تم تحميل الملف من موقع
البوصلة التقنية
www.boosla.com

فن الإختزال

Steganography

إخفاء البيانات داخل الصورة

Hiding data within image

فوزى برزنجى

2008 \ 2007

إهداء

إلى روحك الطاهرة

إلى جسدك الطاهر

إلى كل مَلَك يزورك ليسلّم عليك وأنت نائمة مطمئنة

إلى التراب الذي تتوسدينه

إلى الأرض التي أحتضنتك طيّبة

إلى قبرك الذي صار الى روضة من رياض الجنة

إلى كل دقيقة أمضيتها بقربك

إلى كل لحظة أحسست بالأمان وأنا في حضنك

إلى التي أتوسل الى الله أن يحشرها مع النبيين والصديقين والشهداء

إلى التي أرتجي شفاعتها بعد شفاعة النبي

إلى أمّي (وكفى بمدلولاتها معانٍ)

أمّي

أهدي هذا الكتاب

إلى أخي الشهيد عمر عبد العزيز

الذي وضع قدمي على البرمجة وثبتها

أهدي هذا الكتاب

إلى أخي الحبيب المهندس فتحي عبدالعزيز

أهدي هذا الكتاب

إلى كل أخوتي وأخواتي وزوجتي وأولادي وأقاربي وكل أهلي

الهدف من هذ الكتاب

بعد التطورالذى طرأ على علوم الكمبيوتر في مجال الإتصالات والإنترنيت، ظهرت الحاجة الى إيجاد وسائل متعددة، لغرض إيصال المعلومات والبيانات بصورة صحيحة، ومحميّـة من الجهات غير المخولة لها بالإطلاع على هذه المعلومات ،ويندرج تحت هذه التقنيات والوسائل : التشفير ،العلامة المائية ،الكتابة المخفية، وإخفاء البيانات (الرسائل) داخل الملفات الصورية أو الصوتية أو كلاهما معاً (ملفات الفيديو).

وقد ظهرت وسائل التشفير منذ أزمنة قديمة، عملت على تشفير المعلومة، بشكل يصعب فهمه وتحليله (كشفه) ويمكن إعادة إسترجاعه بمفاتيح خاصة يملكه المشفر (المرسل) والمشفر اليه (المستلم).

إخفاء البيانات هو علم إخفاء المعلومات والبيانات السرية في غطاء رقمي مثل الملفات الصوتية، الصور أو ملفات الفيديو، وبحيث يصعب على المشاهد العادي حتى معرفة وجود شيء مخفي فيها .

ويعتبر هذا سبباً رئيسياً للتقدم الأوسع للكتابة المخفية مقارنة بطرق التشفير، لأن الكتابة المشفرة أو المشوهة يدفع المتابع الى الخوض بشتى الوسائل للحصول على المعلومة الأصلية ومحاولة كسر الشفرة، في حين أن الكتابة المخفية لا تثير الشك عند المشاهد العادي، وقد يمر عليه مرور الكرام دون أن يترك أثراً للمعلومة المخفية داخل الملف المضمّن.

عرضتُ في هذا الكتاب أكثر طرائق إخفاء البيانات شهرة، ثم تطرقت بتفصيل أكثر الى الطريقة المستحدثة، وهي إستغلال البت الأقل أهمية Least significant bit للحصول على أفضل نتاج ممكن لإخفاء النص داخل الصورة.

الكتاب يحتوى على عرض لتأريخ إخفاء البيانات، مع مراجعة سريعة للصور الرقمية، وأنواعها، بالإضافة الى تحليل خوارزمية البت الأقل أهمية ثم شفرة البرنامج المرفق مع هذا الكتاب.

fowzibarazenji@yahoo.com

شكر وتقدير

أتقدم بخالص الشكر والتقدير الى منتدى فيجوال بيسك للعرب www.vb4arab.com على تيسيره لي نشر هذا الكتاب، وأشكر كل أعضاءه الكرام، بكل درجاتهم، على المازرة التي أبدوها لي في إتمام الكتاب ونشره، تحية للمشرف العام وكل المشرفين الكرام وكل أعضاء المنتدى الكرام، وكلهم إخوتي في العلم ونبراساً في الأخلاق.

كذلك أتقدم بخالص الشكر والتقدير الى منتدى فيجوال سي للعرب www.vc4arab.com على تيسيره لي نشر هذا الكتاب هم أيضاً، وأشكر كل أعضاءه الكرام، وبكل درجاتهم، على ما أبدوه من ترحيب لي ولكتابي هذا، تحية للمشرف العام وكل المشرفين الكرام وكل أعضاء المنتدى الكرام، وكلهم إخوتي في العلم ونبراساً في الأخلاق.

كل الشكر والتقدير أزينه وأقدمه كتحية حب وتقدير لموقع البوصلة التقنية www.boosla.com الذين أسهموا مع المنتديين الكريمين في توسيع نطاق نشره، والإستفادة منه قدر الإمكان.

تحية شكر مقدماً لكل مواقع الإنترنيت التي ستنشر هذا الكتاب ليستفيد منه إخوتي وأخواتي، في العاراق وكل الدول العربية والإسلامية.

تحية لكل العاملين في هذا الموقع الرائع، تحية تقدير وإحترام لكل ما يبذلونه من جهد في سبيل رفع المستوى العلمي للمسلمين.

fowzibarazenji@yahoo.com

المحتويات

fowzibarazenji@yahoo.com

فن الإختزال Steganography

الفصل الأول

- **مقدمة:-**

ما المقصود بـ (فن الإختزال Steganography) ؟ .

هو علم وفن إخفاء البيانات المُراد إرسالها (قد تكون رسائل نصّية أو صورية) داخل بيانات مُرسلة (ويُفضّل أن تكون صور من نوع bmp او ملفات الصوت او الفيديو، وذلك لإحتواها على كمية كافية من البيانات التي تُمكّن المبرمج من إخفاء البيانات داخلها) .

يختلف فن الاختزال عن الكتابة المشفرة cryptography فبينما تتعمل الكتابة المشفرة على إخفاء محتوى الرسالة، يعمل فن الاختزال على اخفاء وجود ملف آخر في الرسالة .

يتلخص مبدأ تقنية فن الإختزال باختصار في إخفاء البيانات ضمن البيانات، كإخفاء رسالة نصية ضمن صورة أو ملف صوتي أو ملف فيديو، وهي طريقة جديدة تستخدم كبديل لتقنية التشفير المعروفة.

أما كيفية عمل هذه التقنية فيتمثل في الاستفادة من الـ bits غير المهمة، أو تلك التي يصعب اكتشافها في حال تم تحويرها، ,الموجودة ضمن ملف الصورة أو الصوت أو الفيديو، واستخدامها لإخفاء الرسالة المضمنة.

وما يميز هذا النوع من الرسائل المخفية هو أنها تصل إلى وجهتها بشكل سري تماماً، على خلاف الرسائل المشفرة التي على الرغم من أنه لا يمكن أبداً فك شيفرتها من دون الحصول على مفتاح التشفير، فإنه بالإمكان تحديدها كرسالة مشفرة.

تهدف تقنية فن الإختزال (Steganography) التي سيتم الحديث عنها في هذا الكتاب، إلى إخفاء البينات داخل بيانات أخرى، بطريقة لا تؤدي إلى التأثير في هذه الأخيرة، بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف الحقيقة، والغرض من عملية الإخفاء هذه أن لا يعلم المهاجم المحتمل عن وجود هذه البيانات، وبالتالي يتم حمايتها من القراءة أو التغيير أو التدمير عن طريق هذا المهاجم، لأنه إذا كنت لا تعلم بوجود شيء ما أصلاً فكيف يمكن لك الاستفادة منه أو تدميره؟.

وهذا يعني أنّ فن الإختزال ليس جزأ من فن التشفير، فالفرق بينهما كبير وعلى سبيل المثال فإن علم التشفير يترك أثراً واضحاً في معالم الرسائل المرسلة، ولا يتطّلب وسطاً ثانياً لإخفاء البيانات،

fowzibarazenji@yahoo.com

ويمكن القول أن التشفير هو تغيير المعالم الظاهرة للنص المُرسَل بإحدى خوارزميات التشفير الكثيرة، بحيث يصعُب فهمها بعد تشفيرها، الاّ من قبل المرُسِل و المُستقبِل، بينما فن الإختزال كعلم يتطلّب وسطاً ثانياً يتم إخفاء البيانات داخله، ولا يشترط تغيير معالم البيانات المُرسَلة.

وهذا الذي يجعل هذه التقنية مختلفة عن التشفير(Cryptography)، ففي التشفير يعلم المهاجم بوجود هذه البيانات، وقد يستطيع الوصول إليها، لكنه لا يستطيع قراءتها إلا بعد كسر الشفرة، لكنه قادر على إزالتها إذا شك فيها مثلاً .

ولا ضرر من دمج العلمين معاً في العمل الواحد، وبالتأكيد سيضيف قوة ومتانة فيتم تطبيق إحدى خوارزميات التشفير على البيانات المطلوب إرسالها أولاً، ثم يتم تطبيق احدى خوارزميات الإختزال، وفي رأيي ستكون البيانات المُرسلة في منأى عن اكتشافها أولاً، ويَصعُب فك تشفيرها إن تم الكشف عن وجودها.

وهذا يعني أن البيانات المطلوب إرسالها، تُسمى بيانات مُرمّزة (مشفّرة Encoded) في حال تطبيق فن التشفير عليها، بينما تسمى بيانات (مخفية Hidden) في حال تطبيق فن الإختزال عليها.

- **لمحة تأريخية لفن الإختزال:**

إنّ كلمة Steganography اليونانية الأصل والمعنى والتي يعود تأريخها الى العام 440 قبل الميلاد، تعني لغوياً التغطية أو الإخفاء، ويشير التأريخ الإغريقي القديم الى إستخدام فن الـ Steganography عندما كانو يكتبون الرسائل المهمة على لوح خشبي ثم يغطون اللوح بالشمع و يكتبون على الشمع مالايثير الشُبهة أوالإهتمام ويرسلونه الى الجهة المطلوب الإرسال اليها.

وهنالك فنون أخرى عندهم في إستخدام الـ Steganography، فعلى سبيل المثال حلق رأس الجندي وكتابة الرسائل بطريقة الوشم عليه، ويتركونه حتى يطول شعره فيغطي الكتابات، وفي هذه الحالة يكون رأس الجنود عندهم الوسط الناقل للرسائل السريّة، ولم يذكر التأريخ فيما إذا يعود الجندي بعد توصيله الرسالة، أو هل يمكن إعادة استخدام نفس الجندي في حال رجوعه سالماً، أم إنه من نوع الDisposable، ويقبل الإستخدام مرة واحدة فقط ، وإن كانت هذه الطريقة وحشية بعض الشيء، بمقاييس عصرنا بالطبع. حيث حلق رؤوس العبيد، ثم (وشم) الرسالة السرية على هذه الرؤوس البائسة.

fowzibarazenji@yahoo.com

في العصور الوسطى أصبح فن الإختزال شيئاً معروفاً، فاستخدمت الكتابة السريّة من قبل الكنيسة الكاثوليكيّة في صراعاتها المتعدّدة عبر التاريخ و من قبل الحكومات أيضاً في تلك الفترة. كما و استخدم علم فن الإختزال بشكل متلازم مع الكريبتوغرافي للحصول على إخفاء أفضل للمعلومات.

في أواخر عام 1400 م كتب الراهب تريثميوس العديد من كتب الدين عن حياة أشخاص هامّين من أمراء، و رهبان، و كذلك عن حياة سانت ماكسيموس وغيره. وفي عام 1499 م كتب مجموعة من الكتب سمّاها ستيغانوغرافيا وصف فيها طرقاً و أنواعاً من الكتابة المخبّأة .

و في فينيسيا عام 1500 م، كان تحليل الأسرار و فك رموز الرسائل المشفرة هامّ جدّاً عند حاكم المدينة كونسيلتين، مما ولد اهتماماً عاماً لدى رعيته بهذا الموضوع فما إن كانت تقع رسالة مشفّرة في أيدي أهالي فينيسيا كانوا يترجمونها على الفور بسبب الخبرة التي أضحت لديهم، حيث أجرى كونسيلتين ندوات حول التشفير قدم فيها العالم ماركو روفائيل طرقاً جديدة و متنوعة لأساليب و طرق الكتابة الخفيّة.

في ميلان ولد العالم جيرولامو كاردانو عام 1501م، و نشر 131 كتاباً وخلّف وراءه 111 مخطوطة، ناقش فيها الرياضيات و الفلك و الفيزياء و الشطرنج و الموت، وكتب أيضاً كتابين عن الكريبتوغرافي، كما صنّع شبكة كاردانو وهي عبارة عن صفيحة مصنوعة من مادّة قاسية فيها فتحات مستطيلة الشكل موزّعة عليها بشكل غير منتظم، وتستخدم هذه الصفيحة لإخفاء رسالة سرّيّة ضمن رسالة عادية، حيث يقوم الشخص الذي يريد تشفير الرسالة بوضع هذه الشبكة على ورقة المراسلة و يكتب رسالته السريّة عبر الفتحات التي توفرها له الشبكة، هذه الفتحات يمكن أن تضم كلمة كاملة أو حرفاً، يتمّ بعد ذلك إزالة الشبكة و ملء الفراغات المتروكة برسالة تغطي الرسالة السرّيّة وبشكل غير مؤذٍ لها، فالشخص الذي سيفكّ رموز الرسالة يضع الشبكة التي يملكها على الرسالة المستقبلة ويقرأ المعلومات المخبّأة فيها عبر الفتحات. المشكلة في هذه الطريقة هي أنّها بحاجة لبراعة في تركيب العبارات لذا فإنّ الضعف في التراكيب قد يفضح حقيقة وجود رسالة مخفيّة ضمن الرسالة الحاملة. استخدمت شبكة كاردانو من قبل العديد من الدول في مراسلاتها الدبلوماسيّة في الفترة ما بين 1500 م و 1600 م .

في عام 1641م كتب جون ويلكينس، أسقف تشيستر، أوّل كتاب في الإنكليزيّة عن منطق التشفير، حيث وصف نظاماً يتمّ فيه تقديم الرسالة بشكل نقط و خطوط و مثلثات، فيعبَّر عن الأحرف بنقط ثمّ يتم وصل هذه النقط لتشكّل خطوط ومثلثات، و في النهاية تبدو الرسالة المشفّرة على شكل رسم أو نوع ما من أنواع الصور.

fowzibarazenji@yahoo.com

في عام 1779م تم اكتشاف الحبر السري على يد جيمس جاي، وهو فيزيائي يعيش في لندن واستخدم من قبل العملين الأمريكيين صموئيل و ودل و روبرت تاونسند، لقد اعتمدوا على أرقام الصفحات والأسطر في كتب معيّنة مستخدمين الحبر غير المرئي لكتابة رسائلهم عند هذه الصفحات والأسطر.

في أوائل عام 1800 أصبح لدى معظم الدول الأوروبيّة خدمات سرّيّة وظهر آنذاك ما عرف باسم الغرف السوداء، و هي عبارة عن مكان يضمّ مجموعة من الأشخاص يفحصون الرسائل الخاصّة بالغرباء و المشبوهين، كمثال على هذا كان الإنكليز يتفحصون مراسلات الشعب الأمريكي الذي ظهر حديثاً على الساحة، و الذي كان يكتب رسائله السرّيّة بالحبر السرّي، حيث تمكن بعض الكيميائيّين الإنكليز من اكتشاف عدد من الرسائل المكتوبة بحبر سرّي.

أما في العصور الحديثة، و في الحربين العالميتين الأولى والثانية، فقد استخدم الحبر السرّي على نطاق واسع، و نذكر على سبيل المثال طريقة أنيس التي يتمّ فيها وضع نقاط من الحبر السرّي على أحرف معيّنة من جريدة أو كتاب بحيث تشكّل هذه الأحرف بمجملها الرسالة السرّيّة.

لكن الجرائد كانت تنقل كرسائل من الدرجة الثالثة من حيث الأهمية لذا فإن هذا الأسلوب لم يكن الأسرع لإيصال المعلومات إلى حيث ينبغي. في عام 1940م أوقف مكتب المراسلات البريطاني في برمودا إحدى الرسائل لأنّها بدت مختلفة عن باقي الرسائل، و تبعتها العديد من الرسائل لنفس الكاتب، وقد تمكّن العلماء الإنكليز بعد إجراء تجارب وتحاليل من اكتشاف حبر سرّي على الوجه الخلفي للرسالة.

نفس المحطّة في برمودا اكتشفت رسائل مكتوبة بنفس الحبر السرّي، وأدّى ذلك إلى إعدام رجل في كوبا لإرساله معلومات سرّيّة عن السفن الموجودة في ميناء هاربر في هافانا، و كان هذا الرجل قد استخدم رسائل مكتوبة باللّغة الأسبانية ليضع فيها المعلومات السريّة، إلاّ أنّ أسلوبه في الكتابة الإسبانية كان له طابع ألماني مما أثار الشبهة فيها و أدّى إلى فضح أمرها.

لقد قام الجواسيس النازيّون بالعديد من التجارب والقياسات لإحباط اختبارات الكتابة السريّة التي ينفذها مكتب مراقبة المراسلات.

ومن الطرق التي أوجدها الجواسيس فصل قطعة الورق إلى قطعتين و كتابة الرسالة السريّة بحبر سرّي على الوجه الداخلي ثمّ إعادة دمج القطعتين في قطعة ورق واحدة. و حيث أنّ الحبر السرّي موجود في داخل الورقة فإنّ وضع أيّ كاشف على سطح الورقة لن يكفي لإظهار الكتابة السريّة.

fowzibarazenji@yahoo.com

- **تمهيد:-**

مع تطور الحياة أصبح للSteganography وجود مهم في تناقل البيانات السريّة وخصوصاً مع وجود إمكانية النقل الهائل والسريع عبر شبكات الإنترنيت، اضافة الى تداخل فن التشفير مع فن الإخفاء، الذي زاد من صعوبة الكشف عن الإخفاء وفك التشفير معاً .

حاليا تشغل الأبحاث في مجال هذه التقنية، حيزا كبيرا من اهتمام الباحثين، لسبب بسيط وهو أن لها استخدامات هامة في التجارة الإلكترونية، التي تزداد تطبيقاتها، والاهتمام بها يوما بعد آخر. حيث من تطبيقاتها العلامات المائية أو ما يعرف ب (Watermarks). وتستخدم هذه الأخيرة في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة، مثل الاسطوانات الخاصة بالموسيقى وغيرها، وكذلك الصور والبرامج التي تباع عبر الإنترنت. فبالرغم من المشتري هنا قد يعلم بوجود هذه العلامات، لكنه لا يعرف أين توجد داخل المنتج، ولا البرنامج الذي استخدم في عملية الإخفاء، ولا كلمة السر ومفتاح التشفير، وبالتالي يصعب عليه، إزالتها، وإعادة النسخ.

لذا يمكن القول أن فن الإختزال هو إخفاء رسالة ما (بيانات) داخل رسالة أخرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولى، لهدف محدد. والبيانات المستخدمة كظرف أو وعاء للإخفاء يمكن أن تكون عبارة عن ملفات الوسائط المتعددة (الملتيميديا) كالصور، والنصوص، وملفات الصوت أو الفيديو، وغيرها. وقد تكون كذلك ملفات تنفيذية لبرامج مختلفة من نوع (exe). وهكذا في عملية الإخفاء هذه نحتاج إلى ملفين أحدهما يسمى الغطاء(cover)، والآخر هو المادة المراد إخفاؤها.

ويُعَرفها(Jojodia & Johnson 1998) على أنها " فن إخفاء المعلومات بطريقة لا تسمح اكتشافها".

يتطلب عمل ملف مختزل وجود ثلاثة أشياء مهمة وهي الملف الأصلي المراد اختزاله والملف الناقل الذي سيخفي الملف الأصلي واخيراً الخوارزمية التي سيتم تطبيقها في برنامج الاختزال.

fowzibarazenji@yahoo.com

- **المصطلحات العلمية المستخدمة مع فن الإختزال:-**

من المهم أن أعطي التعريف المبسّط للمصطلحات التي ستتردد كثيراً في معرض كلامنا عن الـ Steganography في هذا الفصل والفصول اللاحقة، وهي:

أ- ملف الغطاء : وهو ملف نصّي أو صوري أو صوت أو فيديو، نستخدمه في إخفاء البيانات المطلوب إخفاها فيه، يتم الإختيار حسب كمية البيانات المطلوب إخفاءها، ومدى إستيعاب ذلك الملف لتلك البيانات، مع مراعاة خفض نسبة التشوه الذي يحصل له عند إدخال البيانات، ويفضّل عند إستخدام ملف صوري أن تكون الصورة من نوع (الخريطة النقطية Bitmap) لكبر حجمها وقابليتها على استيعاب البيانات بسهولة، وبرمجياً سهولة إعادة خزنها، خصوصاً بلغة الفيجوال بيسك 6، بعد اخفاء البيانات داخلها، أمّا ملفات الصوت فتقريباً أغلب أنواع الملفات الصوتية قابلة للإستيعاب، أما ملفات الفيديو فبإمكانها إخفاء أكبر حجم من البيانات، وذلك لأنها تمثل في خصوصيتها الجمع بين الملفات (الصورية + الصوتية)، ولكن ما يقلل إستخدام النوع الأخير من الملفات كُبر حجمها وبطئ تناقلها عبر الإنترنيت .

ب- الملف المضمَّن : هو ملف يحتوي البيانات المطلوب إخفاءها، وقد يكون نص رسالة أو صورة، مع ملاحظة حجم تلك البيانات ومقارنتها بملف الغطاء المستخدم، وعلى العموم لاتكاد تقارن الملفات النصية بحجمها مع حجم الملفات الصورية، ويفضل عند إستخدام الملفات الصورية أن تكون من نوع JPG أو مثيلاتها في الحجم .

ت- خوارزمية الإخفاء : الأسلوب الذي سنعتمده في إخفاء البيانات، وهنالك عدة خوارزميات معتمدة في الإختزال، ومنها:

1. **خوارزمية البت الأقل أهمية Least significant bit.**
2. **تحويل الجيب تمام المباشر direct cosine transformation.**
3. **العلامة المائية Watermarking .**

1. خوارزمية البت الأقل أهمية Least significant bit :

الحديث بالتفصيل عن هذه الخوارزمية في الفصل الثالث، مع تطبيق برنامج بلغة فيجوال بيسك 6 لإخفاء نص رسالة ما داخل ملف صوري من نوع BMP في الفصل الرابع.

fowzibarazenji@yahoo.com

2. تحويل الجيب تمام المباشر direct cosine transformation:

يتم التعامل في هذه الخوارزمية مع عناصر الصورة بشكل رياضي بحت، حيث يعتمد فكرة إستخدام دالة الجيب تمام الرياضية، في تحليل عناصر الصورة وإخفاء الرسالة المراد إرسالها بذلك الإسلوب.

3. العلامة المائية Watermarking :

تعتبر هذه العلامات الرقمية من أهم تطبيقات التقنية التي نتحدث عنها، وأكثرها رواجا واستخداما. فالعلامة الرقمية المائية، هي رسالة مخفية داخل صورة رقمية، أو ملف صوتي، أو ملف فيديو رقمي أو غيرهم من الملفات الرقمية التي يتم تداولها تجاريا. ويتم تخزين هذه الرسالة داخل محتويات الملف ذاته، فلا تحتاج لمساحة إضافية للتخزين. فالمساحة مهمة جدا ومحدودة، ولذلك فإن هذه الرسالة (العلامة) غالبا ما تكون صغيرة، أي تحوي كمية محدودة من البيانات، رقما ما غالبا. ويمكن أن تكون هذه العلامة المائية عبارة عن اسم المنتج، اسم الناشر، بيانات الشركة، رقم تسلسلي، أو رقم تعريف خاص بالمشتري تضمن له حقوقه في ملكية ما اشتراه وتحميه في حالات التحقيق. كما قد توضح له عدد النسخ المسموح له إنتاجها منها .

وقد اكتسبت العلامة المائية الرقمية هذه الأهمية، لأنها تسهم في حفظ حقوق الطبع والنشر والتأليف والملكية في العالم الرقمي، في ظل تزايد عمليات القرصنة والاستنساخ غير المشروع، خاصة عبر الإنترنت. ومع تنامي التجارة الإلكترونية، تزداد الحاجة لتقنية تحفظ هذه الحقوق، فغياب وسيلة فعّاله حتى الآن في التدقيق والمحاسبة من أجل الحفاظ عبر الملكيات، مشكلة كبيرة لهذا النوع من التجارة، خاصة للأعمال الفنية والموسيقية .

شكل(1) لاحظ العلامة المائية الحمراء كمثال على طريقة Watermarking لمنع تزوير العملة النقدية

fowzibarazenji@yahoo.com

الفرق الرئيسي ما بين فن الإختزال التقليدي وما بين العلامة المائية، أنه في الحالة الأولى يتم إخفاء البيانات، حيث تكون هذه البيانات هي الهدف من عملية الاتصال والتبادل، وهي التي يراد حمايتها.

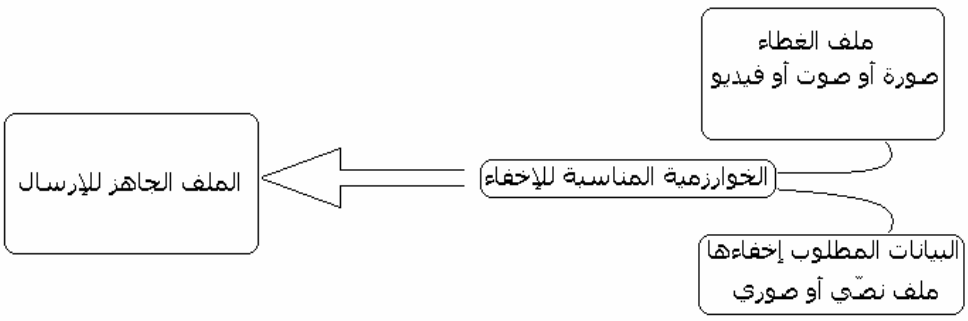
بينما في الحالة الثانية، فإن المادة الرقمية نفسها، أو الملف الرقمي ذاته، هو الهدف من عملية الاتصال والتبادل والحماية، والبيانات المخفية في داخله تصبح جزء منه، وتهدف إلى الحفاظ عليه، وتنظيم عملية تبادله.

ففي الحالة الأولى إذن إخفاء سر وجود المعلومات هو الغاية، ويصبح هدف العدو اكتشاف وجود هذه المعلومات من الأساس. بينما في الحالة الثانية لا يضيّر أن يعرف أحد بوجود هذه المعلومات، وقراءتها، وإنما هدف العدو سيكون حذف هذه المعلومات أو تغييرها لمصلحته .

- **المبدأ العام لفن الإختزال:-**

أغلب طرائق فن الأختزال تتبع المبدأ العام التالي:

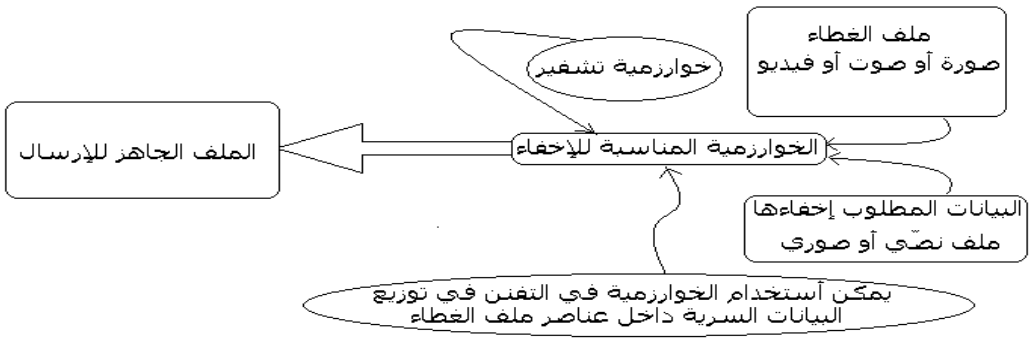
1) تحليل عناصر ملف الغطاء، وتحضيرها لأستقبال البيانات السرية.
2) تحليل عناصر الملف المطلوب تضمينه (إخفاء بياناته).
3) تطبيق الخوارزمية المناسبة للإخفاء.
4) أرسال ملف الغطاء المتضمن للبيانات السرية من قبل المرسل.
5) استلام ملف الغطاء من قبل الطرف المقصود الإرسال اليه.
6) تحليل عناصر ملف الغطاء وإستخراج عناصر الملف المضمّن وفق نفس الخوارزمية المتّبعة في الإخفاء.
7) تجميع البيانات للحصول على الملف المضمّن كاملاً.



شكل (2) مخطط عملية إخفاء ملف التضمين داخل ملف الغطاء

fowzibarazenji@yahoo.com

وقلنا في مقدمة الموضوع أن علم التشفير يمكن أن يزيد من قوة العمل، إذ سيصبح من الصعب تحديد وجود إخفاء في الملف المُرسل، ثم يصبح من المعقد فك النص المخفي المشفر، وهنالك طرائق عديد جداً من أساليب التشفير.



شكل (3) إضافة فن التشفير يزيد من قوة العمل

- **مثال بسيط على الـ Steganography:-**

قلنا في معرض الكلام عن ملف الغطاء أنه يُمكن أن يكون ملفاً نصَياً، وقد يستغرب القارئ، كيف يكون ملفاً نصياً، ويحتوي داخله بيانات نصية مخفية فيه، وأسرد المثال التالي على أبسط أنواع فن الإخفاء لنص داخل نص:-

((سوف يكمل عماد واجبات دروسه، أنا لست على رأيك الذي قلته، حرية رأيه افضل من وقوفه حائراً دون اكمالها)).

أعد قراءة النص ولعدة مرات، وحاول تفسير الرسالة، لن تجد فيها شيءٌ يدلّ على وجود نص مخفي داخلها، علماً أنني سبقت قرآءتك بالإشارة الى وجود نص مخفي داخلها، حتى أني قلت أنها من أبسط أنواع الـ Steganography.

والآن اسحب من كل كلمة الحرف الأول فقط واجمعها واقرأ ما سيظهر لك بعد جمع الأحرف الأولى من هذه الرسالة، ولاتنسى أن تقول آخرها (إن شاء الله).

قد يتبين للبعض أن هذا تشفيراً وليس إخفاءاً للبيانات !! وأقول أن التشفير يغيّر من معالم الرسالة، اما هنا فقد قمت بأخفاء أحرف الرسالة بين كلمات الرسالة الغطاء.

fowzibarazenji@yahoo.com

وهنالك أمثلة كثيرة عن طرائق فن إخفاء نص داخل نص، مثلاً كتابة الكلمات المطلوبة(الملف المضَمَّن) بصورة خاطئة إملائياً، من بين كل كلمات الرسالة المرسلة (ملف الغطاء)، أو اختيار الحرف الأول من كل كلمة في ملف الغطاء، ثم تجميع الأحرف لتكوين الملف المضَمَّن.

أو قطع الكلمات المطلوبة من نسخة صحيفة يومية، وإرسال الصحيفة بعد تقطيع الكلمات، وفي هذه الطريقة يستوجب وجود نفس النسخة عند المرسل والمستلم، ليتسنى للأخير معرفة الكلمات التي أقتُطِعت من الصحيفة لتجميعها وفهم الرسالة المقصودة.

- **تحليل (كسر) الإخفاء Steganalysis :-**

لكل طريقة أو أداة ذكية لتطوير إخفاء المعلومات في البيانات المتعددة الأوساط، عدد مساو من الطرائق والأدوات الذكية التي تتطور لتحديد وكشف أسرارها.

القصد من هذه المقدمة، أنه مع تطور العلم والأساليب المستخدمة في الإخفاء فهنالك أساليب تتطور بموازاتها في فن تحليل وكسر هذا الفن .

تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية، أو قراءتها، أو تغيرها أو حذفها ب (Steganalysis) . ولنجاح هذه العملية فلابد من أمرين، أولا: اكتشاف وجود معلومات مخفية، وثانيا: تغيرها، أو حذفها أو مجرد قراءتها. وكل وظيفة تقنيتنا هنا هو محاولة إخفاء البيانات بطريقة لا تثير الشبهات، أي لا تترك علامات أو أثرا يدل على حدوث تغير ما. فمثلا في حالة الإخفاء داخل الصور، يجب مراعاة عدة عوامل منها: عدم استخدام صور معروفة، أو نماذج من صور يمكن لأي شخص الحصول على نسخ منها (مثل صور الإنترنت) للإخفاء حيث تسهل المقارنة في حالة وجود صورتين. وكذلك مراعاة ألا يحدث تغير ظاهر في الصور كتشوهها، أو تغير ألوانها بشكل واضح. ولهذا يُنصح بعدم إخفاء بيانات كثيرة في ذات الصورة خوفا من تغيير هيئتها، بطريقة تهدم الهدف الأساسي من استخدام التقنية، لأن إثارة الشبهة يعني فشل العملية .

ومع وجود الحاسوب بمختلف سُرعه الفائقة، أصبح فن تحليل الإخفاء من الأمور اليسيرة والتي لا تستهلك وقتاً طويلاً في التنبؤ بوجود بيانات مخفية في ملف نصي أو صورة مُرسلة عبر البريد الألكتروني أو الأنترنيت بصورة عامّة، ليستمر الصراع قائماً، الى أن يرث اللهُ الأرضَ ومَن عليها.

فهدف القائم بالإخفاء هو عدم إثارة أي نقطة للشك بوجود بيانات مخفية، وستراتيجية محلل الإخفاء هو الشك في كل الرسائل المُرسَلة، وهذا لايعني صعوبة أو إستحالة هذه العملية، وكما قلنا

fowzibarazenji@yahoo.com

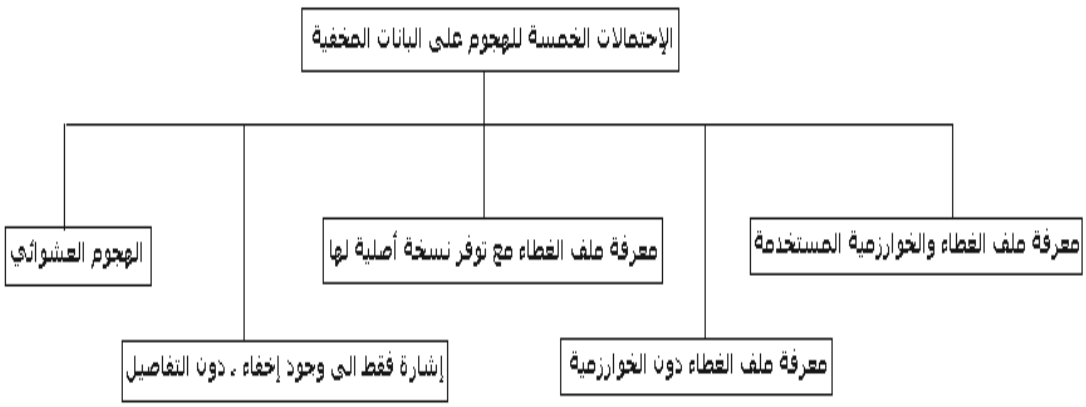
أن وجود الحواسيب المتطورة والفائقة السرعة جعلت من فحص الملفات المُرسَلة أمراً ليس بالعسير.

وهنا يكون دور القائم بعملية الإخفاء مهم جداً في إختياره ملفات الغطاء التي يصُعُب معها التمييز فيما اذا كانت قد ضُمِّنت 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 لحداد وهو يستخدم آلة كهربائية لتصفية الحديد، أو صوت سرب طيور، وغيرها من الأساليب المتوفرة وبسهولة، وضمن البيئة المحيطة لنا.

- **طرائق تحليل (كسر) الإخفاء:-**

لعملية تحليل الإخفاء خمسة إحتمالات. في مهاجمة ملف الغطاء المُرسل، وهي كما موضّحة في الشكل التالي:



شكل (4) خمسة إحتمالات للهجوم على عملية الإخفاء وكسرها

1) **الهجوم المباشر بعد معرفة ملف الغطاء و الخوارزمية المستخدمة:**

هذه الحالة تنفذ عندما تكون المعلومات المسرّبة كافية لتمييز 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:**

fowzibarazenji@yahoo.com

هذه الطريقة ليست عسيرة 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 ملف الغطاء مع وجود نسخة أصليه لديه منها:

بمقارنة بسيطة بين عناصر ملف الغطاء الأصلي مع المرسل يستطيع محلل الإخفاء أن يكتشف الخوارزمية المستخدمة، وكسر الإخفاء المستخدم، وإستخراج البيانات السرّية المـُرسَلة.

4) لا ملف الغطاء معروف ولا الخوارزمية معروفة:

ما يملكه المحلل هو فقط إشارة الى وجود إخفاء في أحد الملفات المـُرسَلة، دون تحديد الملف المقصود ولا الخوارزمية المستخدمة، هنا يكون الهجوم على كل الملفات المـُرسَلة وتخمين (تجربة) كل الخوارزميات المتوفرة لدى المحلل، هذه الطريقة قد تستهلك وقتاً، ولنها في النهاية قد تصل الى النتيجة المطلوبة.

5) الهجوم العشوائي:

حيث لايمتلك المحلل أي معلومات عن وجود بيانات مـُرسَلة، أو وجود ملف غطاء، وهذا ما يحصل كثيراً في شبكات الأنتريت، دون علمنا أو انتباهنا، حيث أن الملفات التي تُرسل عبر ألأنترنيت أو البريد الألكتروني تخضع (إن لم يكُن جميعها) فمعضمها، الى الفحص والتحليل، ولا تستغرب من ذلك.

fowzibarazenji@yahoo.com

الفصل الثاني

- **الإخفاء بإستخدام الملفات الصورية:-**

ليس القصد من الملفات الصورية إستخدامها كملف غطاء فقط، أو كلمف مضمَّن فقط، بل إستخدامها في الحالتين معاً، أي أن تكون ملف غطاء، وكذلك ملف مضمَّن، (إخفاء صورة داخل صورة Hiding image within image) .

وقبل الخوض في تفاصيل هذا الموضوع، نود إلقاء نظرة سريعة جداً على ملفات الفيديو والملفات الصوتية والملفات الصورية بشكل عام ومختصر:

❖ **هيئات ملفات الفيديو :**

- **AVI ملفات الفيديو القياسية لنظام الويندوز وهذه الملفات يمكن أن تكون كبيرة أو ضخمة الحجم.**
- **WMV فيديو خاص ببرنامج Windows Media Player ويتميز بحجمه الصغير لكن دقته منخفضة نوعاً .**
- **MPG ; MP1 ; MP2 ; MP2V ; MP4 ; MPA ; MPE ; MPEG ; MPV; MPV2**

هي اختصار لكلمات تعني مجموعة من الصور المتحركة وتكون بشكل مضغوط وتعتبر من أشهر صيغ الفيديو

- **MOV وهي صيغ فيديو خاص بنظام ماكنتوش، ويمكن تشغيلها في بيئة وندوز باستخدام برنامج Quick Time المعروف .**
- **Ramأو rm فيديو خاص بالبرنامج الشهير Real Player يتميز بحجمه الصغير**
- **3gpأو 3g2 أو 3gpp فيديو خاص بالجوال(موبايل)، ويمكن تشغيله على الكمبيوتر باستخدام برنامجي Quick Time أو Nokia Multimedia Player .**

❖ **هيئات ملفات الصوت :**

- **Wavملف الصوت المطور لشركة مايكروسوفت يتميز بأنقى صوت وأفضل جودة ولكن عيبه أن حجمه كبير جداً**

fowzibarazenji@yahoo.com

- MP3 أحد أفراد مجموعة MPEG ملفات الموسيقى ذات الشعبية الهائلة ، تتميز بالجودة العالية جداً مع الحجم المناسب .
- MPGA أحد أفراد مجموعة MPEG وهو تنسيق صوت .
- Wma نوع يتميز بدقة أقل من mp3 مع حجم أصغر .
- Ra ملفات صوت real audio خاصة ببرنامج Real Player .
- auأوaifأوaiff أو snd هذه الامتدادات تعبّر عن كل ملفات الصوت التي يمكن تشغيلها على معظم برامج الـaudio أو برامج Media player وReal Player .
- midأو midi أو amr ملفات صوتية معروفة، وتستخدم بكثرة كنغمات رنين في الموبايل .

❖ **هيئات ملفات الصور:**

العلم الحديث، وفّر للمستخدمين أنواعاً كثيرة كهيئات للملفات الصورية، وتختلف أنواع الصور بحسب إمتداداتها (Extensions)، حيث يعتمد الإمتداد على:

1- نوع الصورة من حيث حجمها ونمط تلوينها وعدد ألوانها.
2- البرنامج المستخدم لصناعتها.
3- الغرض منها.

ونظراً لكثرة العوامل المؤثرة في تكوين هيئة الملف الصوري، تنوعت الملفات الصورية الى حد كبير بحسب احتياجاتها، ويمكن تقسيم الصور بشكل عام الى قسمين:

الأول: هيئات الصور المحلية: حيث يقدم المنتجون وبإستمرار برامج جديدة لمعالجة الصور، أو تطوير التطبيقات الموجودة، ويُلاحظ أن لديهم إتجاه نحو تأسيس هيئات خاصة بتطبيقاتهم وتُعرف بالهيئات المحلية Native Formats، والهدف من إبتكار الهيئات الجديدة شمول الإجراءات والإمكانات الجديدة، والتفوق على المنافسين، غير أن الهيئات المحلية تتسبب في العديد من المشاكل الصعبة الخاصة لمن يرغب بمعالجة الصور بإستخدام أكثر من تطبيق، وفي الغالب تكون الهيئات المحلية مقروئة فقط من قبل برنامجها، ويستعصي تحميلها من برنامج لآخر.

الثاني: هيئات الصور العامّة: والتي يمكن إستخدامها في مختلف التطبيقات، وأنواعها كثيرة ومتداولة من قبل الجميع في كل التطبيقات تقريباً، فمنها على سبيل الذكر الملفات على

fowzibarazenji@yahoo.com

هيئةBmp, Jpg, jpeg, psd, Gif, Png, Tiff وغيرها، ومن أشهر أنواع هيئات الصور:

- JPEG: إختصاراً للعبارة (Joint Photographic Expert Group) وهي الأكثر شعبية وإنتشاراً لاسيّما لأغراض الصور على الإنترنيت.

إنّ تصميم JPEG هو للتعامل مع الصور وليس الخطوط أو الرسوم الخطية، و تتمتع الصور على هذه الهيئة بالصفات التالية:

- إستعمالها آلية ضغط متغيرة، حيث تستطيع التحكم بدرجة الضغط عند الخزن للحصول على حجم ملف مناسب جداً، وكلما كانت درجة الضغط أكبر كان ذلك على حساب جودة الصورة.
- هذه الهيئة تدعم نظام عمق لوني يصل لغاية 24 bits/Pixel أي عدد الألوان يصل الى 16 مليون لون.
- تعمل وفق آلية ضغط ثنائي المراحل، وهذا يفسر الوقت المستغرق من أجل تحميل و عرض الصورة وسبب ما نشاهده عند عرض الصور في الإنترينت.
- تحمل الصور من هذا النوع الإمتداد ".jpg" و ".jpeg"

- TIFF: إختصاراً للعبارة (Tag Image File Format) صممتها شركة Aldus في الأصل لحفظ الصورة الآتية من الماسح الضوئي Scanner، ثم إنتشرت بشكل واسع وشاعت كهيئة صور دون إرتباطها بماسح ضوئي معين أو طابعة أو برنامج معالجة خاص.
- GIF: إختصاراً للعبارة (Graphics Interchange Format) وهي تُستعمل بشكل واسع على الويب، وعلى الأغلب لفنون الخط وليس للصور الفوتوغرافية، وهذه الهيئة تجمع لغاية 256 لون.
- PNG: إختصاراً للعبارة (Portable Network Graphics) وهي تتفوق على الهيئة السابقة في إحتوائها 256 مستوى شفافية بينما تمتلك الهيئة GIF مستوىً واحداً فقط، كذلك تتحكم بأكبر درجة سطوع للصورة ودعم لنظام 48 Bit/Pixel بينما الGIF يدعم 8 Bit/Pixel فقط .
- EpS: إختصاراً للعبارة (Encapsulated Post Script) وهي تتألف من جزئين:

1) عبارة عن وصف نصّي يوضح للطابعة كيف ينبغي أن يكون شكل الصورةالمطبوعة.

fowzibarazenji@yahoo.com

2) صورة إضافية على هيئة PICT تستخدم للعرض على الشاشة.

- **BMP:** صور الخريطة النقطية، حيث تتكون من مجموعة من نقاط ضوئية تكون بمجموعها عناصر الصورة، وتتأثر جودة ونوعية الصورة عند تغيّر الحجم، وهذه الهيئة تندرج ضمن نوع الصور المسمى Raster Image.

بالتأكيد هنالك أنواع كثيرة أخرى، ولكون بحر عالم الصور عميق جداً، ولأننا نريد أن نلقي نظرة سريعة ومختصرة وحتى لانغرق فيه، سأكتفي بالجدول التالي للمقارنة بين حجوم هذه الصور، والفرق بين هذه الهيئات، لصورة واحدة وبقياس (408 x 393) على سبيل المثال:

نوع الصورة	Bmp 24 bits	Bmp 16 bits	Bmp 1bits Monochrome	Bmp 256 colors	IFF image	GIF image	JPEG image	PNG image
الحجم(KB)	470	79.8	20.7	158	160	111	51.1	372

جدول (1) إختلاف حجم الصورة بإختلاف نوعها

❖ أمّا تقسيم الصور حسب تركيب ألوانها فيمكن تقسيمها الى أربعة أقسام:

1- الصور الثنائية:

وهي أبسط أنواع الصور، وتأخذ قيمتين فقط للألوان، وهما 0 ويعني اللون الأسود، 1 ويعني اللون الأبيض.

ويمكن التعبير عن الصور الثنائية بقيمة بت واحد للعنصر الواحد 1Bit/Pixel، وهذا النوع من الصور له تطبيقات كثيرة في رؤية الحاسوب، كأن تكون المعلومات المطلوبة للشكل العام، أو الحدود الخارجية للجسم وكذلك لتحديد مكان الجسم وإدراكه من قبل الإنسان الآلي مثلاً، أو التحقق من تشوهات الأجسام المصنوعة، وغيرها من التطبيقات الملائمة لها.

ويمكن الحصول على الصور الثنائية من الصور الملونة أو ذات التدرج الرمادي بالإعتماد على عملية التعتيب Thresholding Operation، وهي تحديد قيمة معينة لشرط العتبة، تتحول فيها الألوان الأعلى منها قيمة الى اللون الأبيض 1، والألوان الأدنى الى اللون الأسود .

يمكن تجربة ذلك لمستخدمي لغة الفيجوال بيسك 6، بإستخدام الكود التالي:

```
Dim a As Long
```

```
Private Sub Command1_Click()
   For i = 1 To P1.ScaleWidth
      For j = 1 To P1.ScaleHeight
         a = Picture1.Point(i, j)
         If Picture1.Point(i, j) > 8000000 Then     تم اختيار الرقم 8000000 كشرط العتبة،
            a = vbWhite          يتم تحويل اللون الى أبيض إذا كان أكبر من شرط العتبة،
            Else
            a = vbBlack                                  أو أسود إذا كان أقل،
         End If
         If a < 0 Then a = 0
         Picture2.PSet (i, j), a  إعادة رسم نقاط الصورة الثانية بالقيم المستخرجة من التحويل،
      Next j
   Next i
End Sub
```

هذا الكود يتم كتابته في زر الأمر Command1 بعد تحميل الصورة الملونة في Picture1 ثم نقلها الى Picture2 بعد إجراء التغير على قيم الألوان لعناصرها.

شكل (5) تحويل الصورة الملونة الى صورة ثنائية

fowzibarazenji@yahoo.com

2- الصور ذات التدرج الرمادي:

صور التدرج الرمادي يُعبّر عنها بالصور أحادية اللونMonochrome ، وهي تحتوي على معلومات الإضاءة Brightness فقط، دون معلومات الألوان، وتستخدم عدد من الBit/Pixel بحسب حجمها، لتحديد مستوى الإضاءة المختلفة فيها،ومثالياً تحتوي كل صورة على Bit/Pixel 8، أي بايت واحد فقط لتمثيل كل عنصر فيها، أي أنها تسمح ل256 مستوى من مستويات الإضاءة (من 0 (أسود) الى 255 (أبيض)) .

هنالك خوارزميات كثيرة لتحويل الصور الملونة الى التدرج الرمادي، ومنها ما سنطبقها الآن وهي طريقة المعدل اللوني، فكل عنصر في الصورية الملونة سيتم قرآءة القيمة اللونية له، ثم تمييزها الى الأحزمة الثلاث RGB، ثم حساب معدل القيم الثلاث لتكوين قيمة واحدة تُعطى لعنصر الصورة ذات التدرج الرمادي، لاحظ الكود التالي المكتوب في زر الأمر Command1 بعد تحميل الصورة الملونة في Picture1 ثم نقلها الى Picture2 بعد إجراء التغيير على قيم الألوان لعناصرها وحساب المعدل ثم رسم نقاط الصورة الثانية بقيمة المعدل فقط .

```
Dim a As Long
Dim i As Integer, j As Integer
Private Sub Command1_Click()
Dim red As Integer, green As Integer, blue As Integer, Av As Integer
  For i = 1 To Picture1.ScaleWidth
    For j = 1 To Picture1.ScaleHeight
      a = Picture1.Point(i, j )          قراءة القيمة اللونية لعنصر الصورة،
      red = a Mod 256                  إستخراج القيمة اللونية للون الأحمر،
      green = a / 256 Mod 256                          والأخضر،
      blue = a / 256 / 256                             والأزرق،
      Av = (red + green + blue) / 3،      حساب المعدل لعناصر ثلاثة
      Picture2.PSet (i, j), RGB(Av, Av, Av)
    Next j
  Next i
End Sub
```

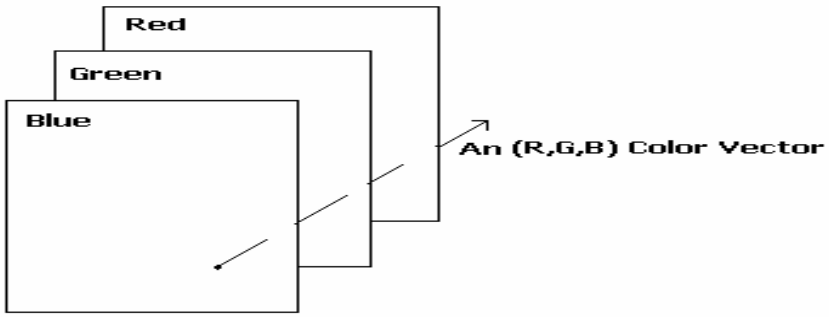

fowzibarazenji@yahoo.com

شكل (6) تحويل الصورة الملونة الى صورة ذات تدرج رمادي

3- الصور الملونة:

وتتكون من ثلاث أحزمة (3 Bands)، كل حزمة تُمثَّل ببايت واحد، لذا يمكن القول أن كل عنصر في الصورة الملونة يتم تمثيله ب(3 Bytes) وهذا يعطي سبب كبر حجم الصور الملونة بالمقارنة مع سابقاتها.

وكل حزمة تعني لون من الألوان الرئيسة الثلاث (أحمر، أخضر، أزرق)، والمعروفة بإسم (RGB)، ويمكن أن نقول أن كل صف Row أو عمود Column يُمثَّل بمتجه العنصر اللوني Color Pixel Vector (RGB).



شكل (7) متجه العنصر اللوني للألوان الثلاث

fowzibarazenji@yahoo.com

فيجوال بيسك 6 توفر الكود المناسب لقراءة عنصر الصورة بعد تحميلها في الأداة Picture Box وكالتالي: Picture.Point (i, j) حيث يمثل الرمز i الصف الذي فيه العنصر، بينما يمثل الرمز j العمود الذي يحتوي العنصر المطلوب قراءة قيمته اللونية .

أمـّا رسم القيمة اللونية للعنصر الى صورة ما، فيتم بالكود: Picture.Pset(i,j).

4- صور متعددة الطيف:

وتحتوي على معلومات خارجة عن مدى الإفتراضات الطبيعية لدى الإنسان، حيث تتضمن بيانات الأشعة تحت الحمراءInfrared وفوق البنفسجيةUltraviolet والأشعة السينية X-Ray والصوتية والرادارية وغيرها، ومصادر هذه الصور هي الأقمار الصناعية، أنظمة متحسسات تحت الماء، مختلف أنواع الرادارات، أنظمة التصوير الحراري، وأنظمة التشخيص الصورية الطبية .

هذه الصور تحتوي معلوماتها على أكثر من ثلاث حزم 3Bands لتمثيل الصورة، فقد تصل الى سبعة حزم، ثلاثة منها للطيف المرئي (من 1 الى 3)والباقي في منطقة الطيف تحت الحمراء، علماً أن المتحسسات الحديثة للأقمار الصناعية تجمع المعلومات في أكثر من ثلاثين حزمة.

هذا الكم الهائل من البيانات يحتاج الى نقل وخزن فائق، بالإضافة الى زيادة في قدرة المعالجة، وغالباً ما تُضغط هذه البيانات لتصبح أكثر وضوحاً .

وقبل أن نختتم هذا الفصل نود التنويه الى أننا سنستخدم ملف الغطاء صورة من نوع BMP ، بينما سنستخدم أخفاء بيانات نوع Text كرسالة مطلوب إخفائها .

fowzibarazenji@yahoo.com

الفصل الثالث

- **شرح خوارزمية البت الأقل أهمية Least significant bit:-**

يتم في الحواسيب تخزين المعلومات و معالجتها في شكل بتات وبذلك يكون نظريا البت أصغر وحدة حاملة أو ناقلة لمعلومة أو لمعنى ما معين. عمليا، في الحواسيب و المعالجات الرقمية، البت هو عبارة عن نبضة كهربائية تكون إما موجبة أو سالبة (في الحقيقة تكون نبضة أقوى من الأخرى مثلا نبضة 5 فولت و نبضة 1 فولت) ويرمز لها بأحد الرقمين الثنائيين إما 1 أو 0.

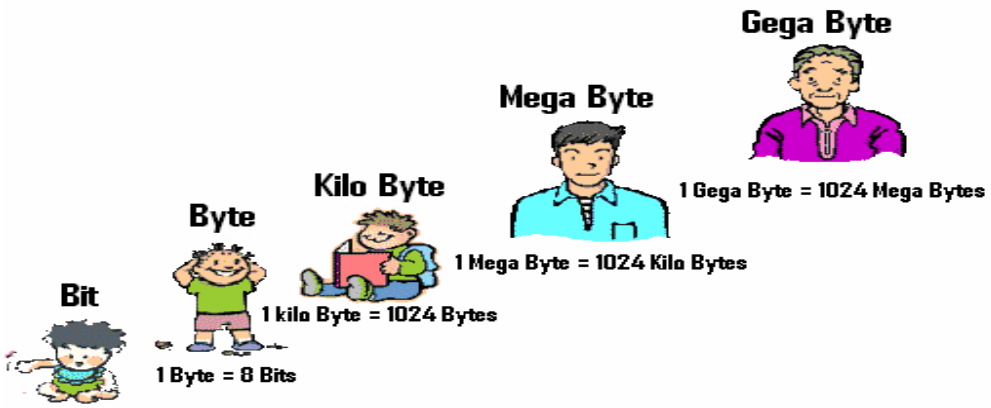
و تسمى كل ثمانية بتات (مجتمعة) بايت Byte. البت عبارة عن خانة واحدة من رقم ثنائي وله أحتمالين فقط اما ان يكون البت 0 أو يكون 1.

البايت من الإنجليزية Byte هو وحدة شائعة الاستخدام لقياس سعة التخزين في الحاسوب، بغض النظر عن نوع المعلومات المخزنة أو وسيلة التخزين.

يتكون البايت عادة من 8 بت، ولذلك فأن البايت يحتوي على 2مرفوع الى قوة 8 = 256 احتمال مختلف يخزن البايت القيم من 00000000 إلى 11111111، لتسهيل كتابة البايت وقراءته بشرياً يحول الرقم الثنائي إلى نظام ست عشري أو نظام عشري فالحرف A رمزه حسب جدول الآسكي 10000001 ويقابله الرقم 41 بالنظام ست عشري والرقم 65 بالنظام العشري.

تذكر أن البايت هو الوحدة المستخدمة في قياس كمية المعلومات على الحاسب (سعة الأقراص – حجوم الملفات والمجلدات ... إلخ)، ولقد علمنا أن البايت = 8 بت، أما مضاعفاته فهي:

كيلو بايت = 1024 بايت، ميغا بايت = 1024 كيلو بايت، غيغا بايت = 1024 ميغا بايت.



شكل (8) البت والبايت ومضاعفاته

fowzibarazenji@yahoo.com

أصبح واضحاً لجميع محبي علم الحاسوب ماهو البايت Byte وماهو البت Bit، لذا لن نصرف معظم الوقت في الحديث عنهما، وكل ما يهمنا هنا هو تقسيم البايت الى 8 بت، ومعرفة البت الأقل أهمية من بينها، علماً أن البت لا يقبل سوى 0 أو 1.

وتوزيع قيم البتات في البايت الواحد، يكون كالتالي:

128	64	32	16	8	4	2	1

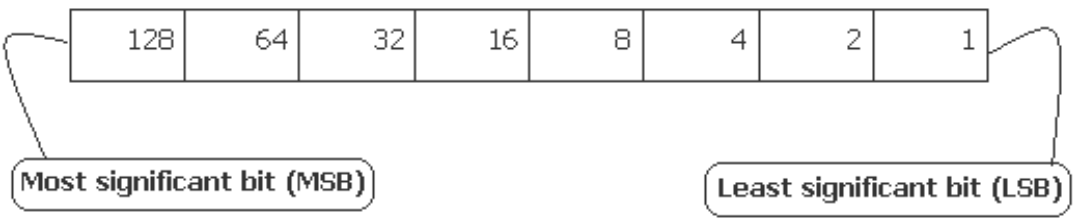
وهذا ما يوضح أن البايت الواحد يمثل 256 قيمة (من 0 في حال جميع البتات تحمل قيمة 0)الى (255 عندما تكون كل قيم البتات = 1)، فلو أردنا تمثيل الرقم 65 بطريقة النظام الثنائي، بالتأكيد سيكون:

0	1	0	0	0	0	0	1

وعندما كنا في أحلى أيامنا الدراسية، في مرحلة الطفولة تعلمنا أن الرقم على اليمين يمثل أقل الأرقام تأثيراً، وكما يُسمى (الأحاد).

جرب معي أن تغير الرقم الذي على اليمين من 1 الى 0، سيصبح الرقم 64 بدلاً من 65، وجرب معي أن تغير البت على اليسار من 0 الى 1، سيصبح الرقم 193.

هذا معناه أن البت الأخير هو البت الأقل أهمية (البت الذي على اليمين طبعاً)، والذي لو جعلناه صفراً لأصبح الرقم 64.



شكل (9) البت الأقل أهمية والبت الأكثر أهمية

أظنك الآن فمهت القصد من كون البت أقل أهمية، وستجيبني وبكل تأكيد لو أننا غيرنا هذه القيمة فلن يكون التأثير واضحاً الى الحد الذي يُمكن أن تنكشف فيه الأضافة أو التغيير، وأضيف أن البايت الواحد لايمثل القيمة اللونية للصورة الملونة لوحده، بل يشترك معه بايتان آخران، وهذا معناه أن

fowzibarazenji@yahoo.com

التاثير سيكون أقل بكثير مما لو كان لوحده، وهذا ما يجعلنا نميل الى الصور الملونة في عملية الإخفاء بدل الصور ذات التدرج الرمادي.

ورياضياً سأعطيك مثالاً أخيراً على توزيع بايت واحد على 9 بايتات تمثل 3 عناصر صورة ما، حيث قلنا سابقاً أن العنصر الواحد يتم تمثيله ب 3 Bytes، لاحظ المثال التالي:

البايت الذي يمثل الرمز B، الذي يُمثّله الرقم 66 في نظام (ASCII Code): وهذا معناه تمثيل الرقم 66 بالصورة التالية: 01000010 ، أي أننا نمتلك ثمان بتات سنقوم بتوزيع كل بت على بايت واحد من بايتات الصورة الثمانية الأولى، ولنفترض أن لدينا قيم البايتات التالية كقيم لونية لعناصر الصورة: 145و161، 210,80,26,77,10، لاحظ تمثيل هذه البايتات :

145	161	10	77	26	80	210
10010001	10100001	00001010	01001101	00011010	01010000	11010010

لتحضير البت الأقل أهمية للأضافة يجب تصفيره:-

10010001	10100001	00001010	01001101	00011010	01010000	11010010
- 1	1	0	1	0	0	0

قيم البايتات بعد تصفير (تحضير) البت الأقل أهمية:-

144	160	10	76	26	80	210
10010000	10100000	00001010	01001100	00011010	01010000	11010010

لاحظ التأثير القليل الذي أحدثناه لحد الآن، ثم نضيف البتات الثمانية التي تمثل الرقم 66:-

145	160	10	77	26	80	210
10010001	10100001	00001010	01001101	00011010	01010000	11010010
+ 0	1	0	0	0	1	0

145	161	10	77	26	81	210
10010001	10100010	00001010	01001101	00011010	01010001	11010010

وبعد عملية الإحلال أصبحت القيم: 145و161، 210,81,26,77,10، وأنا متأكد أنك تلاحظ

fowzibarazenji@yahoo.com

الفرق البسيط جداً وغير الواضح في عملية إخفاء حرف داخل 3 عناصر صورة .

وإذا ما سألت هل تغيير بت واحد من كل بايت يكفي لإخفاء بيانات كاملة لنص أو لصورة؟ فأجيبك: بأنني سبق وأن قلت أن الصور من نوع BMP هي المستخدمة كملف غطاء لكثرة البيانات التي تجمعها، وقلت أن الصور المضمّنة هي من نوع JPG أو مثيلاتها، إن لم تكن أقل من ناحية الحجم(راجع الجدول (1) في الفصل السابق)، كانت الصورة بقياس 408 x 393 فبلغ حجم الصورة BMP (9) أضعاف حجم نفس القياس من نوع JPEG، بينما صفحة الشكر والتقدير في هذا الكتاب لم يصل حجمها الى (25 KB)، وبالتالي فبإمكان صورة صغيرة من نوع BMP أن تخفي في بياناتها ملفاً نصّياً لأكثر من صفحتين.

إن تغيير البت الأقل أهمية في رأيي هي من أقوى الخوارزميات الموجود في فن الإخفاء، والتي تترك أثراً بسيطاً جداً في ملف الغطاء، اذا ما أحسنت برمجتها، ويتعسّر على العين البسيطة إستكشاف التأثير، وبالتالي يستعصي فك رموزها حاسوبياً إذا ما أخذ بنظر الإعتبار التفنن في الإخفاء، وإضافة اللمسات التشفيرية، وإستخدام صور غير متوفرة النسخ .

والآن سننتقل الى المرحلة الأكثر صعوبة في هذا الكتاب كله: عملية تحليل البيانات المضمّنة وتحليل بيانات ملف الغطاء، وإخفاء البيانات الأولى داخل الثانية، وبنفس هذه الخوارزمية.

fowzibarazenji@yahoo.com

الفصل الرابع

- **التطبيق العملي لخوارزمية البت الأقل أهمية:-**

وصلنا الى المرحلة الأخيرة من موضوعنا، صناعة البرنامج بلغة فيجوال بيسك 6، لتطبيق خوارزمية البت الأقل أهمية، وسيتألف هذا الفصل من التطبيق العملي لموضوع الكتاب: إخفاء البيانات داخل الصورة:-

إن كنت من مبرمجي فيجوال بيسك 6، فلن تتعبني في شرح هذا البرنامج، أمّا إن كنت من الضيوف عليها أو المبتدئين فيها، فأرجو أن لايزعجك شرحي المختصر، أملاً في أن تكون الأيام القادمة كفيلة بتطورك، ومن ثمّ فهمك له.

سنحضر الأدوات التالية في واجهة البرنامج:

1. Text Box : لإدخال النص، مع تغيير بعض من خصائصه مثل:
   1) Name : لغرض عدم اختلاط الكود لدى القارئ الكريم، نبدل إسم الأداة الى txtmsg.
   2) Height: أجعله بالإرتفاع المناسب لتقبّل أكبر قدر من البيانات.
   3) Multi Line: إجعله True.
   4) Scroll Bars: أجعله 2- Vertical.
   5) طبعاً إضافة الى مسح محتوى الأداة.
2. خمسة أزرار أمر Command Buttons وبالتسميات التالية:
   1) cmdLoad أما الـ Caption فاجعله Load .
   2) cmdSave أما الـ Caption فاجعله Save ، والخاصية Enabled إجعلها False.
   3) cmdstego أما الـCaption فاجعلهِ Stego ، والخاصية Enabled إجعلها False.
   4) cmdDeStego أما الـCaption فاجعله DeStego ، والخاصية Enabled إجعلها False.
   5) cmdLanguage أما الـCaption فاجعله عربي.

fowzibarazenji@yahoo.com

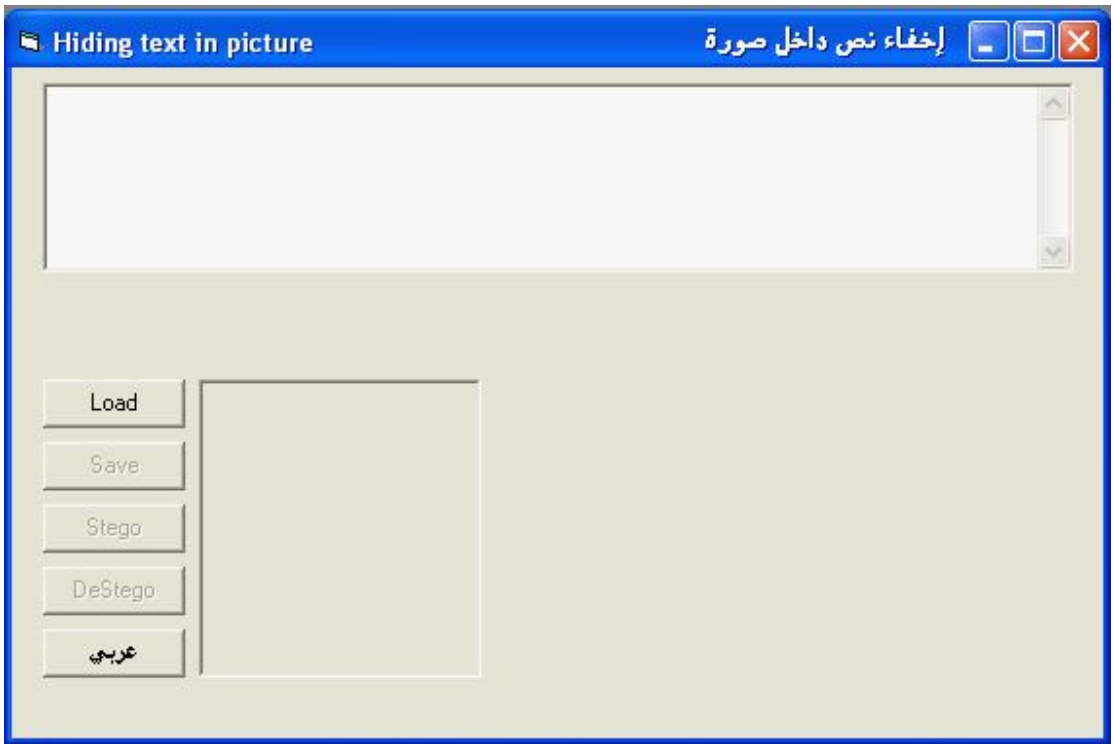
3. الأداة **Microsoft Common Dialog Control 6.0 (SP3):**

وللإختصار نقوم بتغيير إسمها الى CmnDlg، للإختصار فقط .

4. **أداة عرض الصورة Picture Box:**

مع تغيير خاصية ال (Auto Size) الى True، ولا تنسى ومرة أخرى أكرر لا تنسى أن تجعل الخاصية Scale Mode = 3- Pixel.

لذا ستكون واجهة برنامجنا بالشكل اتالي:



شكل (10) واجهة البرنامج بداية التنفيذ

ثم نبدأ بكتابة الكود، ولكل أداة كودها الخاص بالتأكيد، وسأبدأ بسرد الكود كما هو ترتيب أزرار الأوامر من الأعلى الى الأسفل:

1) **كود تحميل الصورة. وإختبارها من حيث (تم إستخدامها سابقاً أو أنها صورة جديد)، هذه الفكرة ليست مقصد الموضوع الآن:**

```
Private Sub cmdLoad_Click()
Dim flag As Boolean
```


fowzibarazenji@yahoo.com

```
CmnDlg.ShowOpen
If CmnDlg.Flags = 0 Then Exit Sub
Picture1.Picture = LoadPicture(CmnDlg.FileName)
w = Picture1.ScaleWidth
h = Picture1.ScaleHeight
flag = True
DoEvents
For i = 1 To 3
    cColor = GetPixel(Picture1.hdc, i, 1)
    Call GetRGB(cColor, r, g, b)        هذه الدالة ستجد كودها أسفل الجميع ,
      C1 = (r Mod 10) * 100
      C2 = (g Mod 10) * 10
      C3 = (b Mod 10)
      If (C1 + C2 + C3) <> Asc(Mid(k, i, 1)) Then
       flag = False
       Exit For
      End If
Next
If flag Then
  cmdStego.Enabled = False
  cmdDeStego.Enabled = True
  txtMsg.Locked = True
Else
  cmdStego.Enabled = True
  cmdDeStego.Enabled = False
```


fowzibarazenji@yahoo.com

```
    txtMsg.Locked = False
  End If
  cmdSave.Enabled = False
  txtMsg"" =
End Sub
```

2) كود خزن الصورة بعد إجراء عملية الإخفاء فيها:

```
Private Sub cmdSave_Click()
  CmnDlg.ShowSave
  SavePicture Picture1.Picture, CmnDlg.FileName
  cmdSave.Enabled = False
End Sub
```

3) كود عملية الإخفاء:

```
Private Sub cmdStego_Click()
  If txtMsg = "" Then Exit Sub
  Form1.MousePointer = 11
  length = Len(txtMsg)
'  If h * w < length + 10 Then Exit Sub
  For i = 1 To 3
        cColor = GetPixel(Picture1.hdc, i, 1)
        Call GetRGB(cColor, r, g, b)
        C1 = Asc(Mid(k, i, 1)) \ 100
        C2 = (Asc(Mid(k, i, 1)) - C1 * 100) \ 10
        C3 = (Asc(Mid(k, i, 1)) - C1 * 100) Mod 10
        r = r - r Mod 10 + C1
        g = g - g Mod 10 + C2
```


fowzibarazenji@yahoo.com

```
    b = b - b Mod 10 + C3
    SetPixel Picture1.hdc, i, 1, RGB(r, g, b)
Next
'Length
cColor = GetPixel(Picture1.hdc, 9, 1)
Call GetRGB(cColor, r, g, b)
C1 = length \ 100
C2 = (length - C1 * 100) \ 10
C3 = (length - C1 * 100) Mod 10
If r - r Mod 10 + C1 > 255 Then r = r - 10
r = r - r Mod 10 + C1
If g - g Mod 10 + C2 > 255 Then g = g - 10
g = g - g Mod 10 + C2
If b - b Mod 10 + C3 > 255 Then b = b - 10
b = b - b Mod 10 + C3
SetPixel Picture1.hdc, 9, 1, RGB(r, g, b)
x = 9: y = 1
For i = 11 To length + 10
    x = x + 1
    If x > w Then
      x = 1: y = y + 1
    End If
    cColor = GetPixel(Picture1.hdc, x, y)
    Call GetRGB(cColor, r, g, b)
    C1 = Asc(Mid(txtMsg, i - 10, 1)) \ 100
```

```
        C2 = (Asc(Mid(txtMsg, i - 10, 1)) - C1 * 100) \ 10
        C3 = (Asc(Mid(txtMsg, i - 10, 1)) - C1 * 100) Mod 10
        If r - r Mod 10 + C1 > 255 Then r = r - 10
        r = r - r Mod 10 + C1
        If g - g Mod 10 + C2 > 255 Then g = g - 10
        g = g - g Mod 10 + C2
        If b - b Mod 10 + C3 > 255 Then b = b - 10
        b = b - b Mod 10 + C3
        SetPixel Picture1.hdc, x, y, RGB(r, g, b)
        DoEvents
    Next
    Set Picture1.Picture = hDCToPicture(Picture1.hdc, 0, 0, w, h)
    cmdStego.Enabled = False
    cmdDeStego.Enabled = True
    cmdSave.Enabled = True
    Form1.MousePointer = 0
End Sub
```

4) كود كسر الإخفاء وإستخراج النص المخفي من الصورة:

```
Private Sub cmdDeStego_Click()
    txtMsg = ""
    cColor = GetPixel(Picture1.hdc, 9, 1)
    Call GetRGB(cColor, r, g, b)
    C1 = (r Mod 10) * 100
    C2 = (g Mod 10) * 10
    C3 = (b Mod 10)
```


fowzibarazenji@yahoo.com

```
 length = C1 + C2 + C3
 x = 9: y = 1
 For i = 1 To length
  x = x + 1
  If x > w Then
   x = 1: y = y + 1
  End If
  cColor = GetPixel(Picture1.hdc, x, y)
  Call GetRGB(cColor, r, g, b)
  C1 = (r Mod 10) * 100
  C2 = (g Mod 10) * 10
  C3 = (b Mod 10)
  txtMsg = txtMsg + Chr(C1 + C2 + C3)
 Next
 cmdDeStego.Enabled = False
End Sub
```

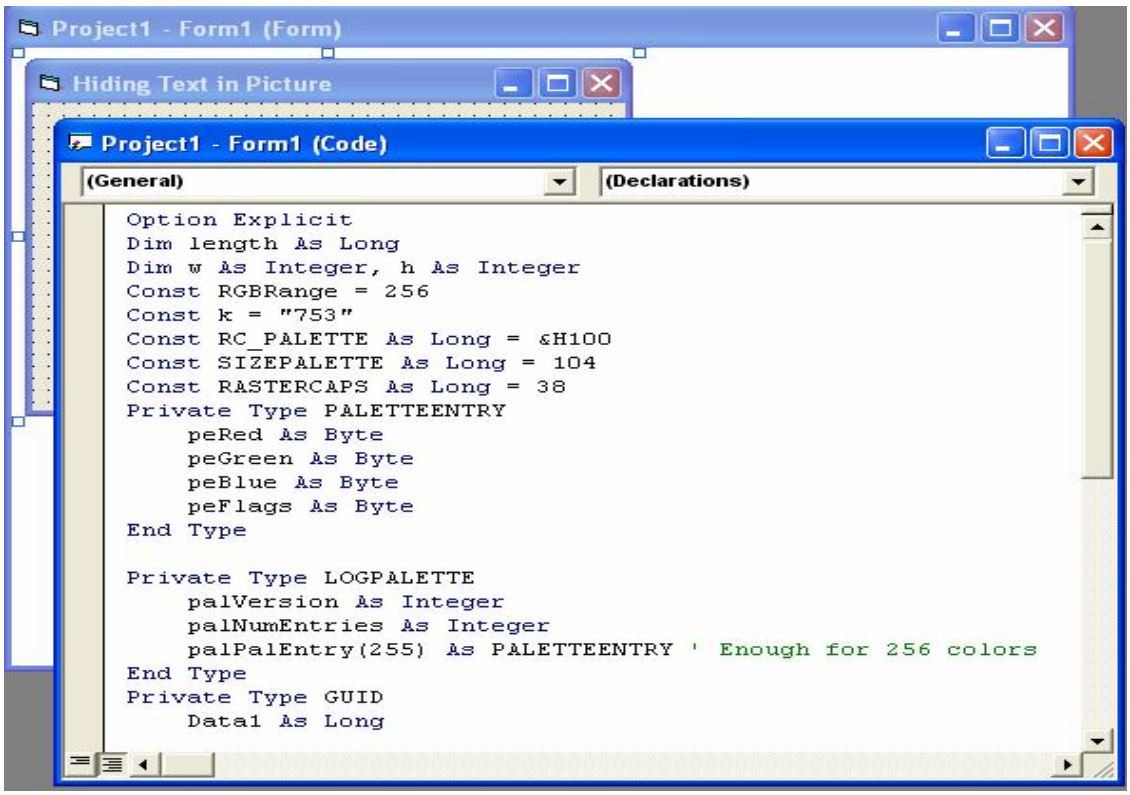
5) كود تحويل نظام الـ TextBox والإستعداد للكتابة بالعربية أو الكوردية من اليمين الى اليسار:

```
Private Sub cmdLanguage_Click()
 If cmdLanguage.Caption = "English" Then
  cmdLanguage.Caption = "ÚÑÈí"
  txtMsg.RightToLeft = False
  txtMsg.Alignment = 0
 Else
  cmdLanguage.Caption = "English"
  txtMsg.RightToLeft = True
```


fowzibarazenji@yahoo.com

```
    txtMsg.Alignment = 1
  End If
End Sub
```

بقيت ملاحظة واحدة، هنالك بعض التعريفات الواجب كتابتها، قبل الشروع بكتابة الكود المطلوب، حيث تكتبها في الحقل الخاص بالتعريفات العامة General، هذه التعريفات تخص المتغيرات المستخدمة، تعريفات لخزن الصورة على هيئة BMP، والدوال المستخدمة في عملية تحليل وتفكيك عناصر الصورة، وكذلك تحليل وتفكيك القيمة اللونية المتكونة من 3 Bytes وكما أسلفنا، الى المركبات الرئيسة الثلاث، ووفق نظام (RGB):-



شكل (11) كتابة التعريفات في حقل General

```
Option Explicit
Dim length As Long
Dim w As Integer, h As Integer
Const RGBRange = 256
```


fowzibarazenji@yahoo.com

```
Const k = "753"
Const RC_PALETTE As Long = &H100
Const SIZEPALETTE As Long = 104
Const RASTERCAPS As Long = 38
Private Type PALETTEENTRY
   peRed As Byte
   peGreen As Byte
   peBlue As Byte
   peFlags As Byte
End Type
Private Type LOGPALETTE
   palVersion As Integer
   palNumEntries As Integer
   palPalEntry(255) As PALETTEENTRY ' Enough for 256 colors
End Type
Private Type GUID
   Data1 As Long
   Data2 As Integer
   Data3 As Integer
   Data4(7) As Byte
End Type
Private Type PicBmp
   Size As Long
   Type As Long
   hBmp As Long
```

```
    hPal As Long
    Reserved As Long
End Type
Private Declare Function OleCreatePictureIndirect Lib "olepro32.dll" (PiCmnDlgesc As PicBmp, RefIID As GUID, ByVal fPictureOwnsHandle As Long, IPic As IPicture) As Long
Private Declare Function CreateCompatibleDC Lib "gdi32" (ByVal hdc As Long) As Long
Private Declare Function CreateCompatibleBitmap Lib "gdi32" (ByVal hdc As Long, ByVal nWidth As Long, ByVal nHeight As Long) As Long
Private Declare Function SelectObject Lib "gdi32" (ByVal hdc As Long, ByVal hObject As Long) As Long
Private Declare Function GetDeviceCaps Lib "gdi32" (ByVal hdc As Long, ByVal iCapabilitiy As Long) As Long
Private Declare Function GetSystemPaletteEntries Lib "gdi32" (ByVal hdc As Long, ByVal wStartIndex As Long, ByVal wNumEntries As Long, lpPaletteEntries As PALETTEENTRY) As Long
Private Declare Function CreatePalette Lib "gdi32" (lpLogPalette As LOGPALETTE) As Long
Private Declare Function SelectPalette Lib "gdi32" (ByVal hdc As Long, ByVal hPalette As Long, ByVal bForceBackground As Long) As Long
Private Declare Function RealizePalette Lib "gdi32" (ByVal hdc As Long) As Long
Private Declare Function BitBlt Lib "gdi32" (ByVal hDestDC As Long, ByVal x As Long, ByVal y As Long, ByVal nWidth As Long, ByVal nHeight As Long, ByVal hSrCmnDlgC As Long, ByVal xSrc As Long, ByVal ySrc As Long, ByVal dwRop As Long) As Long
Private Declare Function DeleteDC Lib "gdi32" (ByVal hdc As Long) As Long
Private Declare Function GetDC Lib "user32" (ByVal hwnd As Long) As Long
Private Declare Function SetPixel Lib "gdi32" ( _
        ByVal hdc As Long, _
        ByVal x As Long, _
```

```
            ByVal y As Long, _
            ByVal crColor As Long) As Long
Private Declare Function GetPixel Lib "gdi32" ( _
            ByVal hdc As Long, _
            ByVal x As Long, _
            ByVal y As Long) As Long
Dim nWidth As Integer, nHeight As Integer
Dim x As Integer, y As Integer, i As Integer
Dim r As Byte, g As Byte, b As Byte
Dim C1 As Integer, C2 As Integer, C3 As Integer
Dim cColor As Long
```

وهذه دالة لإيجاد المركبات اللونية لعنصر الصورة

```
Public Sub GetRGB(Clr As Long, r As Byte, g As Byte, b As Byte)
  If Clr < 0 Then Exit Sub
     r = Clr Mod RGBRange
     g = (Clr \ RGBRange) Mod RGBRange
     b = (Clr \ RGBRange) \ RGBRange
End Sub
```


fowzibarazenji@yahoo.com

شكل (11) لاحظ الأزرار الفعّالة والأخرى غير الفعّالة، وكيف تحول زر الأمر من عربي الى English

بمجرد الضغط على زر الأمر Stego يصبح زر الأمر Save فعّالاً، وأتمنى تجربة البرنامج لديك عزيز القارئ الكريم، للتأكد من صحة النتائج.

fowzibarazenji@yahoo.com

خاتمة

مجال أمن المعلومات ليس مجالا هامشياً ولا سهلاً، وله استخدامات قصوى في تناقل البيانات على خطوط الإنترنيت بشكل كبير وجدير بالإهتمام وخصوصاً في عصرنا هذا، عصر الحروب بكل أنواعها، عصر الجاسوسية والتجسس ، عصر الحرب الباردة و الساخنة، ونظرا لأن قرننا هذا يبدو أنه قرن الحروب التكنولوجية، أو قل حرب المعلومات، فستزداد الحاجة لمثل هذه التقنيات والتطبيقات في عصرنا هذا، لذا لابد من مواكبة التطور العلمي في شتى مجالات العلم، وشتى المجالات التي يمكن لنا من خلالها أن نكون ولو بشيء بسيط افضل من عدونا، أنا أعلم أنهم سبقونا بالعلم درباً طويلاً، ولكن كما كان أجدادنا أسيادهم، فقد يأتي اليوم الذي يكون فيه أحفادنا أسياداً.

يعتمد فن إختزال البيانات وإخفاءها على تحليل النص الى حروف وتحويلها الى نظام البايت، ثم تحليل كل عناصر الصورة المراد الإخفاء بداخلها، الى نظام البايتات الثلاث، ثم تجربة خوارزمية البت الأقل أهمية في إخفاء كل بت من بايتات الحروف (النص) داخل بايت واحد من البايتات الثلاث (وهكذا لكل عناصر الصورة).

تختلف فكرة الإختزال عن فكرة التشفير بعدم تشويه النص المراد إرساله، ومحاولة عدم تشويه الصورة المطلوب الإخفاء فيها، بأعلى قدؤ ممكن من التقنية، وذلك لعدم إثارة أي فرصة شك بوجود بيانات مخفية داخلها.

أتمنى ألاّ أكون قد أثقلت عليكم بشرحي

ولا أرجو الاّ رحمة ربي

لأمي وأبي اللهم إرحمهما كما ربياني صغيراً

ولا تنسوني في دعائكم

فوزي برزنجي

fowzibarazenji@yahoo.com