المجلة العراقية للعلوم الاحصائية (10) 2006
ص ص [107-120]

تطبيق تقنية حساسة لإخفاء العلامات المائية الرقمية في الصور الرقمية الثابتة

عامر تحسين سهيل الصميدعي*

الملخص

العلامات المائية الرقمية حقل جديد من حقول السرية مهمته التحقق من علائقية المعلومات الرقمية واسعة الانتشار عبر وسائل تناقل المعلومات المختلفة . انها تحمي الصور الرقمية الثابتة، الصورالرقمية المتحركة او الاصوات ، من السرقة او القرصنة. لعلامات المائية الرقمية تعطي المالك الشرعي لملفات المعلومات اعلاه المقدرة على التاكد من كون هذه الملفات نسخة شرعية النسخ ام انه قد تم تحريفها بدون تخويل من مالكها .

مع تطور تقنيات العلامات المائية الرقمية ، تطورت وسائل مهاجمة هذه العلامات لمحاولة حذفها او تحريفها لتحقيق الاستنساخات غير الشرعية .

تم في هذا البحث تطبيق تقنية حساسة لإخفاء العلامات المائية الرقمية داخل الصور الرقمية الثابتة ، باسلوب يحقق العشوائية في الاخفاء وشمولية أجزاء الصورة كافة لحمايتها من الهجوم.

Applying sensitive technique to hid digital watermarking in still images

ABSTRACT

Digital watermarking is a new field of security, it is important in verifying from widespread digital information transmission

*مدرس مساعد/رئيس قسم الحاسبات/ المعهد التقني _نينوى.

تاريخ التسلم : 22/ 8 /2005 ـــــــــــــــــ تاريخ القبول : 31/ 5 /2006

techniques, it protects digital still images, video, or sounds from piracy.

Digital watermarking gives real owner the ability to check if a file is an unauthorized copy or if it has been modified without authentication.

Within the development of digital watermarking technique, methods of watermarking attacks have been developed for deleting or modifying to improve illegal copying.

In this research, new sensitive technique is developed for hiding digital watermarking into a still image in a way that satisfied randomly hiding which includes every part of image, to protect it from attacking.

1- المقدمة:

العلامات المائية الرقمية تقنية من تقنيات اخفاء البيانات. اذ تنفذ باخفاء بعض البيانات داخل صورة رقمية، ملف صوتي، أو صور فيديوية . وبالامكان الاستفادة من هذه البيانات فيما بعد للتحقق من ملكية وشرعية الملفات الاصلية التي تحوي ذلك الإخفاء، فالمالك يقوم باسترجاع تلك العلامات المائية لتحديد ملكيتها.

هنالك عدة استخدامات للعلامات المائية، الغاية منها جميعا تحقيق المشروعية، ومن ذلك بصمة الإصبع، الوثوقية وتكامل البيانات، علامات الملكية، محددات السيطرة، حماية المحتوى [1،2،3] .

بصمة الإصبع تتحقق عند اخفاء المنتج او المؤلف علامة مميزة عند كل عملية استنساخ لنسخة جديدة، إذا وجدت أية نسخة غير موثوقة بعد ذلك يمكن تحديدها باسترجاع بصمة الاصبع. في هذه الحالة، يجب ان تكون العلامة المائية غير مرئية وغير قابلة للتلاعب او التزوير في حالة تعرضها للهجومات المتعمدة أو غير المتعمدة [2] . ولتحقيق الوثوقية وتأكيد تكامل البيانات يتم اخفاء بعض المعلومات الخاصة التي تصف الملف نفسه داخل ذلك الملف، هذا الوصف قد يكون بعض المعلومات عن المقاطع او الاجزاء المهمة فيه، لذلك فأي تلاعب في اي جزء من الملف سيؤدي من

ثم إلى حذف أو تشويه تلك العلامات المائية المخفية فيه وبذلك يتم تحديد وثوقيتها[3]. أما علامات الملكية فمثالها ما يتم استخدامه في القنوات الفضائية من وضع علامات ظاهرة عند احدى زوايا الشاشة للدلالة على مرجعية تلك الصور او الأفلام، هذا يمنع اعادة بث تلك المنتجات من فضائيات أخرى، كذلك يمنع الاستنساخ او البث غير المشروع لها ما لم يتم محوها او تحريفها [4]. أما استخدام محددات السيطرة، فمن أمثلتها خاصية التفاعل مع اجهزة استنساخ الاقراص كأن يتم تحديد عدد من النسخ المقبولة للاستنساخ وبذلك عند كل استنساخ لنسخة اضافية يتناقص عدد النسخ المسموح به، وهكذا يتكرر التناقص حتى يصل الى الصفر اذ لا يسمح لنسخ اضافي اخر [2]. وأخيرا حماية محتوى الملف من اي تلاعب فيتم بإخفاء علامة مائية غالباً ما تكون شاملة لكل اجزاء الملف حتى تحقق الغاية بمنع اي تلاعب مهما كان طفيفاً وفي اي جزء من الأجزاء [5] .

وعلى الرغم من تلك الاستخدامات المختلفة للعلامات المائية الرقمية، فان هذه الانواع يمكن ان تقسم الى فئتين هما العلامات المائية الهشة والعلامات المائية الحساسة. العلامات المائية الهشة سهلة التحطم وعادة تستخدم خاصية اخفاء العلامات المائية في جزء محدد من الصورة، لذلك فانه لا يمكن اكتشاف أي تلاعب قد يحصل في اجزاء الصورة عدا المنطقة التي تتواجد فيها هذه العلامات. أما العلامات المائية الحساسة فقد استخدمت بصيغة اكثر حساسية ففي حالة تعرض الملف لاي تلاعب مهما كان طفيفا، فان تلك العلامات سوف تتحطم مما يسهل اكتشاف هذا التلاعب. العلامات المائية الحساسة يمكن ان تقسم كذلك الى فئتين فرعيتين. الفئة الأولى يعبر عنها بالمحلية وهي التي تتطلب الصورة الاصل او المرجع عند الفحص واسترجاع العلامات المائية من الملف. اما الفئة الاخرى فهي العامة التي بالامكان استرجاعها دون الحاجة الى عملية المقارنة مع الملف الأصل [5]، تجدر الإشارة هنا إلى أن التقنية التي تم تطبيقها هي من نوع العلامات المائية الرقمية الحساسة العامة وطبقت على الصور الرقمية الثابتة .

في الآونة الأخيرة كان التوجه نحو ايجاد تشريعات قانونيـــة معتمـــدة عالميـــاً كتشريعات قياسية يتم العمل بها لمقاضاة المتجاوزين على حقوق الملكية فـــي جميـــع مجالات الانتاج الرقمي من ملفات صورية او فيديوية او صوتية، وقد ســـهلت تقنيـــة العلامات المائية بانواعها المختلفة مهمة هذه التشريعات حيث يتم اتخـــاذ الاجـــراءات القانونية لمقاضاة المتجاوزين استناداً الى تلك العلامات المائية التي تثبت خصوصـــية وعائدية تلك المنتجات لمالكيها الشرعيين المستخدمين لها وعلى الرغم من ذلك كله فانه لم توجد الى حد الان تشريعات عالمية قياسية وموحدة يمكن اعتمادها فـــي كـــل دول العالم نتيجة لاختلاف هذه العلامات المائية وتنوعها وتطور تقنياتها المستمر [4] .

2-خصائص تقنية العلامات المائية الرقمية الحساسة العامة:

لكي تصنف العلامات المائية ضمن الفئة الحساسة العامة يجب ان تتمتـــع بجملـــة خصائص أهمها [6،7،8] .

1- الفرق بين الصورة الاصل والصورة ذات العلامة المائية المخفية يجب ان لا يدرك او يميز، اي ان عملية اخفاء العلامة المائية يجب ان لا يحدث اي تشويه جزئي او كلي في الصورة.
2- العلامات المائية غير المنظورة يجب ان لا تكشف من قبـــل المســـتخدمين غيـــر المخولين.
3- عملية فحص الصورة واستخراج العلامة المائية منها يجب ان لا يتطلـــب وجـــود الصورة الاصل لتحقيق ذلك.
4- تعذر استخراج العلامة المائية من قبل المهاجمين حتى في حالة معرفة الخوارزمية التي تمت بها عملية الاخفاء.
5- ان مالك الصورة الشرعي والمخولين وحدهم لهم الحق في امتلاك المفتاح السري الخاص بالاستعادة.

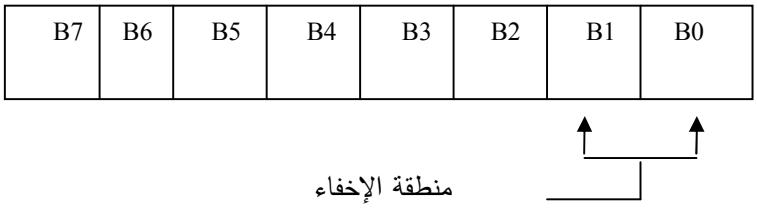
6- يجب ان يكون اخفاء العلامة المائية شاملاً لكل اجزاء الصورة لكي تكون حساسة ضد اي تلاعب في اي جزء من أجزائها. ففي حالة كون العلامة المائية في جزء او حيز من الصورة قد يتجاوزه المهاجم بالعبث ويتلاعب ببقية أجزاء الصورة الخالية من العلامة المائية .

7- يجب ان تكون التقنية حساسة ضد الهجومات المتعمدة وغير المتعمدة التي قد تحصل للصورة.

3- اين يتم الاخفاء؟

قبل الشروع ببيان طريقة الاخفاء المطبقة لابد من الاشارة الى المناطق في الصورة التي من الممكن اخفاء بيانات العلامة المائية فيها دون حصول حالة التشويه او التلاعب في محتوى الصور الذي يؤدي من ثم الى ادراكه وتمييزه من قبل المستخدمين.

تشير جميع تقنيات اخفاء البيانات داخل الصور الى ان الاخفاء في البت الاقل اهمية (Least Significant Bit :LSB) من كل خلية صورية (Pixel) او حتى في البت الذي يليه، لا يؤثر في خصائص الصورة الاصل اياً كان نسيجها، اذ ان كل خلية صورية تتمثل ببايت (ثماني بتات) في الصورة ذات تمثيل 256 مستوى لوني [2,1]، وكما موضح ذلك في الشكل(1) .



الشكل(1)

ان تبديل البت الاقل اهمية من الخلية الصورية يعني تبديل قيمته بـــين 0 أو 1 وهذا يعني زيادة او نقصان قيمة التمثيل لها برقم واحد فقط ، أما تبديل البتـــين الاول والذي يليه B0 و B1 فيعني تغيير قيمة الخلية الصورية بمقدار 3 كاقصى حد زيادة او نقصاناً، وفي كلتا الحالتين المذكورتين انفا لا يمكن ادراك ذلك التغيير فـــي الصـــورة الاصل بعد عملية التبديل، اذ يتم تبديل هذه المواقع من الخلايا الصـــورية المطلـــوب الاخفاء فيها بوضع بتات العلامة المائية بدلاً منها.

4- التقنية المطبقة :

تعتمد التقنية التي تم تطبيقها على اسلوب التوزيع العشوائي لبتات العلامة المائية بحيث يشمل جميع اجزاء الصورة وباستخدام مفاتيح سرية كبيرة الحجم لتعقيد عمليـــة اكتشافها من قبل المهاجمين. ومبدأ عمل الطريقة هو ايجاد نقطة ارتكاز اولية بتحديـــد الموقع (X ,Y) للخلية الصورية الاولى لاخفاء البت الاول من العلامة المائية حيـــث X تمثل البعد الأفقي للصورة و Y تمثل البعد العمودي منها. ومن هذا الموقع يـــتم الانطلاق لحساب الموقع التالي للاخفاء وهكذا لبقية المواقع وتتمثل خوارزمية التطبيق بالخطوات الاتية :

1- اختيار مفتاح سري k على ان يكون حجم تمثيله بطول 16 بتا او من مضاعفاتها لسهولة التعامل معها برمجياً.

2- تكوين نقطة ارتكاز أولية لكل من ($\mathbf{X_o}$, $\mathbf{Y_o}$) باستخدام الصيغة الاتية :

$$X_o = WX^K \bmod N$$

$$Y_o = WY^{(K\hat{}2)} \bmod N$$

حيث : (WX) تمثل عرض الصورة

(WY) تمثل ارتفاع الصورة

(N) تمثل (WX*WY)

3- حساب موقع (LX , LY) :

$$LX= \mathbf{X_o}^2 \bmod N$$

$$LY= \mathbf{Y_o}^2 \bmod N$$

4- حساب موقع الاخفاء (X ,Y) :

$$X=LX \bmod WX$$

$$Y=LY \bmod WY$$

5-حشر بت من العلامة المائية في الموقع (X ,Y) :

6-حساب الموقع التالي (LX , LY) كالآتي :

$$LX= LX^2 \bmod N$$

$$LY= LY^2 \bmod N$$

7-تكرار الخطوات 6,5,4 حتى تنتهي عملية حشر جميع بتات العلامة المائية في الصورة الأصل.

5- عملية استرجاع العلامة المائية:

تجرى عملية استرجاع العلامة المائية من قبل الجهة المستلمة للصورة لغرض التحقق من وثوقيتها أو عائديتها ،وتتم عملية الاسترجاع هذه بتطبيق نفس خطوات خوارزمية الإخفاء الواردة في الفقرة (4) السابقة ، الا انه عند الخطوة (5) من الخوارزمية تتم عملية قراءة قيمة البت المخفي من العلامة المائية في الموقع (X,Y) ،

وبتجميع هذه البتات وتحويلها إلى سلسلة من البايتات التي تمثل العلامة المائية المخفية، ومن ثم مطابقتها مع العلامة المائية المتفق عليها ، فان كانت مطابقة فـذلك يعنـي أن الصورة المستلمة شرعية ،وإلا فان الصورة المستلمة قد تم التلاعب بها.

6- النتائج والمناقشة:

أ- إن احتمالية التغيير في عينات الصورة بعد إجراء عملية إخفاء العلامـة المائيـة تكون 50% من عدد بتات هذه العلامة ،فقد تكون قيمة البت المـراد إخفـاؤه مـن العلامة المائية مشابهة لقيمة البت المراد الإخفاء فيه من عينات الصورة فيبقى دون تغيير، أو أن تكون قيمة البت مختلفة وهنا سوف تتغير قيمة الخلية الصورية التـي يتم الإخفاء فيها بمقدار (1) زيادة أو نقصانا من (256) مستوى لونيا ،وكما موضح ذلك في الشكل (2) .

0	1	1	0	1	1	0	**1**

قيمة الخلية الصورية (109) ـ قبل عملية الإخفاء ـ

0	1	1	0	1	1	0	**1**

قيمة الخلية الصورية (109) ـ بعد عملية الإخفاء في حالة كون البت المراد اخفاؤة (1)-

0	1	1	0	1	1	0	**0**

قيمة الخلية الصورية (108)ـبعد عملية الإخفاء في حالة كون البت المراد اخفاؤة (0)ـ

الشكل (2): نموذج يبين قيمة الخلية الصورية قبل عملية الإخفاء وبعدها

وعند مقارنة الصورة الأصل مع الصورة بعد وضع العلامة المائية فيها باستخدام معامل نسبة الإشارة إلى الضوضاء(SNR: Signal to Noise Ratio) وجد أن هذه القيمة مرتفعة جدا، مما يدل على أن التغيير الحاصل في الصورة طفيف جدا بعد إجراء عملية الإخفاء.

$$SNR_{RMS} = \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[\hat{I}(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[\hat{I}(r,c)-I(r,c)]^2}}$$

ب – الطريقة المطبقة تواجه بعض المشاكل التي قد تقلل من كفاءتها، عليه يجب معالجتها، وفيما يأتي أهم تلك المشاكل مع بيان الحل المناسب لكل منها.

أولا: في أثناء عملية حساب موقع الإخفاء قد يتكرر ظهور احداثي (X ,Y) لموقع سبق وان تم الاخفاء فيه وهذه مشكلة كبيرة تؤدي الى تحطم العلامة المائية المخفية كون اخفاء البت الجديد يعني الغاء البت القديم الذي كان قد تم اخفاؤه سابقاً في الموقع نفسه. هذه المشكلة يتم حلها بسهولة باعداد جدول يحوي جميع مواقع (X ,Y) التي تم الاخفاء فيها وعند حساب اي موقع جديد يكون الرجوع لهذا الجدول لعرض هل هذا الموقع ضمن الجدول ام لا فان كان كذلك يتم تجاوز الخطوة الخامسة من خوارزمية الاخفاء ويصار لحساب موقع جديد،وإلا فيتم الإخفاء عند ذلك الموقع،على أن ينظم الجدول ذاته عند استرجاع العلامة المائية من الصورة.

ثانيا: الإخفاء في البت الاقل اهمية قد يدفع المهاجم في حالة سرقة المفتاح السري الى تطبيق الخوارزمية لاسترجاع العلامة المائية من الصورة وبعد ذلك يقوم بالتلاعب بمحتوى الصورة ومن ثم يعيد اخفاء العلامة المائية وبذلك تعد الصورة المحرفة عند الاستلام وكانها صورة شرعية المصدر .

هذه المشكلة يمكن حلها بإضافة عامل آخر للخوارزمية، ما دامت هناك إمكانية للإخفاء في البت التالي للبت الاقل أهمية، كما تمت الاشارة الى ذلك ضمن الفقرة (3) من البحث، فانه بالإمكان استخدام مفتاح سري اخر K2 لتحديد مكـــان حشـــر بـــت العلامة المائية هل هو البت الاقل اهمية من الخلية الصورية ام الذي يليه، ولتحقيـــق ذلك تتم اضافة المعادلات الاتية الى خطوات الخوارزمية المطبقة وحسب مامؤشر ازاء كل منها :

الخطوة 1: اضافة مفتاح سري اخر K2 بنفس طول المفتاح الاول K.

الخطوة 2: حساب قيمة معامل الارتكاز Z_o :

$$Z_o=B^{K2} \bmod N$$

حيث B : يمثل عدد بتات تمثيل كل خلية صورية وهي هنا تساوي (8)

الخطوة 3: حساب قيمة LZ كالآتي :

$$LZ=Z_o^2 \bmod N$$

الخطوة 4: حساب موقع اخفاء البت من العلامة المائية :

$$Z=LZ \bmod MZ$$

حيث MZ : تمثل عدد البتات المسموح الاخفاء فيها ضـــمن كـــل خليـــة صورية وقيمتها هنا (2) وهي البت الاقل اهمية والذي يليه .

الخطوة 5: ان كانت قيمة Z مساوية لـــ 0 فالاخفاء يكون في B0 وان كانت قيمته 1 فالاخفاء في B1 .

الخطوة 6: حساب الموقع التالي لقيمة LZ :

$LZ=LZ^2 \bmod N$

ثالثا: قد تتعرض الصورة ذات العلامة المائية لبعض الهجومات بنوعيها المتعمد وغير المتعمد مما يتسبب في فقدان العلامات المائية الموجودة داخل تلك الصور او تحريفها.

يمكن إجمال الهجومات غير المتعمدة بجميع المعالجات التي يتم تطبيقها على الصور كالضغط، التدوير، تغيير الحجم، تحسين الصورة، وأنواع أخرى كثيرة، هذه جميعها لا يمكن اعتبارها من مساوئ الطريقة لان الغاية من العلامة المائية هي لاثبات ملكية الصورة والتحقق من عدم التلاعب بها، وإذا ما تمت تلك المعالجات على الصورة فمعنى ذلك انه تم تغيير محتواها، عندها يتم اكتشاف ذلك وهذا هو المطلوب **[8,6]** .

أما الهجومات المتعمدة فتتم في احدى حالتين، عند معرفة المفتاح السري او عند عدم معرفته، ففي حالة عدم معرفة المفتاح السري للعلامة المائية فالهجوم هنا يتم بطريقة العبث بمحتوى الصورة لتشويه العلامة المائية المخفية ضمن مواقع من الصورة وهذا يتم اكتشافه بسهولة عند استرجاع العلامة المائية حيث تكون فيها محرفة وغير حقيقية، أما في حالة معرفة المفتاح السري فان المهاجم هنا سوف يقوم باستعادة الصورة الاصلية بدون العلامة المائية واجراء بعض التحريفات عليها ومن ثم اعادة العلامة المائية الى الصورة الجديدة، وهذه المشكلة الوحيدة التي لا يمكن اكتشافها لان سارق المفتاح السري هنا اصبح المالك الشرعي للصورة المستخدمة لذلك المفتاح، ولحل هذه المشكلة يتم الاتفاق بين المرسل والمستقبل على تغيير المفتاح السري بشكل مستمر او تحديد مجموعة من المفاتيح السرية واختيار احدها في الاخفاء اعتماداً على خاصية اوصيغة او زمن يتم الاتفاق عليه، وهكذا يكون المفتاح السري بتغير مستمر مما يعقد امكانية اكتشافه من قبل المهاجم.

الاستنتاجات :

1. الطريقة المطبقة تحقق عشوائية عالية في توزيع العلامة المائية مما يعقد عملية اكتشافها و استخراجها من قبل المهاجمين.

2. الاختلاف في احتساب قيمة $\mathbf{X_o}$ و $\mathbf{Y_o}$ لنقطة الارتكاز الأولية يمنع احتمالية تساوي قيمة احداثيي X و Y في الخطوات التالية للخوارزمية مما يزيد من عشوائية الطريقة .

3. الطريقة لا تتطلب وجود الصورة الأصل عند فك الإخفاء لاسترجاع العلامة المائية من الصورة المستلمة.

4. شمولية التوزيع للعلامة المائية في اجزاء الصورة كافة يجعلها حساسة جداً ضد اي تلاعب مهما كان طفيفاً وفي أي جزء من اجزائها.

5. طول المفتاح السري K يعقد محاولة الكشف لصعوبة احتماليات التوقع.

6. إضافة المفتاح السري K2 الخاص بموقع إخفاء البت ضمن الخلية الصورية يزيد تعقيد محاولة الاكتشاف،وكذلك يوفر إمكانية إعادة الإخفاء في نفس الخلية الصورية، حيث يكون الإخفاء في البت الاول الاقل أهمية ومرة أخرى بالذي يليه وهذا يزيد الطريقة كفاءة ويمنحها سرية اعلى.

7. إمكانية تغيير المفاتيح السرية باستمرار حسب صيغة اتفاق بين المرسل و المستقبل وهذا يعطي الطريقة وثوقية أعلى لتفويت الفرصة على المهاجمين بزيادة المحاولات الفاشلة لاكتشافها.

8. القدرة على إخفاء علامة مائية بحجم قد يصل الى 25% من حجم الصورة لامكانية الاخفاء في البتين الاول و الثاني من مجمل ثماني بتات في كل خلية صورية.

9. بالإمكان تطبيق هذه الطريقة على الصور ذات اللون الحقيقي (True Color)، اذ كل خلية صورية تتمثل بثلاث بايتات كل منها يمثل لونا من الالوان الرئيسة الـثلاث (الأحمر، الأخضر والأزرق : RGB) ، فتتم تجزئة العلامة المائية وإخفاؤها في الألوان الثلاثة.

10. عند تطبيق هذه الطريقة على الصور أحادية اللون (mono) (حيث كل خليـة صورية تتمثل ببت واحد فقط) يحصل تغير واضح في معالم الصورة .

المصادر

[1] Bender, W., " Techniques for Data Hiding ", ***IBM System Journal***, Vol.35, 313(23), 1996.

[2] Memon, N., & Wong, P.W., " Protecting Digital Media Control ", ***communications of the ACM***, 35(8),July 1998.

[3] Celik, M., Sharma, G., & Tekalp, A.M. " Localized Lossless Authentication Watermark ", ***Security and Watermarking of Multimedia Content***, Vol. 5020, no. 70 , 2003.

[4] Arn, j., Gatlin, R., & Kordsmeier, W., " Multimedia Copyright Laws and guidelines: Take the test ", ***Business Communication Quarterly*** . 32-39, December 1998.

[5] Cox, I., Miller, M., & Bloom, J. , " Watermarking application and their properties ", ***paper presented at the proceedings of the international conference on information technology: coding and computing*** , Las Vegas, Nevada, 2000,March 27-29.

[6] Wu, Y., Xu , C., & Bao, F., " Counterfeiting Attack on a Lossless Authentication Watermarking Scheme ", ***ACS series conference in Research and Practice in Information Technology*** , 2002 ,
http://www.i2r.a-star.edu.sg/icsd/

[7] Fridrich, J., Goljan, M., & Rui, D. ," Lossless Data Embedding - New Paradigm in Digital Watermarking ", ***Special Issue on Emerging Applications of Multimedia Data Hiding*** , 185-196 , 2002 .

[8] Wu, M., & Liu, B. , " **Attacks on Digital Watermarks** ", 2000, http://www.ee.princeton.edu/-minwn/rsch-datahiding.html.