فن الإختزال
بين الحقيقة والخيال

"عبادة الحارث" خليل قمر / هندسة برمجيات
حمزة لطفي شاهين / علم حاسوب

الأردن / جامعة الحسين بن طلال

2015

تنويه : جميع المكتوب هو تمحيص لأفكار مكتبسه لدراستي لهذا المجال بالإضافة لتفاصيل مأخوذه من مشروعي التخرج لذلك المعلومات الموجوده بهذا الكتاب هي كتابة وليدة اللحظة ما لم يتم ذكر مصدر ما .

[فَن الأختزال بين الحقيقه والخيال]

مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يُسمى نقل البيانات عَبرَ الشَبكة من مَوقعٍ لأخر أو مِن شَخصٍ لأخر بِشتى الطرق أصبح النظر إلى أمن وحماية تلك البيانات والمعلومات بشكل مُهم للغاية لذلك أصبح علم أمن المعلومات هو مَحل إهتمام لكثير من المستخدمين والباحثين التي تحاول جهودهم أن تتوصل إلى حُلول وتقنيات وأفكار جديدة تضمن نقل المعلومات بأمان من خِلال الشَبكة وخاصة شبكة الإنترنت دون حُدوث أي إعتراض أوإختراق وكشف لتلك المعلومات من قبل أشخاص غير مخولين في الحصول عليها ونتيجة لذلك يوجد العديد من التقنيات والأساليب التي تستخدم حالياً في أمنِ المَعلومات ومنها فن الإختزال أو ما يطلق عليه بعلم التضمين .

فإذا كانَ هذا العَصر عَصر التُكنلوجيا
فإن أَمـن المَعلومات هُو عِلمُ هَـذا العَصـر

عُبادة الحارث قمر
جامعة الحسين بن طلال / معان / الأردن

الإهـداء ..

هَـذا الكِتـاب هَديـة :

- إلى المرأه العظيمة الطيبة 'خِتام عويضة ' ومن غير أمي يستحق هذا الإهداء فأنتِ التي تعبتِ وسهرتِ ..

- إلى والدي وصديقي الشيخ ' خليل قمر ' .

كل الشكر والتقدير والإمتنان وبكل نجاح يغمر حياتي ويملأها سعاده , ولا توجد كلمات توفيكَ حقك يا أبتي الغالي الطيب .

- إلى أخواتي وكلا من المهندس 'عبدالرحمن' و 'حسان ' .

- إلى تلكَ الفتاة التي لا تليق بهذا العالم 'عرين' .

- إلى صديقي ورفيقي 'حمزة لطفي شاهين' .

'عُبادة الحارث' خليل قمر

الأردن / جامعة الحسين بن طلال

هَندسة بـَرمجيات

V_o@Hotmail.com

إمتنان وتقدير..

لأن الشكر أقل الواجبات ولأنَّ رسولنا الكريم أخبرنا بـأنـَهُ

" من لا يشكر الناس لا يشكر الله "

فـثمة شكر , نَخجل مِن أَنفسنا إتجاهَه وأخر نُقدمهُ وينتهي الأمر

لذلك مِن صَميم قَلبي أَبعث بِرسالةٍ مِلؤها التَقدير والإحترام إلى الرُبان الماهر الذي يستطيع أن يدير مَركبه ليوصل مَن مَعهُ في المركب إلى شاطئ الأمان

- الدكتور ليالي المزايده / رَئيس قِسم هَندسة البرمجيات

أشكرك على مابذلتيه من جهد من أجل تطويرنا علمياً بأسلوب مميز كأنتِ

- الدكتور مَالك الكساسبه / رئيس قسم علم الحاسوب

فقد أكتسبتُ بِفضلِ اللهِ ثم بفضله المزيدَ من التَفهم والإدراك في تخصصنا التكنلوجي فأنت تتمتع بأسلوب حِوار رَائع ونقاش هادف وإلى أسلوبك التحفيزي الرائع دمتَ رائعاً ومزيداً من التقدم

- الدكتور أيـمن ضـمور / عميد كلية تكنلوجيا المعلومات سابقاً مَنارة العِلم جَامعة , ومَنبع الأخلاق الرَائِعة , كُنتَ أباً حانياً ودكتوراً موجهاً معلماً , وأستاذاً رائعاً مميزاً وشخصاً جميلاً متواضعاً

ولا يسعني إلاّ أن أقف على قَدميَّ وأنا أتقدم بِالشُكر والعِرفان والإمتنان

لجامعة الحُسين بِن طَلال في مَدينة معان الأردنية ، وأشكر كل من أسدى لي عِلماً فيها.

تلميذكم : 'عباده الحارث' قمر

الإخـــتـــزال – Steganograpyh

- **مُقدمه :**

يأتي أصل مصطلح علم إخفاء المعلومات (Steganography) من الكلمتين الإغريقيتين: stegos والتي تعني السقف أو الغطاء و graphia والتي تعني الكتابة ويَصعب إيجاد مَعنى حَرفي باللغه العربية لـ Steganograpyh ذات الأصل اليوناني والتي تأتي بمعنى ' يُخفي ' أو ' يُغطي ' أما كـتعريف تكنلوجي

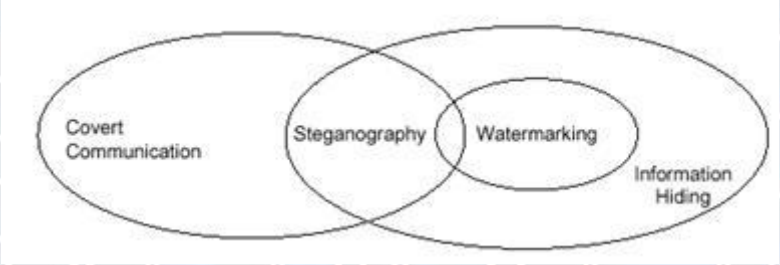
فهو فن وعلم إخفاء المعلومات وعِلم الأختزال هو العلم الذي يـَهتم باخفاء المعلومات الرقمية داخل وسيط إلكتروني دون إحداث أي تشويه أو تعديل ملحوظ في هذا الوسيط يعرف فنستطيع تعريفه على أنه إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى .

وهناك عدة تعاريف أخرى لعلم الأختزال من أبرزها تعريف العالمين جونسن و جوجوديا على أنه: «فن إخفاء المعلومات بطريقة لا تسمح باكتشافها» .

علم الأختزال لا يعد من العلوم المستحدثة، فلقد كان أول ظهور لهذا العلم في العصر الإغريقي، حيث قام أحد رجالات العصر بالتواصل مع احد أقربائه في اليونان، عن طريق حلق شعر رؤوس عبيده ثم وشم الرسائل على رؤوسهم بعد ذلك يقوم بانتظار نمو شعر رأسهم ثم إرسالهم إلى الشخص الذي يهدف إلى التواصل معه , ثم جاء بعده العديد من الأشخاص الذين استخدموا الناس والحيوانات والخشب المغطى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية , واستمر تطور هذا العلم، حتى توصل العالم إلى اختراع الحبر الخفي إبان الحرب العالمية الثانية، والذي ساهم كثيراً في التواصل بين أطراف الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الإسرار , وقد تطور علم الإخفاء في الوقت الحالي كثيراً، فأصبح يستخدم المعلومات الرقمية الحواسيب كوسيلة لنقل البيانات .

ومن تطبيقات حماية الحقوق الملكية أو الفكرية لجميع انواع الملفات الالكترونية، إستخدام العلامة المائية (Watermarking) وتم إستخدامها بشكل أساسي في عملية التجاره الإلكترونيه فمن خلال العلامه المائيه تستطيع أن تثبت بأنك المالك الرسمي للصورة أو ملف الصوت أو الفيديو. كما هي تبدو في خلفية هذا الكتاب , و العلامة المائية تعني إضافة معلومات معينة إلى الوسط الحامل بحيث لا تؤثر هذه الإضافات على إشارة الحامل إن كان من ناحية الرؤيا إذا كان هذا الوسط عبارة عن معلومات مرئية صورة مثلاً، أو من ناحية السمع إن كان الوسط الحامل عبارة عن معلومات صوتية. و تدل هذه العلامة على مالك هذه الصور و ذلك لحماية حقوق الطبع و النشر لهذا المالك، فمن يريد أن ينسخ تلك الصور لن يعلم أن هناك علامة معينة أضيفت لتلك الصور و يمكن أن تفضح أمره إن ادعى أن هذه الصور له. (ويكيبيديا)

- العلاقة بين الأختزال و المجالات ذات الصلة :



- مثال للتوضيح :

لنقل أن لديك معلومات أو ملفات رقمية (نص، صورة، صوت) تريد ارسالها لشخص ما لكي تصل بشكل آمن,ودعونا نطلق على تلك المعلومات والملفات الرسالة السرية , الرسالة السرية لن تُرسل بشكل مباشر ولكن يجب أن تدمج وتكون مخفية داخل رسالة الغطاء (نص، صورة، صوت) بشكل إحترافي دون ترك أي أثر أو شك بأن هناك رسالة سرية داخل رسالة الغطاء , وبالتالي تكون ناتج عملية الدمج هي رسالة التضمين والتي هي عبارة عن نسخة من رسالة الغطاء من حيث الشكل ولكنها تحتوي الرسالة السرية دون إحداث أي شك أو ريب بوجودها .

☒ لماذا لإختزال وليس التشفير ؟

يخلط كثيراً من المبتدئين في العلم المختص بحماية وأمن المعلومات بين فن التشفير و فن إختزال المعلومات ، معتقدين أن كِلا المُصطلحين يُعطي المعنى نفسه ، بينما كل مصطلح منهما يغطي علماً خاصاً من علوم أمن المعلومات , لأن هناك فرق كبير بين اختزال المعلومات وبين تشفيرها، ففي الأختزال المعلومات تكون مخفيه بحيث المستخدم العادي لن يكون على معرفة وعلم بوجود تلك المعلومات ، أما في التشفير فأن المستخدم يكون على علم بأن هناك معلومة مخفية ولكنها مشفرة غير مفهومة وهذا يعني أن الاختزال ليس جزءا من التشفير بل هناك فرق كبير بينهما .
وكذلك فإن علم التشفير يترك أثراً واضحاً في مَعالم الرسائل المُرسلة ولا يتَطلب وسطاً ناقلاً لإخفاء المعلومات (رسالة الغطاء) ويمكن إعتبار التشفير بِأنَه تغير المعالم الظاهره للرسالة المرسله (الرساله السريه) بإحدى الطرق والخوارزميات الكثيره بحيث يصعب فهمها بعد تطبيق عملية التشفير إلا من قبل المرسل والمستقبل فقط بينما الأختزال فإنه يتطلب وسطاً ناقلاً (رسالة الغطاء) يتم إخفاء البيانات بداخله كما أنه لا يشترط تغير في معالم الرسالة المرسله ولذا فإن أنسب طريقة لبناء نظام حماية قوي، هو الإعتماد على التقنيتين لجعل عملية إختراق النظام أكثر تعقيداً.
وهنا يظهر الفرق بين البيانات المطلوب إرسالها , فإنها ستكون مشفره إذا تم تطبيق خوارزميات التشفير , لكنها ستكون مخفيه اذا تم تطبيق خوارزميات الإختزال .
وقد يلاحظ البعض أن هذه العلم لا يتميز بانتشار واسع كما يتميز علم التشفير ، بالرغم من أهميته الكبيرة، وإن الغالبية العظمى من المبتدئين لا يميزون بين الفروقات الهائلة بين كلا العلمين , لذا في هذا الكتاب البسيط سيقوم بعرض المعلومات بطريقة مبسطة للمتلقي ، مما قد يُسهم في نَشرِ هذا العلم وإيضاح أهمية والفروقات بينهم وبين علم التشفير , وبما أن غالبية الأشخاص الذين لا يعرفون عن هذا العلم هم المبتدئين في علم أمن وحماية المعلومات، لذلك سيكون هذا الكتاب موجهاً بالدرجة الأولى لهم .

✓ يتوجب عليك فهم المقصود بالمصطلحات التاليه :

- ملف الغطاء : وهو ملف نستخدمه في عملية الإخفاء (للتمويه)
ومن الممكن أن يكون إما نصاً او صورة أو صوت

- الملف المضمن : وهو ملف يحتوي الملفات المطلوب إخفاءها
ومن الممكن أن يكون إما نصاً أو صورة أو صوت

- خوارزمية الإختزال : وهو الأسلوب الذي سيتم التعامل في عملية الاخفاء
ويوجد هناك العديد من الأساليب منها :

1 - LSB
2 - Watermarking
3 - wavelet transformation
4 - DCT
5 - Jstag
6 - F5
7 - RC4

وغيرها من الخوارزميات ...

- **المبدأ العام للإختزال :**

1 - إحضار ملف الغطاء وتحليله وتحضيره لإستقبال الرساله السريه .
2 - تحليل عناصر الملف المراد تضمينه (المراد إخفاء بياناته) .
3 - تطبيق الخوارزميه المناسبه للإخفاء .

وهكذا يصبح الملف جاهز للإرسال للطرف الأخر , وتم إخفاء البيانات بنجاح

الشكل (1) عملية أخفاء ملف التضمين داخل ملف الغطاء

- **أنواع الإختزال :**

يعتمد إخفاء المعلومات على الوسط المستخدم (رسالة الغطاء)
الذي بدوره سيحدد نوع الخوارزميه التي سيتم إستخدامها ومن أبرز أنواع الإختزال :

1 - إخفاء المعلومات في نصوص (الإختزال النص)
2 - إخفاء المعلومات في الصور (الإختزال الصوري)
3 - إخفاء المعلومات في الصوت والفيديو (الاختزال الصوتي)
4 - إخفاء المعلومات في صفحات الإنترنت (التضمين البرمجي)

وغيرها من أنواع الأختزال ..

فيتضح لدينا أن البيانات المستخدمة في الإخفاء قد تكون عبارة عن ملفات الوسائط المتعددة (multimedia) كالنصوص، الصور، و ملفات الصوت أو الفيديو وغيرها , وقد تكون أيضا عبارة عن ملفات تنفيذية للبرامج (executable file) وفي عملية الإخفاء نحتاج إلى توفر عنصرين مهمين لإتمام هذه العملية، الأول هو الرسالة التي نهدف إلى إخفائها والثاني هو الغطاء (cover) المستخدم لإخفاء هذه الرسالة.

ويعتبر الإختزال النصي , من أصعب الطرق للإخفاء , وهو النوع المفضل لدي لما يحتويه من تحديات وصعوبات في تضمين الرسائل المراد إخفاؤها ويعود سبب صعوبة الأختزال بها لصعوبة وجود بيانات زائده (redundant bits) يمكن إستبدالها , وإستغلالها بإخفاء الرساله السرية كما ان التعديل على النصوص يعتبر من السهوله كشف الإخفاء به وسهولة ملاحظة أي تغيرات أو تعديلات تطرأ على الكلمات المكتوبة
ويوجد عدة خوارزميات مهتمة بالأختزال النصي، وتختلف من لغة إلى لغة فمثلاً، طرق الأختزال في اللغة العربية ليست بالضرورة أن تكون قابلة للتطبيق على جمل اللغة الانجليزية ، والعكس صحيح، لذا قد يستفاد من التنقيط الموجود في أحرف اللغة العربية في اختزال النصوص المراد اخفاؤها، وكما هو معلوم أن حروف العربية غنية بالنقاط ، بل من الصعب أن تجد كلمة عربية بدون تنقيط ، مقارنة باللغة الانجليزية ، فلا يوجد سوى حرفين بهما نقاط هما (i، j)
أما الإختزال الصوري فهو الأسهل لما تحتويه الصور من خصائص الوسط المثالي لعملية الأختزال .

قلنا في أنواع الاختزال عن ملف الغطاء أنه يُمكن أن يكون ملفاً نصَياً، يجد القارئ في ذهنه علامة أستفهام، كيف يكون ملفاً نصياً، ويحتوي داخله بيانات نصية مخفية فيه، وحتى تتضح الفكره جيداً سأبدأ ببعض الطرق التقليديه المتبعه البسيطة التي يمكن تطبيقها بدون أدوات أو برامج ، ومن ثم سأنتقل إلى الطرق المتقدمة والتي قد تحتاج أدوات خارجية وبرامج .

سيكون بدايتها طريقة إستخدام الحرف الأول من كل كلمة
وتعتبر من أوائل طرق الأختزال النصي، يمكن تطبيقها على اللغة العربية والانجليزية، في هذه الطريقة، يجب بناء جمله مفهومة
بحيث اذا جمعت الأحرف الأولى (أو الأخيرة حسب اختيارك)
من كل كلمة تخرج بالرسالة السرية

- إليكَ هذا المثال :
(أنا لست قادراً دائماً سأحاول , سَوف يُكمل عُبادة وصيتَك دوماً)

الان لو قمت بإعادة قراءه النص أكثر من مره , بل وحاول تفسير الرساله أيضا لن تجد شيئاً يدل على وجود نص مخفي بداخلها علماً أنني قد أخبرتك إلى وجود نص مخفي داخلها , وقلت أنها أبسط انواع الاختزال أيضاً .
الأن , قم بكتابة أول حرف من كل كلمة واجمعها في جملة , وأقرأ ماذا سيخرج لك ولا تنسى أن تقول في نهاية الامر (بإذن الله) .

أو هذا المثال باللغة الانجليزية :
My elephant eats too many eels
" فيلي يأكل كثيراً من سمك الأنقليس "
وتظهر الرسالة بطريقة لا لبس فيها مطلقاً
Meet me
بمعنى " قابلني "

ورسائل محجوبة كهذه يسهل فك رموزها , وما أن يفشى السر حتى يتمكن أي شخص من قراءتها , ولهذه الطريقة عدة عيوب وهي: السعة المحدودة وعدم وجودة الليونة في تضمين النص السري، حيث يتوجب على المرسل بناء جمل مفهومة في نفس الوقت تحوي على حروف الرسالة السرية .

والطريقة الأخرى البسيطه تسمى إستخدام " النموذج "
وهي استخدام نموذج جاهز (قطعة جاهزة)
تحوي على فراغات، ثم عليك بتعبئة الفراغات بكلمات الرسالة السرية،

وهذا مثال عليها :

THE MOST COMMON WORK ANIMAL IS THE HORSE. THEY CAN BE USED TO FERRY EQUIPMENT TO AND FROM WORKERS OR TO PULL A PLOW. BE CAREFUL, THOUGH, BECAUSE SOME HAVE SANK UP TO THEIR KNEES IN MUD OR SAND, SUCH AS AN INCIDENT AT THE BURLINGTON FACTORY LAST YEAR. BUT HORSES REMAIN A SIGNIFICANT FIND. ON A FARM, AN ALTERNATE WORK ANIMAL MIGHT BE A BURRO BUT THEY ARE NOT AS COMFORTABLE AS A TRANSPORT ANIMAL

بالطبع الرسالة بالأعلى هي الرسالة بعد استخدام النموذج
وتعبئة كلمات الرسالة السرية، ولكي نستخرج الرسالة السرية نقوم بتطبيق
قوانين النموذج لكي نحصل على:

HE MOST COMMON WORK ANIMAL IS THE HORSE.
THEY CAN BE USED TO FERRY EQUIPMENT TO AND
FROM WORKERS OR TO PULL A PLOW. BE
CAREFUL, THOUGH, BECAUSE SOME HAVE SANK
UP TO THEIR KNEES IN MUD OR SAND, SUCH AS AN
INCIDENT AT THE BURLINGTON FACTORY LAST
YEAR. BUT HORSES REMAIN A SIGNIFICANT FIND.
ON A FARM, AN ALTERNATE WORK ANIMAL
MIGHT BE A BURRO BUT THEY ARE NOT AS
COMFORTABLE AS A TRANSPORT ANIMAL

فتكون الرسالة السرية :

Horse Ferry sank in Burlington. Find alternate transport

إستخدام Unicode Texts في الأختزال:

يمكن القول بأن هذه الطريقة هي من أجدد الطرق التضمين في اللغة العربية.
مكتشفا الطريقة هما دكتور وطالب من جامعة إيرانية .
كلمات اللغة العربية هي عبارة عن أحرف مرتبطة ببعضها البعض. فأي حرف إما أن يكون مشبوك بحرف آخر أو يكون مفصول بمسافة عن الحرف الذي يليه ، فيمكننا استغلال هذه الخاصية في الأختزال.
وحتى تكون هذه الطريقة واضحة يجب أن أقدم نبذة عن حرفين مهمين لتطبيق هذه الطريقة الحرفين متواجدين في ترميز Unicode Texts

Zero width joiner , ZWJ
Zero width non-joiner, ZWNJ

الحرف الأول (ZWJ) يعمل على ربط الأحرف ببعضها
دون ترك أي أثر للقارئ بوجوده، أي انه غير مرئي ولكنه لديه كود خاص وهو "U+200D"
الحرف الثاني (ZWNJ)، فيعمل عكس عمل الحرف الاول،

فهو يفصل الأحرف عن بعضها البعض دون اضافة أي مسافات،و هو أيضا غير مرئي
كود الحرف هو“U+200C“

الخوارزمية هي كالتالي:

في هذه الطريقة، المعلومات السرية والتي هي عبارة عن bits
تكون مخفية في كل حرف، أي كل حرف يمثل بت واحد (bit1)
فاذا كان الحرف في الكلمة متصل بالحرف الذي يليه
فسنضيف الحرف (ZWJ) بين الحرفين لكي نخفي بت 1
ولا نضيف شيئاً لكي نخفي بت 0
ولأن الحرف (ZWJ) غير مرئي، فانه لان يكون له أثر في النص.
أما اذا كان الحرف غير متصل بالحرف الذي يليه، فانا نضيف الحرف(ZWNJ)
بين الحرفين لكي نخفي 1، ولا نضيف شيئاُ لاخفاء 0
أيضا الحرف (ZWNJ) لن يكون له أثر مرئي في النص.
لذا يتبين لنا بواسطة اضافة الحرفين السابقين نستطيع اخفاء المعلومات
(صفر 0 ، واحد 1) دون تشويه النص الأصلي، ليس هذا فقط،
بل ما يميز هذه الطريقة أيضاً أنها تعتمد على ترميز عالمي
(Unicode Texts) ليس خاصاً باللغة العربية فقط. فالنص يمكنه أن يكون على
شكل HTML او مايكروسوفت ورد أو حتى نوت باد (Notepad)

أستخدام التبديل في الاختزال :

الأختزال بالتبديل، أن يتم تبديل كل حرف (أو حرفين أو كلمة) من النص الواضح
للرسالة بحرف أو رمز أو رقم أو كلمة بطريقة معينة يحددها المفتاح السري.

ومن أمثلة الإختزال بالتبديل ما يلي:
- إختزال ِعبادة بتبديل كل حرف بالحرف الذي يليه بثلاثة أحرف حسب الترتيب
الأبجدي كما في الجدول المبين لتصبح ِقهدزذ .
- إختزال ِعبادة· بالأرقام ِ70، 2، 1، 4، 5 حسب حساب الجمَّل،
أو بالأرقام 16، 2، 1، 4، 5 حسب الترميز العشري
-إختزال قمر بالحروف صي , ك ك , عقل

الحرف	أ	ب	ج	د	هـ	و	ز	ح	ط	ي
الترميز العشري	1	2	3	4	5	6	7	8	9	10
حساب الجمل	1	2	3	4	5	6	7	8	9	10
الحرف	ك	ل	م	ن	س	ع	ف	ص	ق	ر
الترميز العشري	11	12	13	14	15	16	17	18	19	20
حساب الجمل	20	30	40	50	60	70	80	90	100	200
الحرف	ش	ت	ث	خ	ذ	ض	ظ	غ		
الترميز العشري	21	22	23	24	25	26	27	28		
حساب الجمل	300	400	500	600	700	800	900	1000		

الشكل (2) الحروف وترميزها العشري وحساب الجمل التقليدي المستخدم في التراث العربي

وهناك عدة طرق أخرى سأقوم بتعدادها فقط للفائده :

1- طريقة استخدام نموذج (Tamplet) .
2- طريقة تغيير أماكن التنقيط .
3- طريقة استخدام المد (إطالة الكلمات باستخدام ـ)
4- طريقة استخدام التشكيل .
5- و طريقة استخدام Unicode Texts.

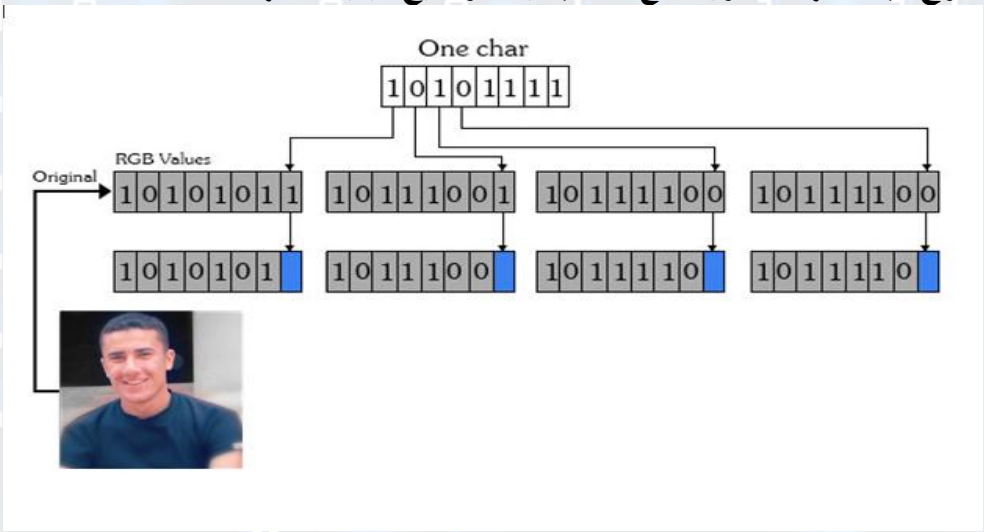
الأختزال النصي من أصعب طرق steganography
لقد قمت بذكر بعض الطرق المتبعة في الأختزال في اللغة الانجليزية والعربية ، ولكن يوجد المزيد و كما لاحظتم، أن جميع الطرق مبنية على أفكار بسيطة جداً ولكن لا أدري فعادة تكون تلك الطرق مخفية أمام أعين الناس لكي يكتشفوها ويفكروا باستخدامها حاول أن تفكر في طريقة جديدة ربما تكون من مخترعي ومكتشفي في علم الأختزال .

الاختزال الصوري :

وذلك عن طريق إخفاء الرسالة المراد إرسالها تحت ملف صوري، ويعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء. ويتم تطبيق هذه النوع من الإخفاء باستخدام أحد الطرق التالية:

1 - التحويل الزاوي المتقطع (direct cosine transformation)
2 - التحويل الموجي (wavelet transformation)
3 - والإخفاء باستخدام الإدخال في البت الأقل أهمية (LSB)

وتعد طريقة الإدخال في البت الأقل أهمية من أكثر الطرق شيوعاً، وفي ما يلي شرح مبسط لهذه الطريقه مع مثال بسيط لتوضيح كيفية عملها



الشكل (3) شرح خوارزمية البت الاقل اهمية

لنفرض أننا نريد إخفاء حرف واحد وهو الحرف A نقوم بتحويله للنظام الثنائي فتظهر لنا قيمته تتكون من 8 Bit اي 1 Bayt
ويكون كالتالي :
1010111 مثلاً , الأن ناخذ البكسل الأول من الصوره الشخصيه
وبتتكون من 4 Bay
هي كالتالي : RGB & alpha
وتكون قيمها مثلاً القيم الموجوده في الشكل (3)

R = 10101011
G = 10111001
B = 10111100
Alpha = 10111100

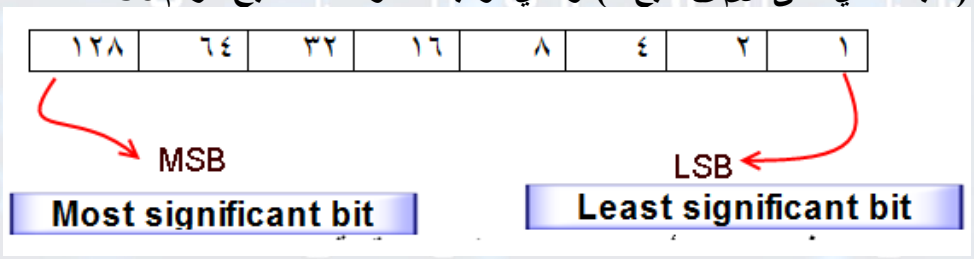
إن توزيع قيم Bits في bayt الواحد، يكون كالتالي:

128	64	32	16	8	4	2	1

وهذا ما يوضح أن Bit الواحد يمثل 256 قيمة
(من 0 في حال جميع البتات تحمل قيمة 0)
الى (255 عند ما تكون كل قيم البتات = 1)
فلو أردنا تمثيل الرقم 95 بطريقة النظام الثنائي، بالتأكيد سيكون:

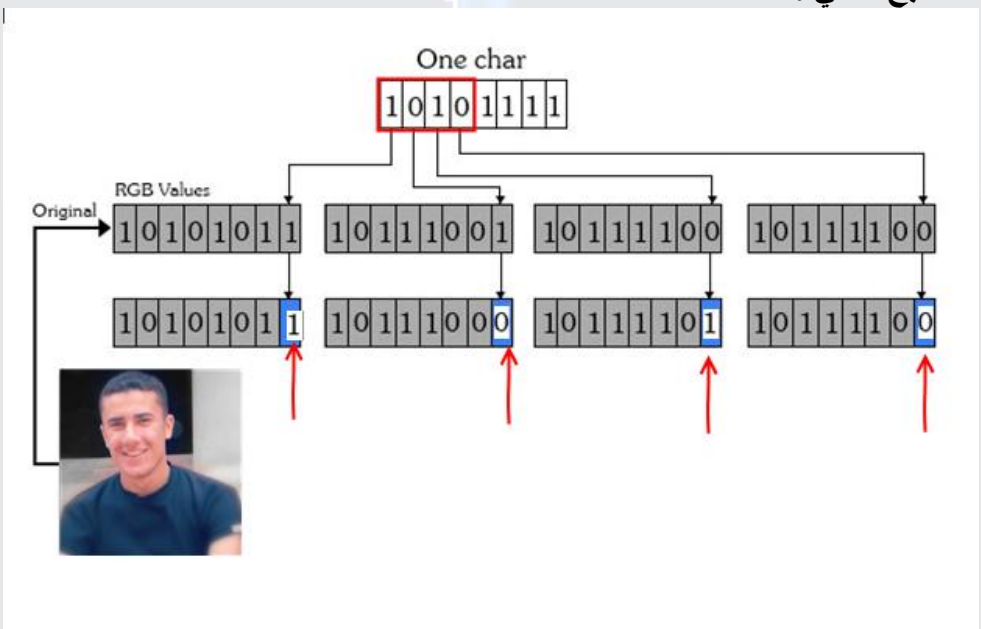
0	0	1	1	0	0	0	0

و في المرحلة الأساسية تعلمنا أن الرقم على اليمين يمثل أقل الأرقام تأثيراً، وكما يُسمى (الأحاد).
جرب معي أن تغير الرقم الذي على اليمين من 0 الى 1، سيصبح الرقم 96 بدلاً من 95 ، وجرب معي أن تغير البت على اليسار من 0 الى 1، سيصبح الرقم 223 .
هذا معناه أن البت الأخير هو البت الأقل أهمية
(البت الذي على اليمين طبعاً)،والذي لو جعلناه واحداً لأصبح الرقم 96



الشكل (4) نتائج عملية جلب القيم

والان بتعويض حرف الـ A مع الـ Bit الأقل أهمية نجد أن قيم الـ RGB ستصبح كتالي :



الشكل (5) شرح خوارزمية البت الاقل اهمية

بالنظر على الشكل (5) نلاحظ انه يجب علينا أن ناخذ 2 بكسل من الصوره حتى نستطيع إخفاء حرف واحد يتكون من 8 Bit

تستطيع مشاهدة هذه النتائج من خلال شاشة المخرجات على برمجية الـ C# من خلال الاكواد البرمجيه التالية , المكتوبه بشكل يدوي ☺
والكود فهمه سهل , إذ اننا نتعامل مع صور هذا يعني اننا نتعامل مع مصفوفه ثنائيه نقوم بإنشاء عداد للمرور على الاعمده وعداد للمرور على الصفوف

ومن ثم أمر احضار قيمة البكسل لكل من الالوان الثلاث الاحمر والاخضر والازرق

```
Bitmap img = new Bitmap(textBoxFilepath.Text);
for (int i = 0; i < img.Width; i++)
{
    for (int j = 0; j < img.Height; j++)
    {
        Color pixel = img.GetPixel(i, j);
        if (i < 1 && j < textBoxmessage.TextLength)
        {
            Console.WriteLine("R = [ " + i + "][" + j + "]= " + pixel.R);
            Console.WriteLine("G = [ " + i + "][" + j + "]= " + pixel.G);
            Console.WriteLine("B = [ " + i + "][" + j + "]= " + pixel.B);
            char letter = Convert.ToChar(textBoxmessage.Text.Substring(j, 1));
            int value = Convert.ToInt32(letter);
            Console.WriteLine(" letter: " + letter + " value: " + value);
            img.SetPixel(i, j, Color.FromArgb(pixel.R, pixel.G, value));
        }
```

الشكل (6) جلب قيم الالوان في البكسل الواحد

فهكذا سيكون شكل شاشة المخرجات

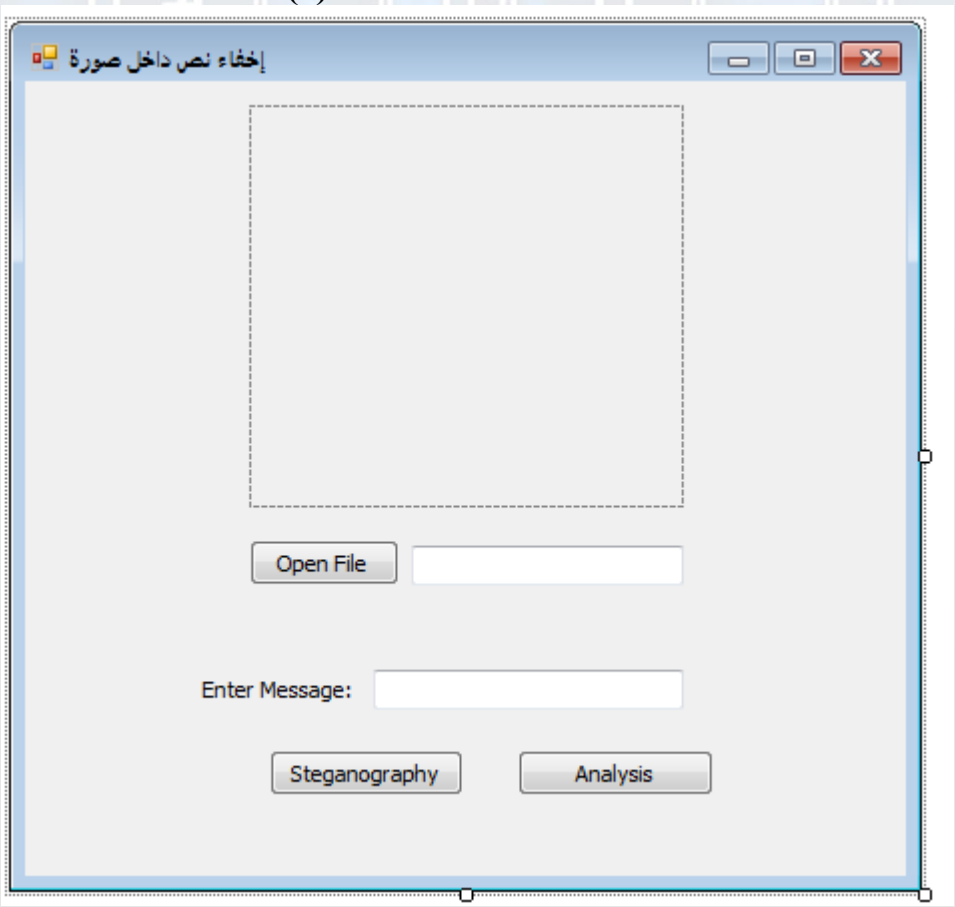
```
Output
Show output from: Debug
The thread 0x468 has exited with code 0 (0x0).
The thread 0x17e8 has exited with code 0 (0x0).
The thread '<No Name>' (0x1270) has exited with code 0 (0x0).
'Obadah_STE.vshost.exe' (Managed): Loaded 'M:\شغلي\مشروع التخرج\Obadah_STE\O
'Obadah_STE.vshost.exe' (Managed): Loaded 'C:\Windows\assembly\GAC_MSIL\Syst
The thread 0xa1c has exited with code 0 (0x0).
R = [ 0][0]= 19
G = [ 0][0]= 121
B = [ 0][0]= 205
 letter: A value: 65
```

الشكل (7) نتائج عملية جلب القيم

هذا يعني ان قيمة ASCII Code الـ R في البكسل 0و0 =19
هذا يعني ان قيمة ASCII Code الـ G في البكسل 0و0 =121
هذا يعني ان قيمة ASCII Code الـ B في البكسل 0و0 =205
وتكون قيمة ASCII Code للحرف A هي 56
فيتم تحويلها جميعها للنظام الثنائي ثم القيام بعملية الأستبدال

وصلنا لهذه المرحله وهي المرحلة المهمة في كتابنا , وهي صناعة برنامج
وأنا سأقوم بالعمل على برنامج بلغة الـ C#
وتستطيع انت التعامل مع أي لغة برمجيه حسب القدرات والخبرات التي تمتلكها .

أولاً) إخفاء نص داخل صورة :
ستجد سهوله بالغه إن كنت من مستخدمين لغة البرمجه C#
يتوجب عليك تحضير الأدوات كما هو ظاهر بالصوره (8)



الشكل (8) الأدوات التي سيتم استخدامها

وهي عباره عن :

Buttons 3
TextBox 2
Label 1
pictureBox 1

ثم نبدأ بكتابة الكود، ولكل أداة كودها الخاص بها ،

كود فتح ملف :

```
{OpenFileDialog opendilog =new OpenFileDialog ();
```

```
            OpenFileDialog opendialog = new OpenFileDialog();
            opendialog.Filter = " Image files (*.png ,
*jpg)|*.png;*.jpg";
            opendialog.InitialDirectory = @"C:\Users\ObadaH\desktop";
            if (opendialog.ShowDialog() == DialogResult.OK)
            {
                textBoxFilepath.Text =
opendialog.FileName.ToString();
                pictureBox1.ImageLocation = textBoxFilepath.Text;
                                                                }
```

مع مراعاة تغير إسم الجهاز , فكما نلاحظ هنا أن إسم الجهاز هو Obadah

كود Button
Steganography

```
Bitmap img = new Bitmap(textBoxFilepath.Text);
            for (int i = 0; i < img.Width; i++)
            {
                for (int j = 0; j < img.Height; j++)
                {
                    Color pixel = img.GetPixel(i, j);
                    if (i < 1 && j < textBoxmessage.TextLength)
                    {
                        Console.WriteLine("R = [ " + i + "][" + j +
"]= " + pixel.R);
                        Console.WriteLine("G = [ " + i + "][" + j +
"]= " + pixel.G);
                        Console.WriteLine("B = [ " + i + "][" + j +
"]= " + pixel.B);
                        char letter =
Convert.ToChar(textBoxmessage.Text.Substring(j, 1));
                        int value = Convert.ToInt32(letter);
                        Console.WriteLine(" letter: " + letter + "
value: " + value);
                        img.SetPixel(i, j, Color.FromArgb(pixel.R,
pixel.G, value));
                    }
                    if (i == img.Width - 1 && j == img.Height - 1)
                    {
                        img.SetPixel(i, j, Color.FromArgb(pixel.R,
pixel.G, textBoxmessage.TextLength));
                    }
                }
            }
            SaveFileDialog savefile = new SaveFileDialog();
            savefile.Filter = " Image files (*.png ,
*jpg)|*png;*jpg";
            savefile.InitialDirectory = @"C:\Users\ObadaH\desktop";
            if (savefile.ShowDialog() == DialogResult.OK)
            {
                textBoxFilepath.Text = savefile.FileName.ToString();
                pictureBox1.ImageLocation = textBoxFilepath.Text;
                img.Save(textBoxFilepath.Text);
            }
                                                                }
```

يرجى مراعاة تغير إسم الجهاز بالإضافه إلى الإنتباه ان عملية الحفظ تتم مباشره داخل نفس Button الإخفاء

كود Button
Steganalysis

```
Bitmap img = new Bitmap(textBoxFilepath.Text);
            string message = "";
            Color lastpixel = img.GetPixel(img.Width-1, img.Height-
1);
            int msglength = lastpixel.B;
            for (int i = 0; i < img.Width; i++)
            {
                for (int j = 0; j < img.Height; j++)
                {
                    Color pixel = img.GetPixel(i, j);
                    if (i < 1 && j < msglength)
                    {
                        int value = pixel.B;
                        char c = Convert.ToChar(value);
                        string letter =
System.Text.Encoding.ASCII.GetString(new byte[] { Convert.ToByte(c)
});
                       message = message + letter;
                    }

                }
            }
                                textBoxmessage.Text = message;
```

- الإختزال النصي :

ويمكن أن نعتبره تشفير ، لأن النص الناتج من هذه العملية يكون على شكل رموز ، لذلك يكون واضح لأي شخص بوجود شيء ما في هذا النص ..
كمثال على طريقة الإخفاء هذه (RC4 Algorithm)

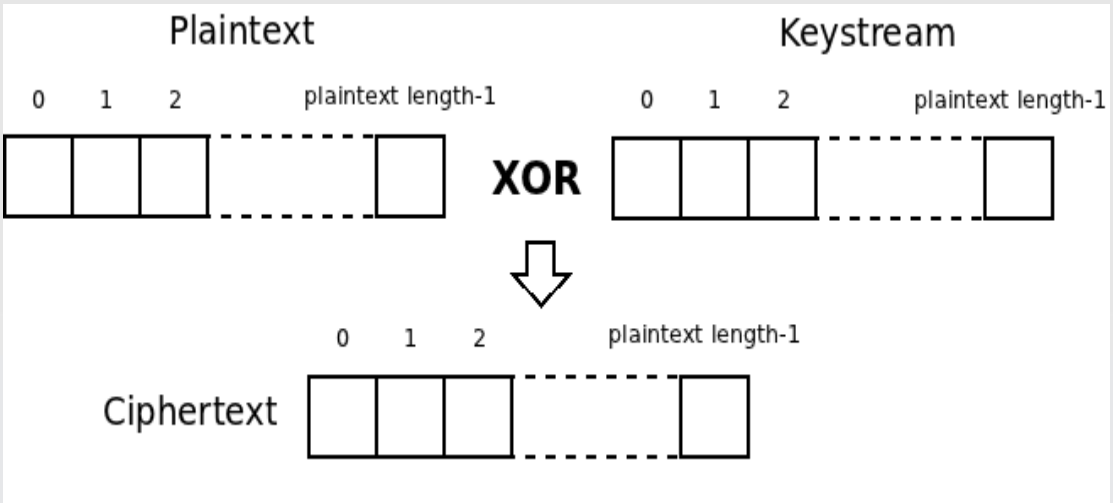
خوارزمية صممها "Ron Rivest" في عام 1989 وبقيت سرية النشر ، وتم نشرها في عام 1994 وكانت تستخدم في التواصل بين صفحات الويب والخوادم ، وهي عبارة عن خوارزمية تعتمد على التنقيل العشوائي بين النص المراد إخفائه والمفتاح لهذا النص .
الخطوات التي نستخدمها في RC4 هي KSA وبعدها الخطوة التالية PRGA

KSA(Key Scheduling Algorithm)

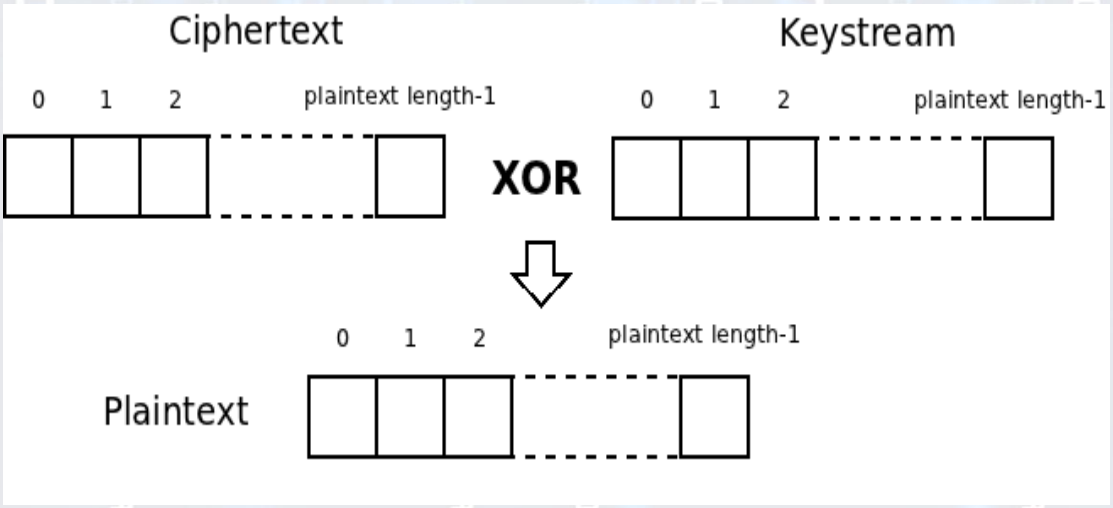
PRGA(Pseudo Random Generation Algorithm)

KSA(K)	PRGA(K)
Initialization: For $i = 0 \ldots N-1$ $S[i] = i$ $j = 0$ Scrambling: For $i = 0 \ldots N-1$ $j = j + S[i] + K[i \bmod \ell]$ $Swap(S[i], S[j])$	Initialization: $i = 0$ $j = 0$ Generation loop: $i = i + 1$ $j = j + S[i]$ $\text{Swap}(S[i], S[j])$ Output $z = S[S[i] + S[j]]$

- الإخفاء :



- فك الإخفاء :



- **وكمثال على هذه الخوارزمية :**

مثال بسيط طول فترة التشفير فيه byte-4

النص المدخل على الخوارزمية المراد إخفائه هو "HI"

والمفتاح المدخل على الخوارزمية هو 17

1 -يتم تخزين المفتاح في مصفوفه بعدد حروف المفتاح مع تكرار المفتاح إلى أن يصل عدد البايت في المثال

K={1,7,1,7}

2 -يتم إنشاء مصفوفه بعدد البايت في المثال وتكون محتوياتها الأرقام من 0 إلى N-1

S={0,1,2,3}

3 -يدخل على كود KSA ويبدأ كالآتي :

First Iteration (i = 0, j = 0, S = {0, 1, 2, 3}):
j = (j + S[i] + K[i]) mod 4 = (0 + 0 + 1) mod 4 = 1
Swap S[i] with S[j]: S = {1, 0, 2, 3}

Second Iteration (i = 1, j = 1, S = {1, 0, 2, 3}):
j = (j + S[i] + K[i]) mod 4 = (1 + 0 + 7) mod 4 = 0
Swap S[i] with S[j]: S = {0, 1, 2, 3}

Third Iteration (i = 2, j = 0, S = {0, 1, 2, 3}):
j = (j + S[i] + K[i]) mod 4= (0 + 2 + 1) mod 4 = 3
Swap S[i] with S[j]: S = {0, 1, 3, 2}

Fourth Iteration (i = 3, j = 3, S = {0, 1, 3, 2}):
j = (j + S[i] + K[i]) mod 4 = (3 + 2 + 7) mod 4 = 0 (mod 4)

Swap S[i] with S[j]: S = {2, 1, 3, 0}

4 -يدخل على كود PRGA ويبدأ كالآتي :

Reset i = j = 0, Recall S = {2, 1, 3, 0}
i = i + 1 = 1
j = j + S[i] = 0 + 1 = 1
Swap S[i] and S[j]: S = {2, 1, 3, 0}
Output z = S[S[i] + S[j]] = S[2] = 3
Z = 3 (0000 0011)

	H
	0100 1000
XOR	0000 0011
	0100 1011

i=1 , j=1 , S = {2, 1, 3, 0}
i = i + 1 = 2
j = j + S[i] = 1 + 3 = 4 (mod 4) = 0
Swap S[i] and S[j]: S = {3, 1, 2, 0}
Output z = S[S[i] + S[j]] = S[1] = 1
Z = 1 (0000 0001)

	I
	0100 1001
XOR	0000 0001
	0100 1000

بعد أن كان النص المدخل عندما مثلناه ASCII
(0100 1000 0100 1001)
أصبح بعد إدخاله على الخوارزمية
(0100 1011 0100 1000)
وهكذا نكون قد أتممنا شرح الخوارزمية ☺ .

- **الأختزال الفيديوي:**

يعتبر الإخفاء باستخدام ملفات الفيديو جزءا مشتقاً من الإخفاء باستخدام الصور، وذلك لأن ملفات الفيديو عبارة عن صور مجتمعة، لأجل هذا تقنيات الإخفاء بالصور يمكن استخدامها في هذه الطريقة
ومن أشهر الطرق المستخدمة في هذا النوع طريقة الإخفاء باستخدام التحويل الزاوي المتقطع (Discrete Cosine Transform)
وتقوم هذه الطريقة بإخفاء جزء من المعلومات في جزء معين من الصور التي يتكون منها الفيديو، وتمتاز هذه الطريقة بأنها غالبا لا يتم اكتشاف البيانات المخفاة بالفيديو باستخدام العين البشرية.
لكن يجب ملاحظة أنه كلما ازداد حجم البيانات المخفاة كلما كان كشفها أسهل في جميع الطرق المستخدمة للإخفاء.

- **الإخفاء الصوتي :**

ويتم في هذه الطريقة إخفاء الرسالة المراد إرسالها داخل إشارة صوتية ممكن أن تكون في مجال الزمن أو مجال الطيف.
ويتم بإحدى الطرق التالية : تغطية الإدراك أو الطيف الممتد .

- **كسر الأختزال (Steganalysis)**

يحتاج تحليل الأختزال بالطرق التقليدية إلى دراسة واسعة وخبرة طويلة ومثابرة غيرعادية ومعرفة بطبيعة المراسلة والمتراسلين , كما أن الحظ المجرد قد يؤدي دورًا في حل بعض طرق الأختزال ؛ إذ قد يكون من المستحيل حل رسالة مختزله قصيرة حتى ولو كان نظامها بسيطًا جدًا. ولكن محللي الأختزال الذين تتوافر لديهم المهارة والقدرة والوسائل التحليلية والوقت الكافي إضافة إلى عدد من الرسائل والمعلومات الجانبية عن طبيعة الرسائل والمتراسلين، قد يستطيعون حل أنظمة الأختزال البالغة التعقيد.
ولكل طريقة أو أداة ذكية لتطوير إخفاء المعلومات في البيانات المتعددةالأوساط، عدد مساو من الطرائق والأدوات الذكية التي تتطور لتحديد وكشف أسرارِها.
ومع تطور العلم والأساليب المستخدمة في الإخفاء فهنالك أساليب تتطور بموازاتها في فنتحليل وكسر هذا الإخفاء والحمايه لهذه المعلومات والبيانات .
ومع وجود الحاسوب أصبح فن تحليل الإخفاء من الأمور العسيرة والتي لا تستهلك وقتاً طويلاً في التنبؤ بوجود بيانات مخفية في ملف نصي أو صورة مُرسلة عبر البريد الألكتروني أو الأنترنت بصورة عامّة، ليستمر هذا ا الصراع قائماً لتخرج لدينا الأفكار والطرق الجديده والحديثه والاحدث ويتطور العلم وتتطور الوسائل
فهدف عملية الأختزال هو عدم إثارة أي نقطة للشك بوجود بيانات مخفية، واستراتيجية محلل الأختزال هو الشك في كل الرسائل المُرسَلة، وهذا لايعني صعوبة أو إستحالة هذه العملية، وكما قلنا أن وجود الحواسيب المتطورة والفائقة السرعة جعلت من فحص الملفات المُرسَلة أمراً ليس صعباً .
وهنا يكون دور القائم بعملية الإخفاء مهم جداً في إختياره ملفات الغطاء التي يصعب معها التمييز فيها اذا كانت قد احتوت على معلومات أ بيانات أو لا.
فمن الممكن إرسال صور شخصية، أو صور إحتفالات جماعية، أو ملف صوتي خاص وغير متوفر عند محللي الإخفاء، ومثال بسيط على ذلك، إستغلال ملف صوتي أو موسيقى ما او غيرها من الأساليب والطرق المتوفره في بيئتنا المحيطه .

- طرق كشف الإخفاء :

لعملية التحليل الإختزال خمسة طرق رئيسيه هي كالتالي :
1 - معرفة ملف الغطاء والخوارزميه المستخدمه .
2 - معرفة ملف الغطاء دون معرف الخوارزميه .
3 - معرفة انه يوجد إخفاء دون أي تفاصيل .
4 - التحليل العشوائي .
5 - معرفة ملف الغطاء مع وجود نسخه أصليه له .

وحتى اقوم بشرح هذه الطرق الخمسه , سأستعين بشرح الأستاذ فوزي برزنجي

خريج جامعة السليمانيه في العراق .

وهي كالتالي :

1 - الهجوم المباشر بعد معرفة ملف الغطاء و الخوارزمية المستخدمة:
هذه الحالة تنفذ عندما تكون المعلومات المسرّبة كافية لتعيين ملف الغطاء المستخدم، والخوارزمية المستخدمة في الإخفاء، وتُعتبر هذه الطريقة أسهل الطرائق الخمسة المتوفرة لدى المهاجم (المحلل).

2 - معرفة ملف الغطاء، دون معرفة الخوارزمية المستخدمة:
هذه الطريقة ليست صعبه على محلل الإخفاء، وكما أشرنا الى وجود الحاسوب المتطور الذي يمكّن المحلل من تجربة أكثر من خوارزمية متداولة أو طريقة مستخدمة في الإخفاء .

3 - معرفة انه يوجد إختزال :
ما يملكه المحلل هو فقط إشارة الى وجود إخفاء في أحد الملفات المُرسَلة، دون تحديد الملف المقصود ولا الخوارزمية المستخدمة، هنا يكون الهجوم على كل الملفات المُرسَلة وتخمين (تجربة) كل الخوارزميات المتوفرة لدى المحلل، هذه الطريقة قد تستهلك وقتاً، ولكن في النهاية قد تصل الى النتيجة المطلوبة.

4 - معرفة ملف الغطاء مع وجود نسخة أصلية لديه منها:
بمقارنة بسيطة بين عناصر ملف الغطاء الأصلي مع المرسل يستطيع محلل الإخفاء أن يكتشف الخوارزمية المستخدمة، وكسر الإخفاء المستخدم، وإستخراج البيانات السرّية المُرسَلة

5 - الهجوم العشوائي:
حيث لايمتلك المحلل أي معلومات عن وجود بيانات مُرسَلة، أو وجود ملف غطاء، وهذا ما يحصل كثيراً في شبكات الأنترنت، دون علمنا أو إنتباهنا، حيث أن الملفات التي تُرسل عبر الأنترنيت أو البريد الألكتروني تخضع (إن لم يكُن جميعها) فمعضمها، الى الفحص والتحليل وخصوصاً من شركات البريد الإلكتروني .

إنتهى بحمد الله