إخفاء نص في صفحات مواقع الانترنت

عائشة صديق شاهين

قسم علوم الحاسبات / كلية علوم الحاسبات والرياضيات

جامعة الموصل

الاستلام	القبول
2011 / 02 / 03	2011 / 11 / 02

Abstract:

In this research the protection techniques are developed by using hiding in HTML pages which is suitable for ease of use on the other hand, the pages written in HTML, distributed largely on the Internet, so there is the possibility that the revealed contacts used for HTML pages is difficult, inspite of used techniques for network monitoring.

Eight methods was applied in the concealment of which match the colors (Color matching) and property size (Size Attribute) and the use of labeling of (JavaScript) and the use of marking (CSS) and has been proposed other modalities of hiding are the property (Hover) and the link attribute (Link) and the property of field hidden (Hidden Field) and the replacement property (Alternate). Has also been used: Java script, CSS,HTML development environment in Dream Weaver8 for application of this research.

الملخص:

تم في هذا البحث تطوير تقنيات الحماية باستخدام أسلوب الإخفاء في صفحات HTML وهو أسلوب ملائم لسهولة استخدامها من جهة ومن جهة أخرى فان الصفحات المكتوبة في لغة HTML موزعة بصورة كبيرة على شبكة الانترنت, لذلك هناك احتمالية ان يكون كشف الاتصالات المستخدمة لصفحات HTML بالرغم من وجود التقنيات المستخدمة في مراقبة الشبكة.

حيث تم تطبيق ثمانية طرائق في الاخفاء منها تطابق الألوان (Color matching) وخاصية الحجم (Size Attribute) واستخدام وسم من (JavaScript) و استخدام وسم (CSS) و تم اقتراح طرائق اخرى في الإخفاء هي خاصية الأرجحة (Hover) و خاصية الرابط

(Link) وخاصية الحقل الخفي (Hidden Field) و خاصية الإبدال (Alternate). كما تم استخدام:Java script، CSS ، ، HTML في بيئة تطوير Dream Weaver 8 لغرض تطبيق هذا البحث.

1- المقدمة:

لقد تعددت وسائل الاتصال بين الناس ورغبتهم بالحفاظ على خصوصية المعلومات المتبادلة ولا يتم تحقيقها إلا بإحدى طريقتين إما باستعمال وسائط اتصال تؤمن قنوات اتصال ذات حماية لا يمكن اختراقها للاطلاع على محتويات الرسالة، أو القيام بتطبيق إحدى التقنيات كالتشفير, والعلامة المائية, والكتابة المخفية, (إخفاء البيانات الرسائل) داخل الملفات الصورية أو الصوتية أو كلاهما معا (ملفات الفيديو) على الرسائل المطلوب إرسالها قبل عملية الإرسال. إن إخفاء المعلومات له أهمية كبيرة وذلك لأن عدم ظهور المعلومات للعيان يعتبر عامل حماية وأمن للمعلومات ما لم تتوصل التقنيات الحديثة إلى اختراع وسيلة اتصال آمنة بالقدر الكافي لنقل رسائل فائقة السرية.

2- ما هو علم الإخفاء:

أن إخفاء البيانات هو علم إخفاء المعلومات و البيانات السرية في غطاء. ومن الممكن أن يكون ملف الغطاء إما ملف صوتي أو صوري أو ملف فيديو أو نص بحيث يصعب على المشاهد العادي حتى معرفة وجود شئ مخفي فيها. ويعتبر هذا سببا رئيسيا للانتشار الواسع للكتابة المخفية مقارنة بطرائق التشفير لان الكتابة المشفرة أو المشوهة تدفع المتابع إلى الخوض بشتى الوسائل للحصول على المعلومة الأصلية ومحاولة كسر الشفرة في حين إن الكتابة المخفية لاتثير الشك عند المشاهد العادي و قد يمر عليها مرور الكرام دون إن يترك أثرا للمعلومة المخفية داخل الملف المضمن.[3][7]

في هذا البحث يتم تقديم طريقة إخفاء نص في صفحات موقع HTML في بيئة تطوير Dream Weaver8.

3 - أنواع نظام التغطية:

يمكن تقسيم نظام التغطية إلى ثلاثة أنواع نسبة إلى المفتاح المستخدم في عملية الإخفاء و هذه الأنواع هي:

أ - الإخفاء النقي Pure Steganography

يطلق على نظام الإخفاء الذي لايتطلب تبادلا مسبقا لمعلومات سرية(مثلا مفتاح الإخفاء) بأنه نظام إخفاء نقي وعملية الإخفاء فيه توصف بالصيغة الآتية:

$E:CXM \rightarrow C$

C : هي مجموعة احتمالات التغطية Covers.

M : هي مجموعة احتمالات الرسالة.

عملية الإرجاع توصف بالصيغة التالية:

$D:C \rightarrow M$

ب- الإخفاء بالمفتاح السري Secret Key Steganography:

هنا يختار المرسل غطاء (Coverْ) يخفي فيه الرسالة السرية فيه باستخدام مفتاح سري وإذا كان المفتاح السري المستخدم في إخفاء الرسالة معروفا للمستلم فانه يستطيع عكس المعالجة واسترجاع الرسالة السرية وأي شخص لا يعرف المفتاح السري لا يستطيع استرجاع المعلومات وتوصف عملية الإخفاء بالصيغة التالية:

$E_K:CXMXK \rightarrow C$

واسترجاع المعلومات بالصيغة التالية:

$D_K:CXK \rightarrow M$

ح- الإخفاء بالمفتاح العام Public Key Steganography:

تتطلب هذه الطريقة استخدام مفتاحين احدهما خاص والأخر عام. يخزن المفتاح العام في قاعدة بيانات عامة في عملية الإخفاء. أما المفتاح الخاص (السري) فيستخدم لاسترجاع الرسالة السرية. وفي التشفير باستخدام المفتاح العام, ليس من الضروري أن يشترك شخصان بمفتاح سري لتكوين قناة سرية (اتصال سري) ولكن عليهما فقط معرفة المفتاح العام للأخر.[2][8]

4 - تحليل (كسر) الإخفاء Steganalysis:

لكل طريقة أو أداة ذكية لتطوير إخفاء المعلومات في البيانات المتعددة الأوساط, عدد ما من الطرائق والأدوات الذكية التي تتطور لتحليل وكشف أسرارها.

القصد من هذه المقدمة, انه مع تطور العلم والأساليب المستخدمة في الإخفاء فهنالك تطور موازي في فن تحليل وكسر هذا الإخفاء. تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية، أو قراءتها, أو تغييرها، باسم (Steganalysis). ولنجاح هذه العملية لابد من أمرين, أولا: اكتشاف وجود معلومات مخفية, وثانيا: تغييرها أو حذفها أو مجرد قراءتها. وكل العملية هنا هي محاولة إخفاء البيانات بطريقة لا تثير الشبهات, أي لا تترك علامات أو اثر يدل على حدوث تغير ما. فمثلاً في حالة الإخفاء داخل الصور، يجب مراعاة عدة عوامل منها: عدم استخدام صور معروفة للإخفاء, أو نماذج من صور يمكن لأي شخص الحصول على نسخ منها (مثل صور الانترنيت) حيث تسهل المقارنة في حالة وجود صورتين.

وكذلك مراعاة ان لا يحدث تغير ظاهر في الصور كتشوهها أو تغير ألوانها بشكل واضح. ولهذا ينصح إخفاء بيانات كثيرة في صور ذات أبعاد كبيرة وألوان كثيرة خوفاً من تغير هيئتها بطريقة تهدم الهدف الأساسي من استخدام التقنية، لان إثارة الشبهة يعني فشل العملية.

ومع وجود الحاسوب بسُرعتهِ الفائقة، أصبح فن تحليل الإخفاء من الأمور اليسيرة والتي لا تستهلك وقتاً طويلاً للتنبؤ بوجود بيانات مخفية في ملف نصي أو صورة مرسلة عبر البريد الالكتروني أو الانترنيت بصورة عامة.

فهدف القائم بالإخفاء هو عدم إثارة أي نقطة للشك بوجود بيانات مخفية، وإستراتيجية محلل الإخفاء هو الشك في كل الرسائل المرسلة, وهذا لا يعني صعوبة أو استحالة هذه العملية. وكما قلنا إن وجود الحواسيب المتطورة والفائقة السرعة جعلت من فحص الملفات المرسلة أمرا ليس بالعسير. وهنا يكون دور القائم بعملية الإخفاء مهم جداً في اختياره ملفات الغطاء التي يصعُب معها التمييز فيما إذا كانت قد ضمنت بيانات أو لا. فمن الممكن إرسال صور شخصية, أو صور احتفالات جماعية, أو ملف صوتي خاص وغير متوفر عند محللي الإخفاء, ومثال بسيط على ذلك, استغلال ملف صوتي لحداد وهو يستخدم آلة كهربائية لتصفية الحديد, أو صوت سرب طيور, وغيرها من الأساليب المتوفرة وبسهولة وضمن البيئة المحيطة لنا [3][4][7][12].

5 – إخفاء المعلومات في صفحات HTML:

سيتم في هذه الفقرة تناول الرسائل المكتوبة بلغة (HTML) كوعاء حاوي على البيانات السرية حيث تم التطرق إلى بعض الطرق المعروفة لإخفاء المعلومات في صفحات HTML ومن ثم توضيح الطرائق التي تم اقتراحها لإخفاء المعلومات وهي: خاصية الأرجحة(Hover) وخاصية الرابط (Link) وخاصية الحقل الخفي (Hidden Field) و خاصية الإبدال (Alternate) كما سيتم توضيحهم لاحقا. ولتمثيل خوارزميات الطرائق أعلاه استخدمت: Java script،CSS، HTML في بيئة تتطوير Dream Weaver8.

6– الجانب العملي (الإخفاء في صفحات HTML) :

تؤدي تقنية تضمين المعلومات في الصورة إلى إحداث تغييرات غير ملحوظة في الشكل، وبما إن كمية المعلومات المتناقلة الكترونيا قد ازدات بصورة كبيرة، لذا توجد العديد من التطبيقات التي تعالج ليس فقط النص الواضح لكن أيضاً بيانات Formatted المكتوبة بلغات Markup مثل HTML حيث استخدمت لغة HTML كتقنية أساسية لتبادل المعلومات في الويبWeb.

حديثا, تم الاهتمام بالطرائق التقنية التي تحمي حقوق الطبع في المحتويات الرقمية المختلفة. وان تطوير تقنيات الحماية مناسب جدا لمحتويات HTML من ناحية أخرى فان هذه المستندات المكتوبة في صفحات HTML هي موزعة بصورة كبيرة على الويب، لذلك فان احتمالية أن يكون كشف الاتصالات المستخدمة لصفحات HTML صعب نسبيا.[7][13]

أن ملف HTML لصفحة الويب سيستخدم كغطاء نصي Cover - text. يتم تضمين البيانات السرية داخل نص HTML بينما تتم المحافظة على نص صفحة الويب الاصلية، ويتم إرسالها على شكل steg-text [1][5][9][14].

6-1- الطريقة الأولى تطابق الألوان Color matching:

طريقة تطابق الألوان تعني أن يكون لون النص المراد إخفاءه بلون الخلفية للصفحة المستخدمة لنقل هذا النص مثال: إذا كان لون خلفية الصفحة ابيض يكون لون النص المخفي ابيض أيضا كما موضح في الخوارزمية التالية.

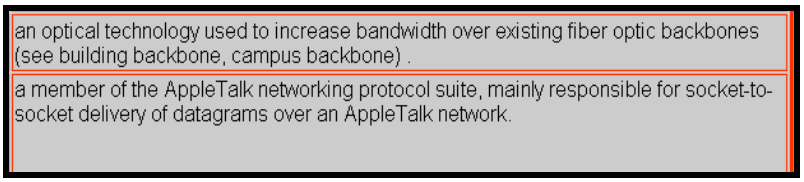
Input: HTML Web page(as Cover-text)&Secret Data & stego key.
Output: HTML Web Page(as stego-text)to transmit.
Processes:-
Step1: Get bgcolor attribute value (as stego key).
Step2: Color Secret Data with Stego Key.

الخوارزمية المستخدمة في عملية الاستخلاص

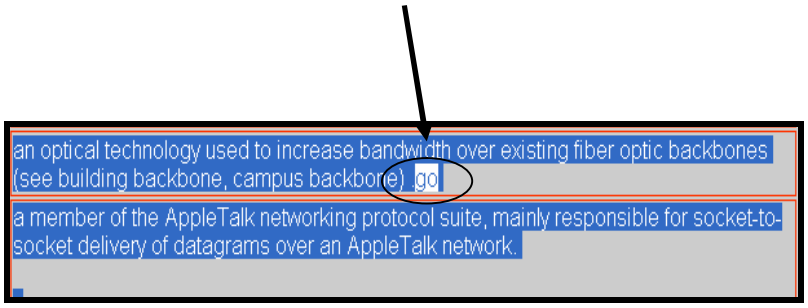
Input:Received HTML Web page (stego-text)&Stego key. Output: HTML Web Page(as stego-text)&Secret. Process:- Step1: selecting all.
or من لوحة المفاتيح Ctrl +A
or r click ➔ View source.

من الخوارزمية أعلاه يمكن إيجاد عدة طرائق من الإخفاء:

حيث تم في هذه الطريقة استخدام (الرابط) ويكون ملون بلونين مثلا رمادي (نفس لون الخلفية) واللون الثاني ازرق أي عند التأشير على ألرابط يصبح لونه ازرق (يظهر الرابط المخفي) كما موضح في الشكل رقم (1)، والشكل رقم [2]:



الشكل رقم (1): الرابط المخفي



الشكل رقم (2): استخلاص الإخفاء

إدراج صورة معينة وكتابة النص المخفي على الصورة بحيث يكون لون النص نفس لون الصورة. كما موضح في الشكل رقم (3) والشكل رقم (4).

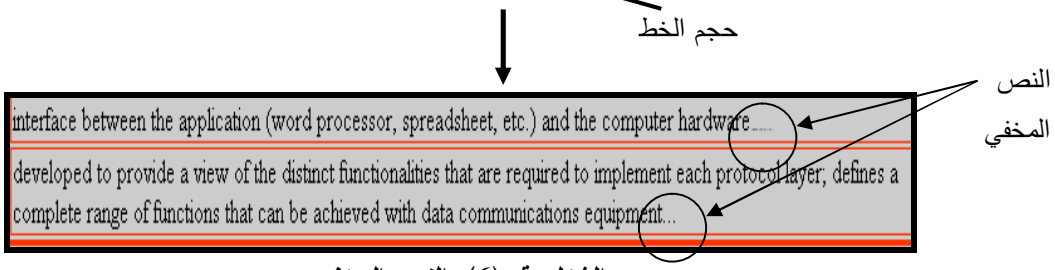
الشكل رقم (3): صورة فيها الإخفاء

الشكل رقم (4): استخلاص الإخفاء

6-2- الطريقة الثانية خاصية الحجم Size Attribute:

يمكن إخفاء نص في صفحة HTML باستخدام خاصية حجم الخط. وذلك بجعل الخط اصغر حجم ممكن كما في الشكل رقم (5) والشكل رقم (6)حيث يظهر الخط بشكل نقاط حيث بالإمكان أن يوزع النص المخفي كل كلمة في نهاية جملة من الجمل المعروضة على صفحة HTML ليظهر على شكل نقطة في نهاية الجملة المعروضة على الصفحة [5][9].

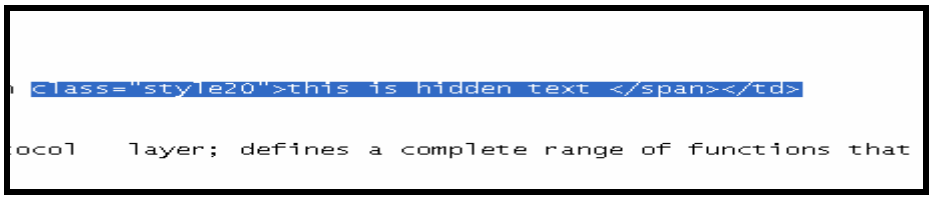
الشكل رقم (5): لوحة الخصائص



الشكل رقم (6): النص المخفي

عملية استخلاص الإخفاء:

يمكن استخلاص الإخفاء من View Source كما في الشكل رقم (7):



الشكل رقم (7): استخلاص الإخفاء طريقة size attribute

6-3- الطريقة الثالثة: استخدام وسم (JavaScript)

<no script>hidden text in html</no script>

عملية استخلاص الإخفاء:

يمكن استخلاص الإخفاء من view source

6-4- الطريقة الرابعة: استخدام وسم (CSS)

<Div style =" display: none "> hidden text in html</Div>

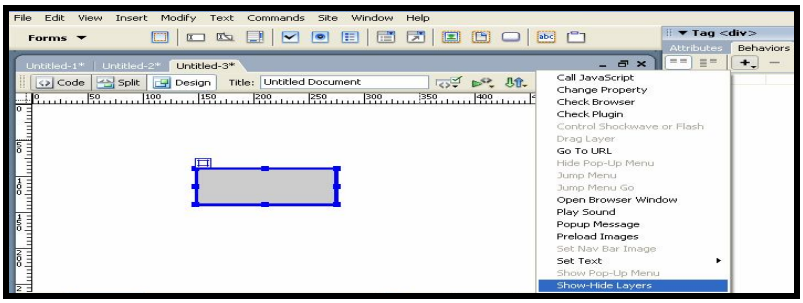
عملية استخلاص الإخفاء:

يمكن استخلاص الإخفاء من View Source

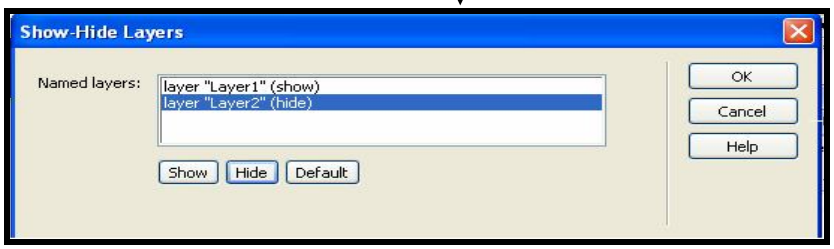
6-5- الطريقة الخامسة: Layers

في هذه الطريقة استخدمت خاصية Java Script ولكن مع Dream Weaver8 بأتباع الخطوات التالية كما موضحة بالشكل رقم (11,10,9,8): [2]

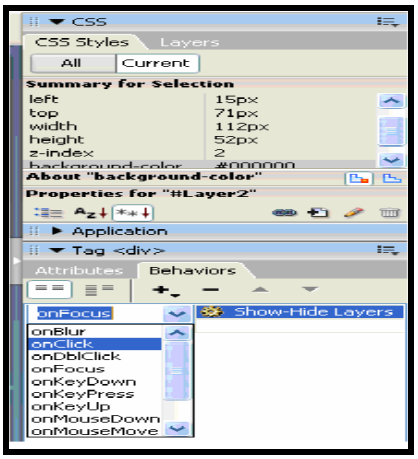
الشكل رقم (8): طريقة إضافة طبقة



الشكل رقم (9): خصائص layers



الشكل رقم (10): إخفاء طبقة وإظهار طبقة



الشكل رقم (11): تفعيل الطبقات

عملية استخلاص الإخفاء:

يمكن استخلاص الإخفاء من View Source والطريقة ألأخرى عند النقر على الطبقة سوف تظهر الطبقة الأخرى حيث يوجد النص المخفي.

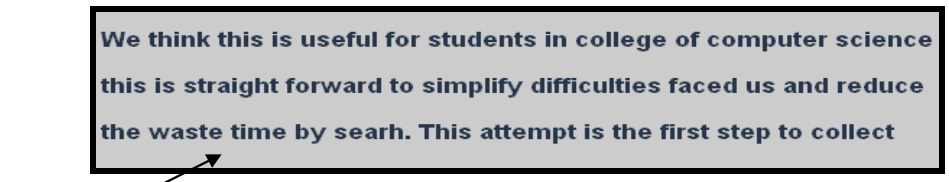
7- الطرائق المقترحة:

لقد لاحظنا في الطرائق الموضحة سابقا إمكانية استخدام صفحة HTML كغطاء نصي - Cover text للبيانات أو الرسالة المراد إخفائها. يتم تضمين البيانات السرية داخل نص HTML مع المحافظة على نص صفحة الويب الأصلية دون تغيير وعلى هذا الأساس تم اقتراح طرق أخرى لإخفاء نص في صفحة HTML وبنفس الكفاءة كما موضحة في الفقرة التالية.

تم في هذا البحث اقتراح أربعة طرائق لإخفاء البيانات وهي:

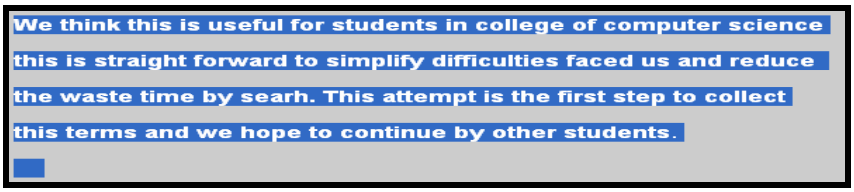
7-1- الطريقة الأولى (طريقة استخدام الرابط):

تم تطبيق هذه الخوارزمية على الطرائق المقترحة في هذا البحث وباستخدام أسلوب CSS وذلك بإلغاء الخط من الرابط لمنع إثارة الشكوك بوجود معلومات مخفية والشكل رقم (12) يوضح طريقة إزالة الخط من الرابط لكلمة time والتي تودي إلى النص المخفي.



الشكل رقم (12): الرابط الذي يودي للنص المخفي

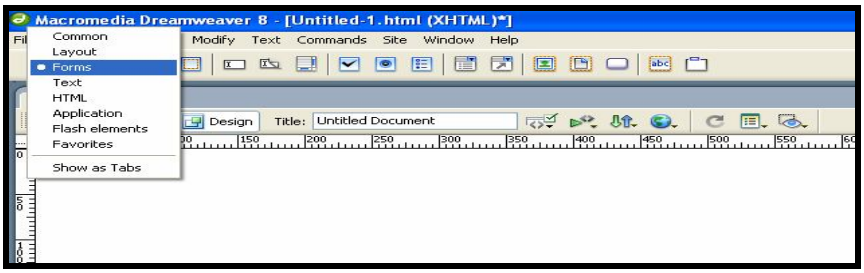
الرابط المخفي



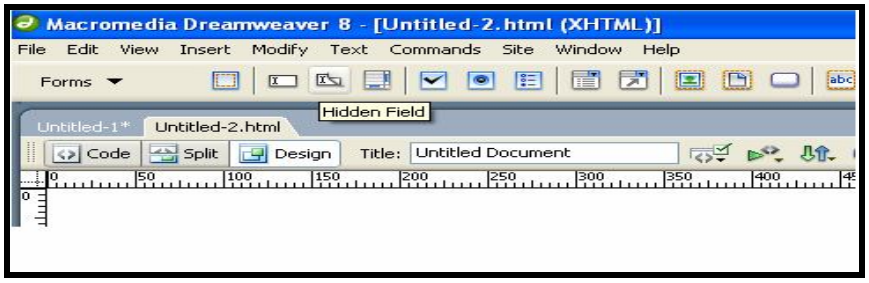
الشكل رقم (13): استخلاص الإخفاء

7-2- الطريقة الثانية استخدام Hidden Field:

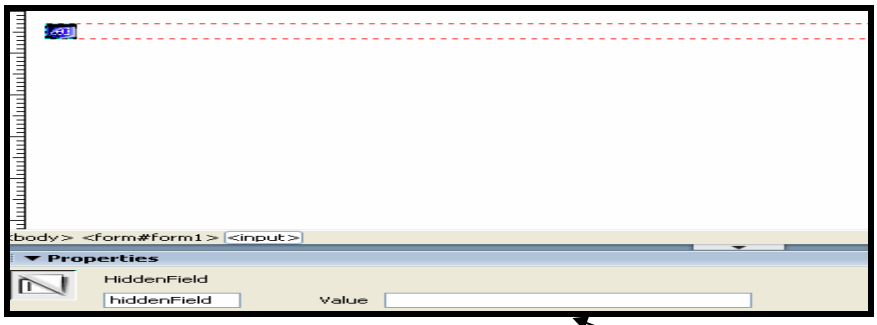
تم اقتراح طريقة :Hidden Field بإتباع الخطوات الموضحة في الشكل رقم (14) والشكل رقم (15) والشكل رقم (16):



الشكل رقم (14): Forms



الشكل رقم (15): Hidden Field



الشكل رقم (16): خصائص Hidden Field

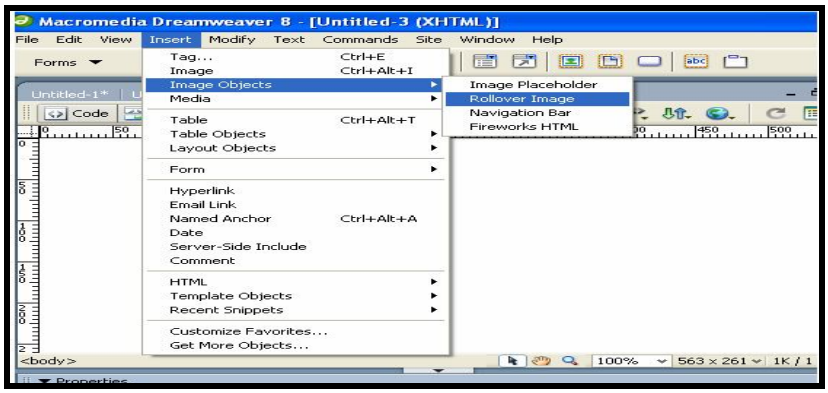
هنا نضع النص المراد إخفائه

عملية استخلاص الإخفاء:

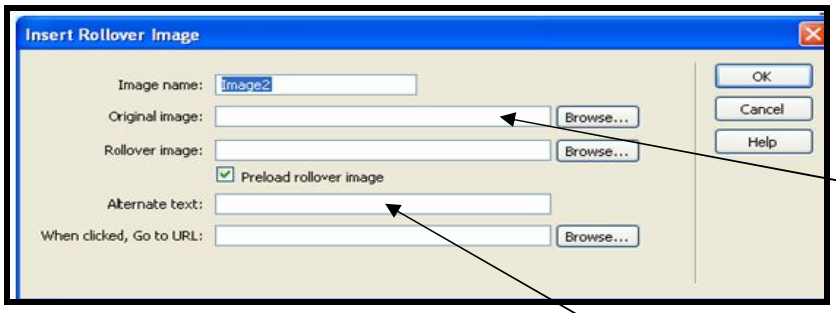
يمكن استخلاص الإخفاء من view source.

7-3- الطريقة الثالثة Rollover Image:

هنا استخدمت هذه الخاصية لإخفاء النص الذي يكون على هيئة صورة حيث نستخدم في هذه الطريقة صورتان الصورة الأولى مثلا منظر طبيعي والصورة الثانية نص على هيئة صورة عند التأشير على الصورة الأولى تظهر مباشرةً الصورة الثانية الذي فيها النص المخفي. وذلك بإتباع الخطوات الموضحة في الشكل رقم (17) والشكل رقم (18):



الشكل رقم (17): إضافة صورة باستخدام خاصية Rollover



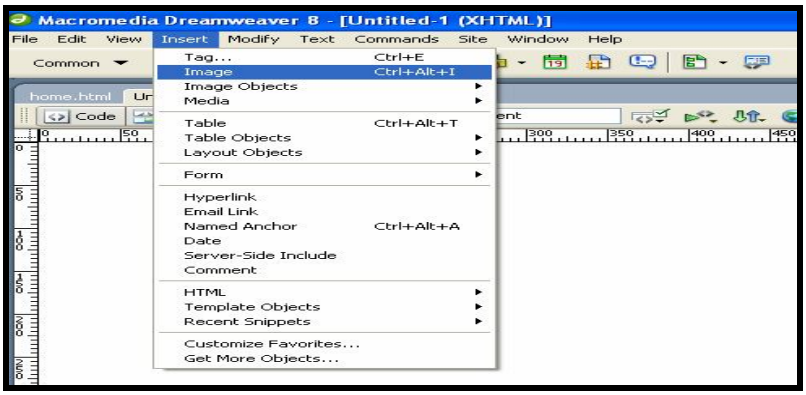
الصورة الأصلية

نص على هيئة صورة

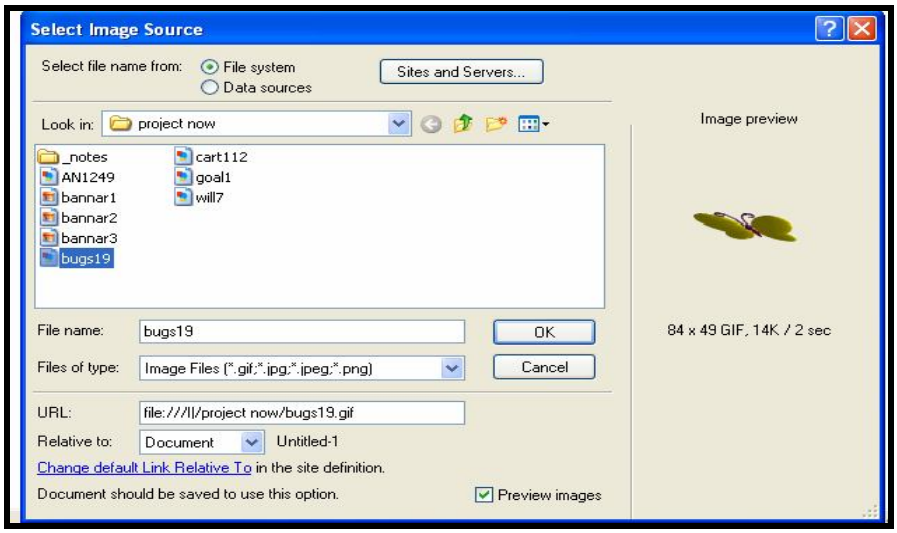
الشكل رقم (18): خصائص Rollover Image

7-4- الطريقة الرابعة استخدام خاصية alternate:

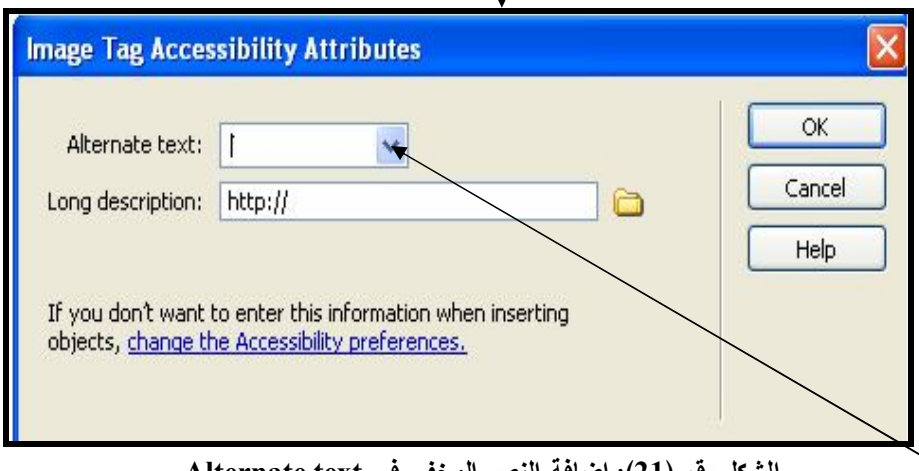
تم اقتراح هذه الطريقة: يتم استخدام خاصية alternate في عملية إخفاء نص وذلك بإتباع الخطوات التالية في الإشكال رقم(19), رقم(20), رقم(21):



الشكل رقم (19): إضافة صورة



الشكل رقم (20): اختيار صورة



الشكل رقم (21): إضافة النص المخفي في Alternate text

النص المخفي

8- استخدام JAVA Script:

طرق أخرى باستخدام اللغات التفاعلية مع المستخدم Dynamic language بالإضافة إلى طريقة no script وذلك باستخدام CSS وهو مختصر (Cascading Style Sheet) حيث يوجد اثنين من السمات الخاصة تستخدم في إخفاء وإظهار النص هي أولا "display" والثانية هي "visibility". أما "display" لها العديد من القيم والخصائص ولكن الذي نحتاج إليه هو "none" و "block". "none" هي مثل كلمة إخفاء و "block" هي مثل كلمة إظهار والمثال التالي يوضح إخفاء وإظهار النص في نفس المقطع البرمجي كما في الشكل رقم (22).

الشكل رقم (22): استخدام Java script لإخفاء نص

أما "visibility" فلها العديد من القيم أيضا والتي تهمنا منها "visible", "hidden" وتستخدم لإظهار وإخفاء النص بنفس الطريقة، أما الفرق بين الاثنين هو مكان النص سيبقى فارغا على الصفحة مما يثير الشك بوجود شي ما وراء هذا الفراغ لذا يفضل في هذه الطريقة أن يكون مكان النص المخفي في الجوانب أو في أسفل الصفحة حتى لا يجذب النظر إليه ومن ثم يثير الشكوك حوله.

9- تحليل النتائج:

كلما تطورت تقنيات إخفاء المعلومات وتحسنت فان طرق الكشف عن الإخفاء تتطور بدورها أيضاً.

الإخفاء في النص: فان التغير الحاصل ممكن كشفه بالنظر إلى نماذج من النصوص ونسب توزيع الأحرف أو كمية الفراغات الغير عادية.

الإخفاء في الصور: أما الصور فممكن فحصها من اجل خواص مشكوك فيها وكشف النص المخفي يحتاج إلى أسلوب ذو تقنية أكثر وان التغيير في حجم وصيغة الملف ولوح الألوان ممكن أن يشير إلى وجود نص خفي. إن أكثر تقنية مستخدمة لكشف الصورة هو التحليل الإحصائي مثال خوارزمية LSB في هذه الخوارزمية الفرق بين البيانات العشوائية والبيانات الحقيقية ممكن كشفه بسهولة وكذلك كشف النص الخفي في صور JPEG باستخدام طريقة DCT.

الإخفاء في الصوت أو الفيديو: يستخدم أيضا التحليل الإحصائي ضد هذا النوع من الإخفاء وذلك لاستخدام LSB في الصوت أيضا إذ أن الترددات الغير مسموعة والتشويش والصدى والضوضاء في الخلفية الموجودة في الصوت تشير إلى وجود نص مخفي لذا فان هناك جمع من التقنيات تستخدم ضد الإخفاء في ملفات الصور والصوت أيضاً.

أما مع ملفات الفيديو فانه تستخدم تقنيات مختلفة لان استعمال إشارات في ملف الفيديو يكون من الصعب جدا اكتشافه بواسطة أنظمة الحاسوب.

مما سبق يتضح أن الإخفاء في النص والصورة والصوت أصبحت تقنيات تقليدية وذلك لتطور تقنيات كشف الإخفاء بالمقابل[6][12] .

أما في الإخفاء في صفحات HTML فان كشف الإخفاء من الصعب السيطرة عليه وذلك لوجود الملايين من صفحات الانترنت المنشورة بالإضافة إلى انه من القليل جدا أن يؤثر النص المخفي على خواص الغطاء صفحة HTML مما لا يثير الشك بوجود نص مخفي. والعامل الأخر الجدير بالذكر هو أن صفحة HTML لا يمكن الحصول على برمجة الصفحة (code source) إلا إذا تم نشرها وتحميلها إلى الخادم ومن ثم تعرض الخادم إلى هجوم من قبل أشخاص غير مخولين، هذا يعني إن قوة حماية الخادم من الهجمات الخارجية هو حماية إضافية للنص المخفي.

إن الطريقة الأكثر استخداما للحصول على النص المخفي هو إظهار برمجة الصفحة (source code) والذي يعتبر أكثر وأسهل الوسائل للوصول إلى النص المخفي وللحد من إظهار source هناك طريقتين:

في حالة استخدام لغة HTML فقط نضيف عدد من الأسطر ما يقارب (40-50) سطر من بيانات عشوائية في بداية الصفحة فإذا أراد احد المتصفحين عرض البرمجة المكونة لهذه الصفحة حصل على هذه البيانات العشوائية مما توحي له بان الصفحة مشفرة وبهذا قد يصرف النظر عن الصفحة أو قد يتحول هدفه إلى فك هذه الشفرة وبالتالي إبعاده عن النص المخفي.

أما في حالة استخدام Java script بالإمكان إضافة مقاطع برمجية تمنع المستخدم من عمل r click في الصفحة المعروضة لإظهار view source أو من قائمة view مما يؤدي إلى صعوبة الحصول على النص المخفي.

10- الاستنتاجات (Conclusions)

1) فن الاخفاء على خلاف الكتابة المشفَّرةِ، لا يَعتمدُ على الخوارزميةِ للتطبيقِ بل يَعتمدُ على السلوك البشري وطريقةِ التفكير.
2) نشر الموقع لكي يصبح متاحاً (لأي مستخدم) بإرسال نص مخفي وذلك بعمل واجهة يتم من خلالها إدخال النص واختيار الطريقة التي يتم بواسطتها إخفاء النص.
3) دمج بين طرائق الإخفاء في خوارزمية واحدة تزيد من قوة الإخفاء.
4) الدمج بين تقنية الإخفاء وتقنية التشفير من اجل زيادة الحماية للنص المخفي.

المصادر

1) الدكتور علاء حسين الحمامي, محمد علاء الحمامي, (2008), إخفاء المعلومات، كتاب.

2) شيماء شكيب, احمد سامي نوري (2004) "الإخفاء في ملف صوت مكبوس" أطروحة ماجستير، علوم حاسبات, كلية علوم الحاسبات والرياضيات, جامعة الموصل.

3) فوزي برزنجي, 2007 / 2008, فن الاختزال، كتاب.

4) Aelphaeis Mangarae [Zone-H.Org] "**Steganography FAQ**" March 18th 2006.

5) Ala'a H. Al-Hamami Prof. Dr. "**A Proposed Method to Hide Text Inside HTML Web Page File**" 24 Apr 2011 **9th European Conference on Information Warfare and Security**.

6) Asoke Nath, Sankar Das and Amlan Chakrabarti, **"Data Hiding and Retrieval"**, © 2010 IEEE.

7) Donovan Artz. "**Digital Steganography: Hiding Data within Data**" Los Alamos National Laboratory.

8) Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, **"Information Hiding|A Survey" 'Computer and Communications Security Reviews':** http://www.anbar.co.uk/computing/ccsr/ for copies of this journal.Version:$Id: bibliography.tex,v 1.25 1999-08.

9) I-Shi Leea, and Wen-Hsiang Tsai, **"Secret Communication through Web Pages Using Special Space Codes in HTML Files"**. International Journal of Applied Science and Engineering 2008. 6, 2: 141-149

10) Iuon-Chang Lin Ping-Kun Hsu, **"A Data Hiding Scheme on Word Documents Using Multiple-base Notation System"**, © 2010 IEEE.

11) Jammi Ashok, Y.Raju, S.Munishankaraiah, K.Srinivas, **"STEGA-NOGRAPHY: AN OVERVIEW"** International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5985-5992.

12) J.R. Krenn **"Steganography and Steganalysis"** January 2004. Hosting **COMPUTER FORENSIC INVESTIGATION** by Glasvezel.net.© 2002-2011 **FORENSICS.NL.** All rights reserved. Page last modified on Thu 21 January 2010 19:05:11 **CET DATA-HIDING.COM - LAWFULINTERCEPT.ORG**.

13) Sudeep Ghosh, **"StegHTML: A message hiding mechanism in HTML tags"**, December 10, 2007. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.597. hosted by The College of Information Sciences and Technology.

14) Yujun Yang, Yimei Yang, **"An Efficient Webpage Information Hiding Method Based on Tag Attributes"** 2010 Seventh International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2010).