldots m_N)=(h_1,\ldots ,h_N)$$ المعادلة رقم (١١،٤)

في أثناء عملية التحقيق، يتم اختبار السلامة عن طريق مقارنة البصمة الخبيئة S_R والبصمة المحسوبة من الصورة التي تم استقبالها $S_R'=f(M')$.

أي أجزاء في الصورة يكون فيها $S_i \neq S_i'$ تعتبر قد تعرضت لتغيرات.

لقد استخدم Cao et al [5] طريقة steganographic لإخفاء بصمة رقمية مشفرة تحتوي على معلومات سرية عن المريض تسمى التغليف الرقمي digital envelope, DE. في البداية يتم تقسيم الصورة مع إزالة الخلفية عن طريق مواءمة أقل مستطيل يحتوي المنطقة ذات الأهمية التشخيصية. هذا المستطيل يفصل منطقة الاهتمام ROI عن منطقة عدم الاهتمام NROI. البصمة الرقمية DS لمنطقة الاهتمام يتم إنتاجها باستخدام دالة استخلاص البصمة باستخدام مفتاح خاص مثل دالة البعثرة للتشفير. يتم إلحاق معلومات المريض مع البصمة الرقمية إذا كان من الضروري تكوين التغليف الرقمي DE. يتم إخفاء الغلاف الرقمي داخل منطقة عدم الاهتمام خارج المستطيل، وبعد ذلك يتم تشفير الصورة المحتوية على الغلاف الرقمي تمهيدا لإرسالها.

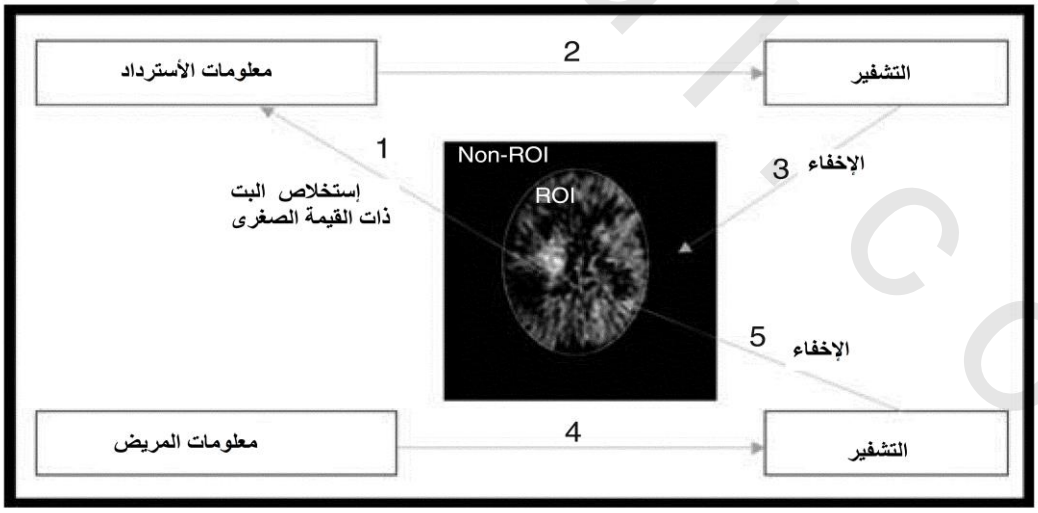
(١١،٥) العلامة المائية المنعكسة المعتمدة على المنطقة لإدارة صور الرسم المقطعي بالانبعاث البوزيتروني الآمن

لقد تم تطبيق إحدى طرق العلامة المائية المعتمدة على المنطقة لصور المسح المقطعي بالانبعاث البوزيتروني PET بغرض السرية والإدارة [54]. لقد تم استخدام الإخفاء المعتمد على المنطقة لتقسيم صور الـ PET إلى منطقتين ROI و NROI، اعتماداً على الأهمية التشخيصية. يتم تشفير معلومات المريض وإخفاؤها في منطقة الاهتمام ROI باستخدام الإخفاء في البت ذات القيمة الصغرى. البتات الأصلية التي تغيرت نتيجة إخفاء معلومات المريض المشفرة

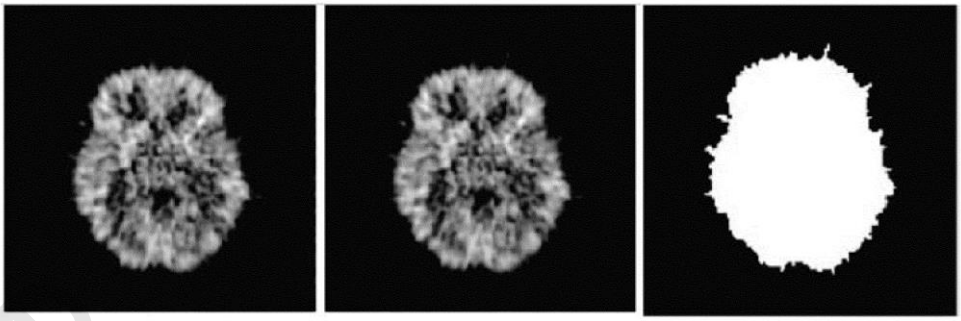
يتم تشفيرها وإخفاؤها في منطقة عدم الاهتمام NROI. القيم الأصلية لمنطقة الاهتمام يُمكن إعادتها باستخدام البيانات الموجودة في العلامة المائية المخفية في الـ NROI.

يتم استخدام طريقة تشبعية لتحديد الـ ROI والـ NROI. البكسلات الموجودة في الصورة والتي لها شدة أقل من حد التشبع يتم تخصيصها لمنطقة الـ NROI. من الممكن الحصول على بكسلات خاطئة التصنيف (فجوات) في كل من المنطقتين، والتي يُمكن ملأها باستخدام عمليات شكلية [55]. يتم استخلاص البتات ذات القيمة الصغرى في منطقة الاهتمام ROI ورصها بجوار بعضها على هيئة سلسلة رقمية، والتي يتم تشفيرها بعد ذلك وإخفاؤها في المنطقة NROI باستخدام تعويض البتات ذات القيمة الصغرى LSB. معلومات المريض (مثل: الاسم وتاريخ الميلاد) يتم إخفاؤها في منطقة الاهتمام ROI كما في الشكل رقم (١١.٣) وتعتمد كمية المعلومات على سعة منطقة الاهتمام ROI.

لقد كانت الصورة المعاد تشكيلها والمستخدمة في النتائج الموضحة في الشكل رقم (١١.٤) تتكون من بيانات خام ١٢٨×١٢٨ بدون إشارة (ولقد تم تحجيم البيانات إلى المدى من صفر حتى ٢٧٥٣٧ من وحدات الشدة). لم يظهر هناك أي فرق جوهري مظهري أو بصري بين الصور الأصلية والصور المخفية (MSE of 0.24+/-0.03). يُمكن للرسالة المستخلصة من الخلفية ثم فك شفرتها أن تعيد منطقة الاهتمام الأصلية ROI. هناك العديد من الاستخدامات الواعدة لمعلومات المريض المخفاة. إن تكامل معلومات المريض الموجودة خلال محتويات الصورة تعطي الكثير من المميزات التي منها سرية المعلومات، والحجم التخزيني المدمج، والتراسل السريع.



الشكل رقم (١١،٣) مخطط تخيلي لعملية إخفاء العلامة المائية المعتمدة على المنطقة مع معلومات المريض. البيانات التي ستتغير نتيجة إخفاء معلومات المريض (معلومات الاسترداد) يتم استخلاصها وإخفاؤها في الـ NROI. معلومات المريض يتم إخفاؤها في الـ ROI..



الشكل رقم (٤,١١) الصورة الأصلية، الصورة المحتوية على العلامة المائية، ونتائج حد التشبع. يوضح هذا الشكل الطريقة المستخدمة، في ماسح المخ الإكلينيكى fluorodeoxyglucose PET والتي تم إجراؤها على ماسح ECAT951R, PET فيمستشفي الأمير ألفريد الملكية. لقدكان هناك ٣١ مستوى مقطعياً للصورة. جدول أخذ العينات العادى يتكون من ٢٢ إطاراً زمنياً تم استخدامها لاكتساب بيانات الـ PET الإسقاطية. الطريقة المستخدمة لإعادة تشكيل الصور كانت طريقة الإسقاط بالترشيح العكسى.

(١١،٦) الملخص

لقد تم في هذا الفصل تقديم عدد من طرق السرية التي يُمكن تطبيقها على الصور الطبية. حاليا: تعتبر خوارزمات التشفير من أكثر خوارزمات مقياس السرية استخداماً، من حيث سرعتها وفعاليتها. على الرغم من ذلك، فإن معظم أدوات السرية لها الحدود الخاصة بها ومن الواضح أن اشتراك أكثر من طريقة من طرق السرية تعتبر أفضل الطرق لحماية البيانات. لقد تم تقديم الطرق الحديثة للعلامات المائية الرقمية كأداة بديلة لتحسين سرية الصور الطبية.

(١١،٧) تمارين

١ - اشرح الفرق بين التشفير والعلامة المائية الرقمية.

٢ - قارن بين مميزات وعيوب كل من طرق قياس السرية المقدمة في هذا الفصل:

- التشفير بالمفتاح الخاص.
- التشفير بالمفتاح العام.
- العلامة المائية المنعكسة.
- العلامة المائية المعتمدة على المنطقة.

٣ - أكتب برنامجاً بأشباه الأوامر pseudo code مستخدماً العمليات على مستوى البت لاستبدال البت ذات القيمة الصغرى LSB لأي صورة معطاة بحمل زائد (رمز الجامعة مثلاً).

المراجع (١١،٨)

1. R. Cushman. Information and medical ethics: Protecting patient privacy. IEEE Technology and Society Magazine 15(3):32–39, 1996.
2. J. G. Hodge. Jr., L. O. Gostin, and P. D. Jacobson. Legal issues concerning electronic health information: privacy, quality, and liability. JAMA. 282:1466–1471, 1999.
3. J. D. Halamka et al. A WWW implementation of national recommendations for protecting electronic health information.JAMIA. 4(6):259–265, 1997.
4. J. Collmann et al. Safe teleradiology: Information assurance as project planning methodology. JAMIA. 12(1):84–89, 2005.
5. F. Cao, H. K. Huang, and X. Q. Zhou. Medical image security in a HIPAA mandated PACS environment. Comput. Med. Imaging Graph. 27(2–3):185–196, 2003
6. C. Coatrieux et al. Relevance of watermarking in medical imaging. 2000 IEEE EMBS Conf. on Information Technology Applications in Biomedicine, 2000.
7. J. Zhang et al. Real-time teleconsultation with high-resolution and large-volume medical images for collaborative healthcare. IEEE Trans. Inf. Technol. Biomed. 4(4):265–273, 2000.
8. D. Feng et al. Medical image data retrieval and manipulation through the WWW. Proceedings of the International Symposium on Intelligent Multimedia, Video and Speech Processing, Hong Kong, 2001.
9. H. Mu¨nch et al. Web-based distribution of radiological images from PACS to EPR. Computer Assisted Radiology and Surgery. Proceedings of the 17th International Congress and Exhibition, 2003.
10. E. B. Suh et al. Web-based medical image archive system. Proceedings of SPIE Medical Imaging 2002: PACS and Integrated Medical Information Systems: Design and Evaluation, 2002.
11. E. Bellon et al. Web-access to a central medical record to improve cooperation between hospital and referring physicians. Stud. Health Technol. Inform. 93:145–153, 2003.
12. H. K. Huang. PACS Basic Principles and Applications. Wiley-Liss, 1999.
13. NEMA. Digital imaging and communication in medicine strategic document version 4.0. [Online]. Available: http://medical.nema.org/. 2005: NEMA.
14. E. Biham and A. Shamir. DiVerential Cryptanalysis of the Data Encryption Standard. Springer Verlag, 1993.
15. A. H. TewWk. Digital watermarking. IEEE Signal Processing Magazine 17:17–88, 2000.
16. N. Nikolaidis and I. Pitas. Digital image watermarking: An overview. ICMCS 99, 1999.
17. I. J. Cox and M. L. Miller. A review of watermarking and the importance of perceptual modeling. Proceedings of Electronic Imaging ’97, 1997.
18. E. T. Lin and E. J. Delp. A review of fragile image watermarks. Proceedings of the Multimedia and Security Workshop at ACM Multimedia ’99, 1999.
19. X. Lai and J. Massey. A proposal for a new block encryption standard. In EUROCTYPT’91, 1991.
20. R. Rivest. The RC5 encryption algorithm. Second International Workshop on Fast Software Encryption, 1994.
21. W. Xiaoyun and Y. Hongbo. How to break MD5 and other hash functions. Lecture Notes in Computer Science: Advances in Cryptology, A ¨ ı` EUROCRYPT 2005. 19–35, 2005.
22. O. S. Markku-Juhani. Cryptanalysis of block ciphers based on SHA-1 and MD5. Lecture Notes in Computer Science: Fast Software Encryption. 36–44, 2003.
23. R. V. Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. 1st IEEE International Conference on Image Processing, 1994.
24. E. T. Lin and E. J. Delp. A review of fragile image watermarks. The Multimedia and Security Workshop (ACM Multimedia ’99), 1999.
25. X. Kong and R. Feng. Watermarking medical signals for telemedicine. IEEE Trans. Inf. Technol. Biomed. 5(3):195–201, 2001.
26. M. Holliman and N. Memon. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. IEEE Trans. Image Processing. 9:432–441, 2000.
27. J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. Technical report, Fraunhofer Institute for Computer Graphics, 1994.
28. L. Chun-Shien et al. Cocktail watermarking for digital image protection. IEEE Transactions onMultimedia. 2(4):224, 2000.
29. P.W.Wong. A public key watermark for image verification and authentication. IEEE Inter. Conf. on Image Processing, 1998.

30. M. Celik, G. Sharma, and E. Saber. A hierarchical image authentication watermark with improved localization and security. Proc. ICIP 2001, 2001.
31. M. D. Swanson, B. Zhu, and A. H. Tewfik. Robust data hiding for images. IEEE Digital Signal Processing Workshop (DSP 96), 1996.
32. W. D. Bender, and N. Morimoto. Techniques for data hiding. IBM Systems Journal. 35(3/4):131–136, 1996.
33. L. Boney, A. H. Tewfik, and K. N. Hamdy. Digital watermarking for audio signals. International Conference on Multimedia Computing and Systems, 1996.
34. O. Bruyndonckx, J.-J. Quisquater, and B. Macq. Spatial method for copyright labeling of digital images. In Nonlinear Signal Processing Workshop, 1995.
35. J. Fridrich. Methods for tamper detection in digital images. Proc. Multimedia and Security Workshop at ACM Multimedia '99, 1999.
36. F. Mintzer, G. W. Braudaway, and M. M. Yeung. Effective and ineffective digital watermarks. IEEE ICIP, 1997.
37. G. Coatrieux, B. Sankur, and H. Maitre. Strict integrity control of biomedical images. SPIE Conf. 4314: Security and Watermarking of Multimedia Contents III, 2001.
38. A. Wakatani. Digital watermarking for ROI medical images by using compressed signature image. Proc. of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02), 2002.
39. F. Bao et al. Tailored reversible watermarking schemes for authentication of electronic clinical atlas. IEEE Trans. Inf. Technol. Biomed. 9(4):554–563, 2005.
40. Y. S. Lim and D. D. Feng. Multiple block based authentication watermarking for distribution of medical images. Proceedings of 2004 International Symposium on
Intelligent Multimedia, Video and Speech Processing, 2004.
41. Y. Yang and F. Bao. An invertible watermarking scheme for authentication of electronic clinical brain atlas. International Conference on Acoustics, Speech, and Signal Processing, 2003.
42. E. Bertino et al. Privacy and ownership preserving of outsourced medical data. 21st International Conference on Data Engineering, 2005.
43. D. Anand and U. C. Niranjan. Watermarking medical images with patient information. Proceedings of the 20th Annual International Conference of the IEEE, Engineering in Medicine and Biology Society, 1998.
44. Y. S. Lim et al. Interactive invisible captioning for medical image using digital watermarking. Proc. of International Conference on Image and Vision Computing, Dunedin, 2001.
45. C. W. Honsinger et al. Lossless recovery of an original image containing embedded data. U.S. patent application, docket no 77102/E/D, 1999.
46. J. M. Barton. Method and apparatus for embedding authentication information within digital data. U.S. patent application, docket no 5 646 997, 1997.
47. J. Fridrich, M. Goljan, and R. Du. Invertible authentication. Proc. SPIE, Security and Watermarking of Multimedia Contents, 2001.
48. A. Alattar. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Processing. 13(8):1147–1156, 2004.
49. C. W. Honsinger. A robust data hiding technique based on convolution with a randomised phase carrier. In Proc. PICS'00., 2000.
50. J. Fridrich, M. Goljan, and R. Du. Lossless data embedding-new paradigm in digital watermarking. EURASIP J. Appl. Signal Processing. 2:185–196, 2002.
51. J. Fridrich, M. Goljan, and R. Du. Lossless data embedding for all image formats. Proc. SPIE, Security and Watermarking of Multimedia Contents, 2002.
52. M. Celik et al. Reversible data hiding. Proc. of International Conference on Image Processing, 2002.
53. X. Wu. Lossless compression of continuous-tone images via context selection, quantization, and modelling. IEEE Trans. Image Processing. 6(5): 656–664, 1997.
54. Y. Lim et al. Web-based functional image display with embedded patient information for security and management. J. Nucl. Med. 45(5):492, 2004.
55. M. V. Droogenbroeck and M. Buckley. Morphological erosions and openings: Fast algorithms based on anchors. Journal of Mathematical Imaging and Vision. 22(2-3): 121–142, 2005.