King Saud University
College of Computer & Information Sciences
Information Systems Department

CEN 448 – Information Security

Steganography

Done By
Yousef Dardeer

Number
423101808

مقدمة
فن الإخفاء والتشفير
أساليب الإخفاء
علم تحليل الإخفاء
المراجع

فن الاخفاء

مقدمة

الرسائل الغير مرئية أو المخفية أو المغطاة كلها تصب في نفس المعنى في عالم التكنولوجيا "ستيجنوجرافي". حيث لا يعلم عن وجود الرسالة إلا المرسل والمستقبل, والرسالة نفسها تبدو بصورة أخرى. وبالرجوع إلى اللغة اليونانية القديمة, نستطيع أن نترجم هذه الكلمة إلى "فن إخفاء الكتابة".

هذا المفهوم تم استخدامه وتطبيقه منذ مئات السنين, حيث كان الملوك والأمراء القدامى يستخدمون العبيد لكتابة الرسائل على ظهورهم. أو كانوا يحلقوا رؤوسهم ثم يكتبوا عليها. كما كانت تستخدم الحيوانات لهذا الغرض أيضا. وبعد ذلك, ظهر الحبر الخفي في الصورة وأصبح وسيلة إخفاء الكتابة الجديد. وعند ظهور نهضة الحاسبات والتكنولوجيا, دخل فا الإخفاء إلى عصر جديد ممكن أن يطلق عليه بالعصر الرقمي.

وبأخذ نظرة دقيقة لهذه العملية نستطيع أن نفصل عناصرها. حيث هناك الغطاء أو الحامل, وهو ما يتم إخفاء الرسالة فيه, ويكون غالبا صورة أو مقطع صوتي أو فيديو. وهناك الرسالة نفسها, وممكن أن تكون من أي نوع. وهناك أيضا مفتاح الإخفاء, وهو المستخدم في الإخفاء نفسه, ولا يعلمه إلا المرسل والمستقبل.

فن إخفاء الكتابة والتشفير

يخطئ كثير من الناس عندما يعتبرون أن التشفير(Cryptography) وإخفاء الكتابة هما نفس الشيء. فبأخذ نظرة دقيقة وتقنية نرى أن التشفير هو دراسة لطرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل. وهذا يختلف عن فن الإخفاء حيث أن التشفير يغير من هيئة محتوى الرسالة لكنه لا يخفي وجودها. أما إخفاء الكتابة فيخفي وجود الرسالة من الأساس. يمكن تقسيم أساليب فن التشفير إلى:

- **أساليب تحويل الكتابة:** وتبنى أما على مبدأ الإبدال, أي يتم تحويل كل عنصر من الرسالة إلى عنصر آخر. ومبدأ النقل, وفيه يتم إعادة ترتيب حروف الرسالة.
- **أساليب معالجة الكتابة:** حيث يتم تقسيم الرسالة إلى قطع, وإدخالها على عملية تعالج هذه القطع باستخدام خوارزميات رياضية.

وبشك عام نستطيع أن نقارن بين فن إخفاء الرسالة و فن التشفير عن طريق هذا الجدول

فن التشفير	فن الإخفاء
العلم بوجود رسالة	عدم العلم بوجود رسالة
يمنع الأطراف الخارجية من معرفة محتوى الاتصال	يمنع الأطراف الخارجية من معرفة وجود الاتصال
تقنية شائعة	تقنية غير شائعة

جدول مقارنة بين التشفير وإخفاء الكتابة

أساليب الإخفاء

تتمحور فكرة الإخفاء في إدخال الرسالة ر داخل الغطاء غ لتكوين الهدف المخفى خ. ويمكن تمثيله بهذه المعادلة:
الهدف المخفى = الرسالة المراد إخفاءها + الغطاء + مفتاح الإخفاء
وبشكل عام, يكن تقسيم أساليب الإخفاء إلى أربعة أساليب أساسية:

1- **الإخفاء النصي:**

ويكون ذلك بكتابة نص يمكن استخلاص الرسالة المخفية منه. إما بطريقة نصية بان يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفاة. أو بطريقة نحوية أو لفظية.

2- **الإخفاء الصوتي:**

إخفاء رسالة داخل إشارة صوتية ممكن أن يكون في مجال الزمن أو مجال الطيف. ويتم بإحدى الطرق التالية:

- **ترميز البت المنخفض:** هذه الطريقة لها سعة إدخال عالية (41,000 bps). لكنها عرضة للاكتشاف. وفيها يتم إبدال أكثر بت غير مهم (Least Significant Bit) من كل إشارة صوتية
- **الطيف الممتد:** يتم فيها إدخال الرسالة داخل الترددات الأعلى من اللازم. وتعتبر أكثر طريقة من ناحية الإخفاء لكن سعة الإدخال فيها منخفضة(4 bps)
- **تغطية الإدراك:** هي أكثر طريقة من ناحية سعة الإدخال(450,000 bps) لكنها أكثرها عرضة للاكتشاف. ويتم فيها إدخال نص الرسالة داخل مناطق لا يمكن للإنسان إدراكها من الإشارة الضوئية.

3- **الإخفاء الفديوي:** مشتق من الإخفاء بالصور حيث أن مقاطع الفيديو ليست إلا مجموعة من الصور المتتالية. لذلك فإننا نستطيع تطبيق أساليب الإخفاء الصوري.

4- **الإخفاء الصوري:** هو أكثر طريقة تمت دراستها من قبل الباحثين. توجد عدة طرق لإدخال رسائل في صور نذكر منها:

- **التحويل الزاوي المتقطع:**
- **التحويل الموجي:**
- **الإدخال في البت الأقل أهمية:**هي أكثر طريقة مستخدمة, وتقضي بإدخال بت أو أكثر من الرسالة المراد إخفاؤها وإبداله بالبت ذي أقل أهمية من الصورة. البت الأقل أهمية هو البت الذي له اقل قيمة حسابية($1=2^0$) في حين أن البت الأكثر أهمية هو البت الذي له اكبر قيمة حسابية($128=2^7$). مثلا: إذا كان لدينا صورة يتكون البكسل الواحد منها من 24 بت(24-bit image) فإننا نستطيع إبدال 3 بت من كل بايت من الصورة بـــ 3 بت من الرسالة المراد إخفاؤها. لذلك فان صورة من حجم 1024 في 768 يمكن أن يخفى فيها نص حجمه 294,912 بايت دون أن تلاحظ بالعين المجردة.

وكمثال آخر: تخيل إننا نريد إخفاء الحرف "G" داخل صورة حاملة من ثمانية بايت تمثيلها الثنائي هو:

10010101 00001101 11001001 10010110
00001111 11001011 10011111 00010000

نعرف أن تمثيل الرف "G" الثنائي هو 01000111 . إذن نستطيع أن ندخل هذا الحرف في الصورة بإبدال البت الأقل أهمية فيصبح تمثيل الصورة :

10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001

علم تحليل الإخفاء

هو عملية كشف الكتابة المخفية من قبل جهة أخرى غير المرسل والمستقبل.لاحظ أن هناك فرق بين اكتشاف وجود رسالة مخفاة, واكتشاف محتوى الرسالة نفسها. فعلم تحليل الإخفاء يدرس بشكل عام اكتشاف وجود الرسالة فقط.

توجد طريقتان لاكتشاف الإخفاء. هناك طرق للاكتشاف تتعلق بأسلوب إخفاء معين, وهناك طرق عامة لا تتعلق بنوع معين.لكل الطريقتين مميزات وعيوب, فالطريقة المتعلقة بأسلوب إخفاء واحد تكون دقة نتيجتها عالية, ولكنها قد تفشل عند تطبيقها على أساليب إخفاء أخرى. في حين أن الطريقة العامة لا تكون ذات دقة عالية, لكن ممكن أن تعطي نتائج مقبولة لعدد من أساليب الإخفاء. نستطيع أن نقول عن أسلوب تحليل بأنه ناجح إذا استطاع اكتشاف وجود الرسالة. أما اكتشاف محتواها فهذا أمر أصعب من ذلك.

يمكن تصنيف طرق التحليل بالاستناد على كمية المعلومات الممكن اكتشافها إلى:

- **Stego-only attack**: هدف الإخفاء هو الشيء الوحيد الذي يتم تحليله
- **Known carrier attack**: الهدف والناقل يتم تحليلهما
- **Known message attack**: الرسالة المخفاة معروفة
- **Chosen stego attack**: الهدف المخفى موجود وأسلوب الإخفاء معروف
- **Known stego attack**: الحامل والهدف وأسلوب الإخفاء كلها معروفة

توجد عدة طرق لاكتشاف الرسالة المخفاة, أشهرها هو اكتشاف التشويش أو التشوه في الصورة مثلا. نعرف أن جميع تشكيلات الألوان في الصور تتكون من مزيج من ثلاثة ألوان رئيسية, الأحمر والأخضر والأزرق. فتختلف الألوان بمدى اختلاف الكمية الممزوجة من هذه الألوان الرئيسية. لذلك يمكن كشف الإخفاء بتحليل كل بايت من الصورة لمعرفة دقة الألوان فيها, وبذلك يتم كشفها.

المراجع

- *Stinsown* "Cryptography: theory and practice"

- *Huaiqing Wang, Shuozhong Wang* Communications of the ACM " Cyber warfare: steganography vs. steganalysis " http://www.acmqueue.com

- *Neil F. Johnson, Zoran Duric, Sushil Jajodia,* Center for Secure Information Systems George Mason University "Information Hiding Steganography and Watermarking – Attacks and Countermeasures"

- *Gary C. Kessler* Associate Professor Computer and Digital Forensics Program Champlain College Burlington " An Overview of Steganography for the Computer Forensics Examiner"

- Curran, K. and Bailey, K. "An Evaluation of Image Based Steganography Methods." *Int.*
- *J. of Digital Evidence*, Fall 2003.

- http://en.wikipedia.org