وزارة التعليم العالي والبحث العلمي

جامعة بابل/كلية التربية للعلوم الصرفة

قسم الرياضيات

أنظمة امنية الصور

بحث مقدم الى مجلس كلية التربية للعلوم الصرفة قسم الرياضيات كجزء من متطلبات نيل شهادة البكلوريوس

من قبل الطالبة :

شهلاء ابراهيم عبد الكاظم

تحت اشراف:

أ.م. د ايناس حمود محيسن

١٤٤٤هـ

٢٠٢٣م

الاية الكريمة

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

[وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ۖ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُمْ بِمَا كُنْتُمْ تَعْمَلُونَ]

صدق الله العلي العظيم (سورة التوبة الاية ١٠٥)

الشكر والتقدير

قال تعالى : بسم الله الرحمن الرحيم [وَمنْ يَشْكُرْ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِ] سورة لقمان:١٢

و قال رسوله الكريم (صلى الله عليه واله): "من لم يشكر الناس ،لم يشكر الله عز وجل " ،احمد الله تعالى حمدا كثيرا طيبا مباركا ملى السموات والارض على ما اكرمني به من اتمام هذه الدراسة التي ارجو ان تنال رضاه.

ثم اتوجه بجزيل الشكر وعظيم الامتنان الى استاذتي (د.أيناس حمود محيسن) على ما بذلته من جهد لغرض الاشراف على بحثي ومتابعتها لي بآرائها القيمة ومساعدتها لي بعلميتها فجزاها الله خير الجزاء كما اتقدم بخالص الشكر والتقدير الى جميع الاساتذة المحترمين في كلية التربية للعلوم الصرفة /قسم الرياضيات/جامعة بابل .

الاهداء

الى صاحبي عند شدتي.... وذكره يطمن قلبي ويجدد املي وقوتي....

الى صاحب الزمان (عجل الله فرجه) .

الى من كلله الله بالهيبة والوقار....الى من علمني العطاء بدون انتظار...

الى من احمل اسمه بكل افتخار....ابي الغالي.

الى ملاكي في الحياة....الى معنى الحب والحنان....

الى من كان دعائها سر نجاحي ....امي الغالية.

الى الشخص الذي كان هو سبب نجاحي....الى من انار دربي....

الى سندي ومشجعي الاول....الى زوجي .

الى فرحتي الاولى ....الى زينة حياتي وبهجتها ....

الى قرة عيني .... ابني.

فهرس المحتويات

الخلاصة

عملية الاتصال بين الناس من أهم الوسائل التي ساعدت على النمو البشري ،تتطلب هذه العملية سرية البيانات المنقولة، ولهذا الغرض فقد سعى الانسان إلى إيجاد طرق متنوعة يضمن من خلالها وصول البيانات بسرية مطلقة ويوجد العديد من التقنيات المستخدمة للحفاظ على امن وسرية المعلومات كالتشفير والاخفاء والعلامة المائية وغيرها.

ظهر التشفير كطريقة جيدة لحماية البيانات المرسلة وكانت الفكرة بان الاتصالات تكون في امان من خلال التشفير لكن هذا نادرا ما يكون صحيح في الواقع العملي فبرزت الحاجة لإيجاد طرق لإخفاء الرسائل بدل من تشفيرها ومع تطور عمليات الاختراق أصبح بإمكان المتطفلين الاطلاع على المعلومات وتغيرها . فظهرت الحاجة إلى اعتماد تقنية أكثر تطورا وأكثر سرية وحفاظا على المعلومات لذا تم استخدام نظام الإخفاء الذي تكون فيه المعلومات المرسلة غير مرئية لأي شخص وذلك عن طريق إخفائها داخل الوسائط المرسلة، مثل الصوت، الصورة والفيديو .

الهدف الاساسي من التشفير والاخفاء هو توفير الحماية للأشخاص ليتم الحفاظ على أمن معلوماتهم. وكما هو معلوم فلا يمكن الاستغناء عن ميزة أمن المعلومات في المواقع الحساسة مثل البنوك والتجارة الالكترونية والمواقع الأمنية .

الفصل الاول

التشفير

١-١ التشفير

التشفير هو عملية الحفاظ على سرية المعلومات باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز او تحويل النص الصريح الى مبهم بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف الغير مفهومة .

لذلك تعبر كلمة " تشفير" عن تحويل أو " بعثرة" البيانات إلى هيئة غير قابلة للفهم لإرسالها عبر وسط ناقل معين إلى جهة محددة . بحيث لايمكن لأي جهة غير الجهة المقصودة تفسير هذه البيانات المبهمة واستخلاص البيانات المفهومة منها وهذه العملية هي أعلى درجة أمان ممكنة.

والغرض من عملية تشفير الصور هو الحفاظ عليها من السرقة او العبث وخصوصاً اذا كانت صور خاصة او مهمة ولانرغب ان يراها احداً سوانا .

والصور هنا نتعامل معها على انها مجموعة من الارقام الثنائية حيث كل رقم في الصورة الرقمية يناظر مسافة صغيرة واحدة في الصور المرئية وهذه المسافة الصغيرة قد خصص لها عدد ثابت يسمى (Pixel) وهو يمثل اختصاراً لكلمة (Element Picture)وان حجم المساحة الفيزيائية بوحدة الصور (Pixel) يسمى (Resolution Spatial) لوحدة الصورة.

ويعد التشفير وحدة البناء الأساسية لأمن البيانات. وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض ضارة.

يُستخدم تشفير البيانات لتأمينها على نطاق واسع من قبل المستخدمين الأفراد والشركات الكبيرة بغرض حماية معلومات المستخدم المرسلة بين المستعرض والخادم. قد تشمل تلك المعلومات أي شيء من بيانات الدفع إلى المعلومات الشخصية. ويتم استخدام برنامج تشفير البيانات، المعروف أيضًا باسم "خوارزمية التشفير" أو "التشفير" فحسب، لتطوير مخطط تشفير لا يمكن اختراقه نظريًا إلا بقوة حوسبية هائلة.

١-٢ ميزات التشفير

١. السرية :لا يمكن الوصول الى المعلومات الى من قبل الشخص المقصود بها ولا يمكن لأي شخص اخر غيره الوصول اليه.

٢. النزاهة : لا يمكن تعديل المعلومات في التخزين او الانتقال بين المرسل والمستقبل المقصود دون الكشف عن اي اضافة الى المعلومات.

٣. عدم التنصل : لا يمكن لمنشى/مرسل المعلومات انكار نيته في ارسال المعلومات في مرحلة لاحقة.

٤. المصادقة : يتم تأكيد هويات المرسل والمتلقي وكذلك يتم تأكيد جهة ومصدر المعلومات.

١-٣ مفاهيم التشفير

١. المفاتيح الخاصة والعامة :

أحد أهم المفاهيم التي يتوجب معرفتها في التشفير هو المفتاح . يسمح لك المفتاح الخاص بوضع تواقيع رقمية لا يمكن تزويرها على الرسائل التي ترسلها إلى الاخرين، والمفتاح العلني هو ملف يمكنك إعطاؤه للأخرين أو نشره .

٢. شهادات الأمان :

شهادة الامان هي مفهوم آخر من المهم معرفته وفهمه، يمكن للمتصفح الأنترنت على جهازك إجراء اتصالات مشفرة مع المواقع باستخدام(HTTP) عندما يقوم بذكاء فانه يتفحص الشهادات للتأكد من المفاتيح العلنية للأسماء النطاقات مثل : ssd.eff.org أو www.amazon.com أو www.google.com الشهادات هي إحدى الطرق لتحديد ما إذا كنت تعرف المفتاح العلني الصحي لشخص أو موقع ما، بحيث يمكنك التواصل معهم بشكل آمن.

٣. بصمات المفاتيح:

إحدى استخدامات المصطلح هي "بصمة المفتاح"، وهي سلسلة من الاحرف مثل:

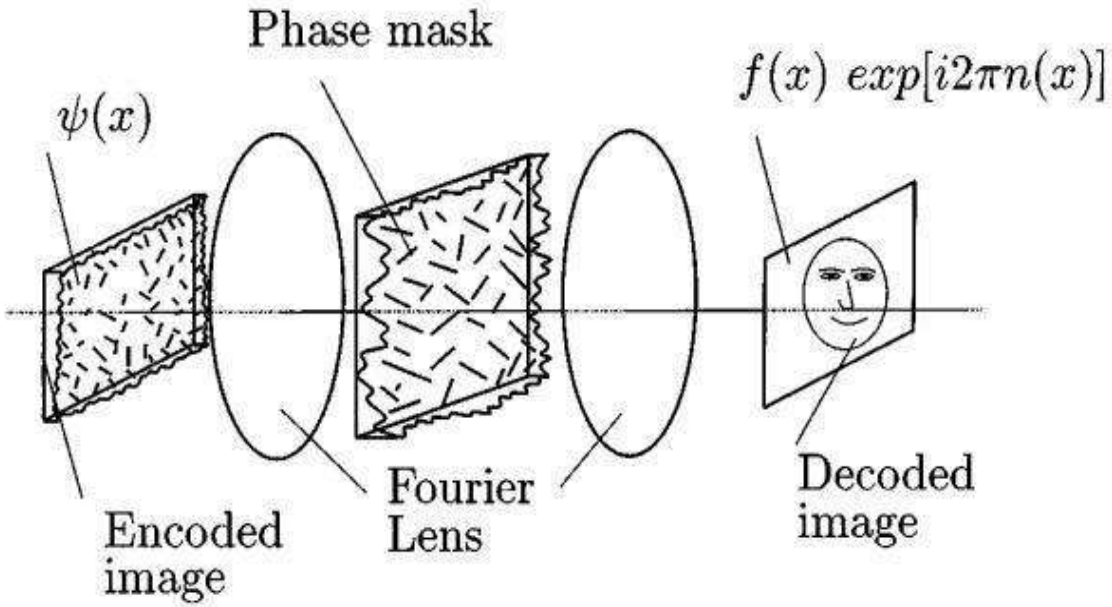
" 1928 2192 6c63 ff10 0912 bd20 2309 تسمح لك بالتحقق بشكل فريد من ان شخصا ما على الانترنيت يستخدم المفتاح الخاص الصحيح .

١-٤ التشفير البصري

التشفير البصري هو أسلوب نموذجي عالي الكفاءة لتشفير الصور ، ويتمثل جوهره في تدافع وترميز المعلومات الكامنة في صور النص العادي من خلال عمليات التحويل البصري ، مثل التداخل والانعراج والتصوير لتحقيق تأثير تشفير جيد. في عملية التشفير ، تشتمل السمات المتضمنة عادةً على الطول الموجي والبعد البؤري ومسافة الانعراج والطور والسمات الأخرى.يمكن استخدام هذه السمات كمفتاح متعدد الأبعاد لنظام التشفير.

من مزايا التشفير البصري تتمتع تقنية أمن المعلومات الضوئية بمزايا الأبعاد المتعددة والسعة الكبيرة وحرية التصميم العالية والتعقيد العالي.
اقترح Refregier لا ول مرة مقالاً في عام 1995 تشفير الصورة البصرية على أساس ترميز مزدوج عشوائي الطور.اقترح هذا العمل بشكل رائد المعالجة بين ترميز مرحلتين عشوائيتين ، له تأثير فعال على التشفير، حيث يتم وضع نموذجي طور عشوائي غير مرتبطين على مستوى الإدخال ومستوى فورييه لتشفير الصور، ويتم استخراج الصورة على مستوى الإخراج كصورة نص مشفر.

عملية التنفيذ المحددة هي كما يلي:
استخدم عدسة لتحويل النص العادي إلى مجال التردد ، وقم بمعالجته أولاً في مجال التردد ، ثم قم بتحويله إلى المجال المكاني من خلال عدسة أخرى لإخراج الصورة المشفرة وكما في الشكل (١-١):



(الشكل ١-١) تشفير الصورة البصرية على أساس ترميز مزدوج عشوائي الطور

يتم وضع نموذجي طور عشوائيين على التوالي بين العدسات ، وعندما يصل الضوء إلى المستوى البؤري الخلفي للعدسة ، يشع الضوء طيف فوريه.

$$\phi(x,y) = FT^{-1}\{FT[f(x,y).A(x,y)].B(\alpha,\beta)\} \qquad (1\text{-}1)$$

١-٥ استخدامات التشفير

يقابل معظمنا التشفير كل يوم. تشمل الاستخدامات الشائعة:

١. في كل مرة تستخدم فيها ماكينة صراف آلي أو تشتري شيئًا عبر الإنترنت باستخدام هاتف ذكي، يتم استخدام التشفير لحماية المعلومات التي يتم نقلها.

٢. تأمين الأجهزة، مثل التشفير لأجهزة الكمبيوتر المحمولة.

٣. تستخدم معظم مواقع الويب السليمة "طبقة المقابس الآمنة" (SSL)، وهي شكل من أشكال تشفير البيانات عند إرسالها من موقع ويب وإليه. وهذا يمنع المهاجمين من الوصول إلى تلك البيانات أثناء نقلها. ابحث عن رمز القفل في شريط URLوحرف "s" في "https://" للتأكد من أنك تجري معاملات آمنة ومشفرة عبر الإنترنت.

٤. يتم أيضًا تشفير رسائل WhatsAppالخاصة بك، وقد يكون لديك أيضًا مجلد مشفر على هاتفك.

٥. يمكن أيضًا أن يتم تشفير بريدك الإلكتروني باستخدام بروتوكولات مثل .OpenPGP

٦. تستخدم الشبكات الافتراضية الخاصة (VPN) التشفير، ويجب تشفير كل ما تخزنه في السحابة. يمكنك تشفير محرك الأقراص الثابتة بالكامل، بل إجراء مكالمات صوتية مشفرة.

٧. يستخدم التشفير لإثبات سلامة وصحة المعلومات، وهذا باستخدام ما يعرف بالتوقيعات الرقمية. التشفير جزء لا يتجزأ من إدارة الحقوق الرقمية وحماية المؤلفات.

٨. يمكن استخدام التشفير لمحو البيانات. نظرًا لأنه يمكن أحيانًا إعادة المعلومات المحذوفة باستخدام أدوات استعادة البيانات، فإنك إذا قمت بتشفير البيانات أولاً وتخلصت من المفتاح، فلن يمكن لأي شخص أن يسترد إلا النص المشفر وليس البيانات الأصلية.

١-٦ فوائد التشفير الأساسية

1. يساعد التشفير في الحفاظ على تكامل البيانات.
فالمتسللون لا يسرقون المعلومات فحسب؛ بل يمكنهم أيضًا تغيير البيانات لارتكاب عملية احتيال. وفي حين أنه من الممكن للمتسللين المهرة تغيير البيانات المشفرة، فإن مستلمي البيانات سيكونون قادرين على اكتشاف التلف، مما يسمح باتخاذ استجابة سريعة.
2. التشفير يساعد المؤسسات على الالتزام باللوائح التنظيمية .
تضع العديد من الصناعات، مثل الخدمات المالية أو الرعاية الصحية، لوائح صارمة حول كيفية استخدام بيانات المستهلك وتخزينها. ويساعد التشفير المؤسسات على تلبية هذه المعايير وضمان الامتثال لها.

٣. يحمي التشفير البيانات عند انتقالها عبر الأجهزة.
يستخدم معظمنا أجهزة متعددة في حياتنا اليومية، ويمكن أن ينطوي نقل البيانات من جهاز إلى آخر على بعض المخاطر. تساعد تقنية التشفير في حماية البيانات عبر الأجهزة، حتى أثناء النقل. كما تساعد إجراءات الأمان الإضافية، مثل المصادقة المتقدمة، في ردع المستخدمين غير المصرح لهم بالوصول.

٤. يساعد التشفير عند نقل البيانات إلى التخزين السحابي.

يقوم المزيد والمزيد من المستخدمين والمؤسسات بتخزين بياناتهم في السحابة، مما يعني أن أمان السحابة بات ضروريًا. يساعد التخزين المشفر في الحفاظ على خصوصية تلك البيانات. ويجب على المستخدمين التأكد من أن البيانات مشفرة أثناء نقلها، وأثناء استخدامها، وأثناء التخزين.

٥. التشفير يساعد المؤسسات على تأمين المكاتب.

يشمل العديد من المؤسسات مكاتب تعمل عن بُعد، وخاصة في مرحلة ما بعد الجائحة. يمكن أن يشكل ذلك مخاطر على الأمن الإلكتروني حيث يتم الوصول إلى البيانات من عدة مواقع مختلفة. وهنا، يساعد التشفير في الحماية من السرقة أو الفقد العرضي للبيانات.

٦. يحمي تشفير البيانات الملكية الفكرية.

تقوم أنظمة إدارة الحقوق الرقمية بتشفير البيانات في حالة السكون، ويُقصد بها في هذه الحالة الملكيات الفكرية مثل الأغاني أو البرامج، لمنع الهندسة العكسية والاستخدام غير المصرح به أو إعادة إنتاج المواد المحمية بحقوق النشر.

١-٧ التقنيات الشائعة فى التشفير

توجد طريقتان للتشفير هما الأكثر شيوعًا: التشفير المتماثل وغير المتماثل. يشير الاسمان إلى ما إذا كان يتم استخدام المفتاح نفسه للتشفير ثم لفك التشفير أم لا:

- مفاتيح التشفير المتماثلة: يُعرف هذا أيضًا باسم تشفير المفتاح الخاص. يكون المفتاح المستخدم للتشفير هو نفسه المستخدم لفك التشفير، مما يجعل هذا الأسلوب الأفضل للمستخدمين الفرديين والأنظمة المغلقة. وبخلاف ذلك، يجب إرسال المفتاح إلى المتلقي. على أن هذا يزيد من خطر التعرض للاختراق إذا اعترضته جهة خارجية، مثل المتسللين. لكن هذه الطريقة أسرع من الطريقة غير المتماثلة.

- التشفير غير المتماثل: يستخدم هذا الأسلوب مفتاحين مختلفين، أحدهما عام والآخر خاص، مرتبطَين معًا حسابيًا. والمفتاحان هما في الأساس أرقام كبيرة، وتم ربطهما معًا لكنهما ليسا متماثلين، ومن هنا جاءت التسمية "غير متماثل". يحتفظ المالك بالمفتاح الخاص سرًا، ويتم إما مشاركة المفتاح العام بين المستلمين المصرح لهم أو إتاحته للجمهور بشكل عام.

ولا يمكن فك تشفير البيانات المشفرة باستخدام المفتاح العام للمستلم إلا باستخدام المفتاح الخاص المقابل .

وعلى الرغم من كون التشفير طريقة جيدة لحماية المعلومات إلا أنه سهل الاكتشاف، ويمكن لي متطفل التلاعب بها، فكانت الحاجة إلى تقنية أكثر تطورا وأكثر سرية وحفاظ على المعلومات وخصوصا مع ظهور وتطور الشبكة العالمية للمعلومات (Internet)فتم اللجوء إلى نظام الإخفاء، لأن رؤية البيانات بصيغتها المشفرة تكفي لدفع المتطفل أو المهاجم إلى الاعتقاد بوجود بيانات مهمة أو حساسة تكمن في العشوائية أو في النص المشفر، فيبدأ باستخدام التقنيات المضادة للتشفير لمحاولة الحصول على محتواها، وحتى لو عجز عن تحقيق ذلك فأنه قد يعبث بها أو يحرفها أو يستخدم بعض الوسائل المتاحة لمنع وصولها إلى هدفها .

الفصل الثاني

الاخفاء

٢-١ مقدمة

هنـــاك طـــرق عديـــدة وكثيـــرة تلعـــب دوراً مهمًـــا فيمـــا يتعلـــق بـــأمن المعلومـــات، ومنهـــا الطريقـــة الأكثـــر شـــيوعاً والمعروفـــة بالتشـــفير (Cryptograph)وهـــو تغيير/إخفـــاء البيانـــات الأساســـية وفـــق أســـلوب معـين لتصـبح غيـر مقـروءة. هنـاك فـن آخـر يهـدف إلـى إخفـاء البيانـات كليًـا للتواصـل مـا بـين جهتـين بشـكل غيـر ظـاهر لجهـة ثالثـة، وهـذا مـا يعـرف بإخفـاء المعلومـات (Steganography)فهـي طريقـة أو تقنيـة لحجـب و إخفـاء البيانـات داخـل وسـيط رقمـي، حتـى يـتم إخفـاء أن هنـاك اتصـال او تبـادل معلومـات يـتم فـي الخفـاء، ولا يكـون علـى علـم بهـذا الاتصال إلا الأشخاص المعنيين.

٢-٢ تاريخ علم الاخفاء

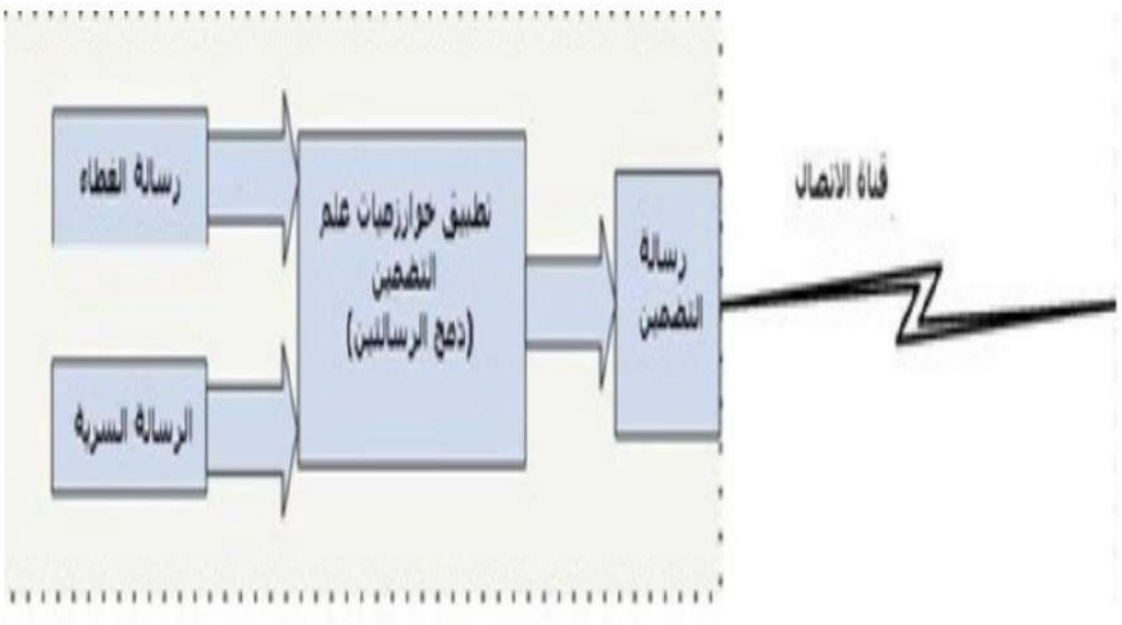
علـم الإخفـاء لا يعـد مـن العلـوم المسـتحدثة، كـان أول ظهـور لهـذا العلـم فـي العصـر الإغريقـي، حيـث قـام أحـد رجـالات العصـر التواصـل مـع احـد أقربائـه فـي اليونـان، عـن طريـق حلـق شـعر رؤوس عبيـده ثـم وشـم الرسـائل علـى رؤوسـهم بعـد ذلـك يقـوم بانتظـار نمـو شـعر رأسـهم ثـم إرسـالهم إلـى الشـخص الـذي يهـدف الـى التواصـل معـه، ثـم جـاء بعـده العديـد مـن الاشـخاص الـذين اسـتخدموا النـاس والحيوانـات والخشـب المغطى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية .

واسـتمر تطـور هـذا العلـم حتـى توصـل العـالم إلـى اختـراع الحبـر الخفـي إبـان الحـرب العالميـة الثانيـة والـذي سـاهم كثيـرا فـي التواصـل بـين الجبهـات فـي الحـرب بطريقـة بعيـدة عـن الشـبهات وسـالمة مـن التعقـب وكشف الأسرار.

وقـد تطـور علـم الإخفـاء فـي الوقـت الحـالي كثيـرا، فأصـبح يسـتخدم المعلومات الرقمية والحواسيب كوسيلة لنقل البيانات .

٢-٣ الاخفاء

هو علم وفن وتضمين البيانات المراد إرسالها (قد تكون رسائل نصية أو صورة) داخل بيانات مرسلة (قد تكون صورا أو ملفات الصوت أو الفيديو) وذلك لاحتوائها علي كمية كافية من البيانات التي تمكن المستخدم من إخفاء البيانات داخلها كما مبين افي الشكل التالي(٢-١):



الشكل(٢-١) تقنية اخفاء المعلومات

(Steganography) الكلمة من أصل يوناني و (stegano) تعني "مغطاة أو الخفية " و(graphy) كتابة .

تم تحديد قيم الاخفاء المعلومات أربعة أشياء :

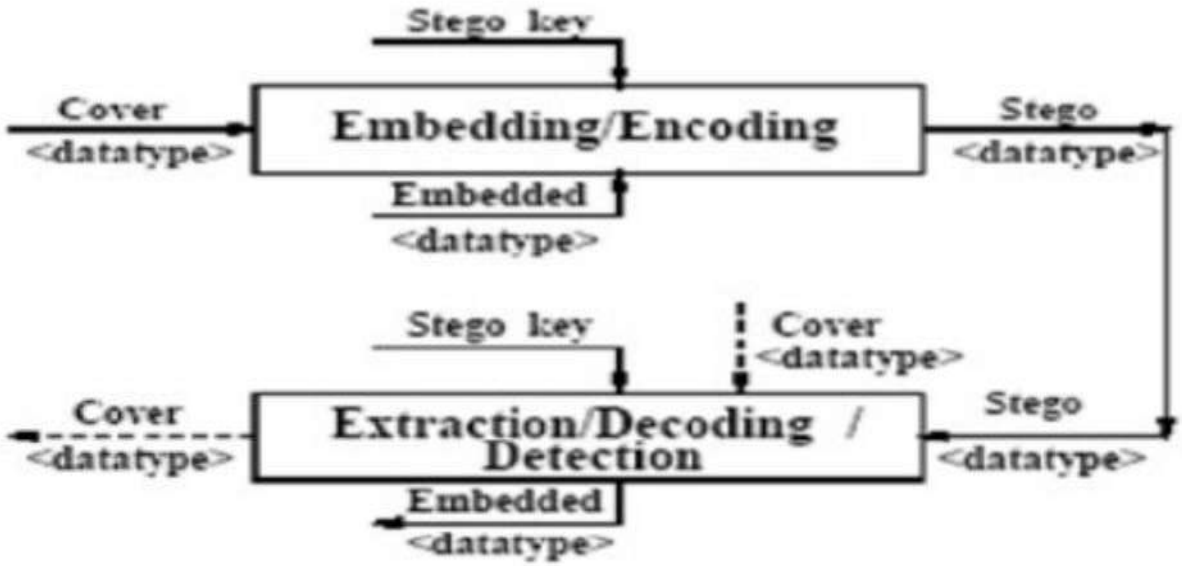
أ/النص (Message Hidden):الرسالة السرية المراد إخفاءها.

ب/غطـــاء (cover):الصـــورة أو الصـــوت التـــي ســـيتم اســـتخدامها لإخفاء النص.

ج/مفتاح(key):هو مفتاح يستخدم لتضمين النص داخل الغطاء.

د/كائن (Stego):هو جمع بين النص، غطاء ومفتاح.

كما مبين في الشكل(٢-٢)



الشكل(٢-٢) نظام اخفاء العام

٢-٤ الدراسات السابقة

١) زيادة سعة اخفاء المعلومات بطريقة ال(LSB) للنص والصورة:

هذه الدراسة مقدمة من قبل ArchanaAtha wale (Halanka.pallaviN) وهذه الطريقة يمكن تطبيقها على الصورة ذات الحجم ٢٤ خانه ثنائية، ,اقترحت تحسين طريقة الخانة الثنائية الاقل أهميه لزيادة سعة التضمين و الدقة، ويتم استخدام مفتاح سري طوله ثمانية خانة ثنائية وقبل أن تتم عملية التضمين تجري عمليه (XOR) للمفتاح السري والخانات الثنائية في الرسالة وكل نقطة في الصورة تحلل ويتم إجراء العمليات الآتية:

- إذا كانت قيمة النقطة في الصورة أكبر من أو يساوي ٢٤٠ وأقل من أو يساوي ٢٥٥ سوف يتم تضمين أربعه خانات ثنائية من البيانات السرية في أربعه خانات من الجهة اليسرى.
- إذا كانت قيمة النقطة أكبر من أو يساوي ٢٢٤ وأقل من او يساوي ٢٣٩ سوف يتم تضمين ثلاثة خانات ثنائية من البيانات السرية في ثلاثة خانات من الجهة اليسرى .
- إذا كانت قيمة النقطة في الصورة اقل من أو يساوي ٢٢٣ و أكبر من أو يساوي ١٩٢ سوف يتم تضمين خانتين ثنائيتين من البيانات السرية افي خانتين من الجهة اليسرى. إذا كانت قيمة الصورة أقل من أو يساوي ١٩٢ وأكبر من أو يساوي ٠ سوف يتم تضمين خانة ثنائيه من البيانات السرية في الخانة الاخيرة من الجهة اليسرى، هذه الطريقة لها مميزات منها زيادة السعة لتضمين المعلومات وسهولة وأداء افضل .

٢)اخفاء البيانات بسعة عالية مبنية على طريقة (LSB)

في الدراسة التي قدمها[Koppola Reddy Rajanikanth] الهدف منها اقتراح تقنية جديدة لإخفاء كمية كبيرة من البيانات. وهذه التقنية تسمح بإخفاء صورة داخل صورة أخرى لها نفس الحجم يتم تقليل حجم الرسالة السرية قبل الاخفاء لإخفاء كمية أكبر من البيانات . ويتم إخفاء البيانات في المناطق من الصورة التي لا تستطيع العين إدراك الاختلاف في الألوان . تم استخدام تقنية (RGBA) عباره عن قيمة تتراوح بين ٠-٢٥٥ حيث قيمة ٠ تعني الصورة شفافة والقيمة ٢٥٥ تعني الصورة معتمة . هذه التقنية صعب الهجوم عليها عند رؤية الصورة ولكنها قابلة للهجوم عن طريق الطرق الإحصائية ويمكن التغلب عليها باستخدام الضغط لزيادة سرية الصورة المستخدمة كغطاء. من مساوي هذه الدراسة تعاني من فقدان البيانات عند الاسترجاع لكنها تمتاز بجودة عالية بالإضافة إلى كمية كبيرة من البيانات

٣) تقنية تعدد المستويات في الصور:

اخفاء المعلومات متعددة المستويات، يكون في المستوى الاول وضع الرسالة النصية (M) في صورة من الابيض والأسود (الهدف الوسيط (-ID) والمستوى الثاني يأخذ من خرج المستوى الاول "اخفاء صورة ابيض اسود " كمدخل إلى صورة RGB(الثانية تغطى الهدف (C)فترض ان العناصر M تعطى في شكل مجموعة {M }من حجم المصفوفة | M | يتم ترميز كل عنصر من عناصر M ب M (nb)لكل بت. وبالمثل، {I }من حجم | ،|

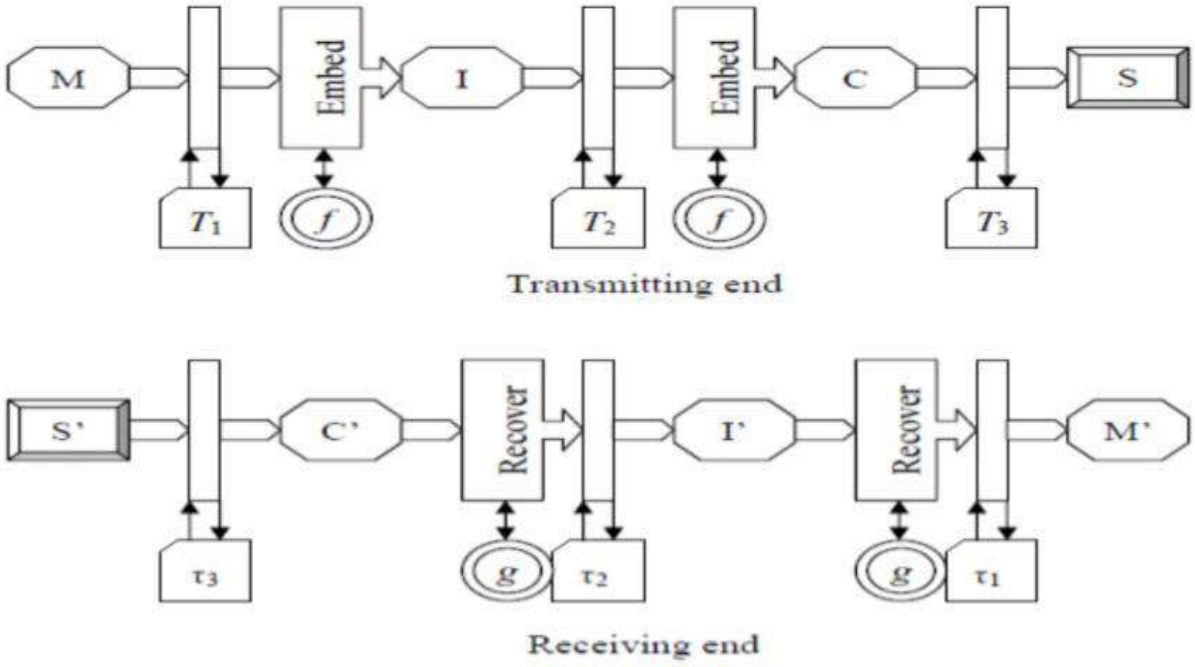
(Cl) من حجم | C| و {S }من حجم | S | تحدد مجموعات وأحجام كل عنصر لفك الشفرة في المرحلة المتوسطة (الشفرة

المغطـــاة) علـــى التـــوالي. وهـــذه الاهـــداف الوســـيطة {I or, D }تعمـــل كشـــكل غطـــاء للرســـالة المســـتهدفة {M } والرســـالة المغطـــاة{C }معـــا. الرســـالة {M }تمـــر عبـــر محـــولات T1 حيـــث يمكـــن ان تحتـــوى أي مـــن الاحتمـــالات (رســـالة مضـــغوطة، محولـــة او أي شـــفرة خاصـــة او عامة).

التحويـــل T1 يمكـــن ان يجمـــع أي مـــن التقنيـــات تحســـب التطبيـــق المفصـــل. ونفـــس الشـــيء يمكـــن أن يقـــال عـــن التحـــولات الاخـــرى T2T3 .فـــي المســـتوى الاول تتضـــمن الرســـالة محتـــوى الرســـالة المخفيـــة {I } or {D} .وخطيـــا LSB يطلـــب M.LSB(0) D.LSB(0) فـــي المســـتوى الثـــاني الهـــدف الوســـيط (الشـــرك(I or D)وهـــو خـــرج المســـتوى الاول صـــورة رماديـــة اللـــون مقـــاس Nr x Nc pixels مضمنة في صورة RGB .

النمـــاذج متعـــددة المســـتويات أكثـــر أمانـــا لإخفـــاء المعلومـــات مـــن المســـتويات العاديـــة. هـــذا يجـــب أن يرضـــى او يلبـــي رغبـــات معظـــم المتســـللين hackers. والمســـتلمين الأساســـين للرســـالة لـــديهم المعرفـــة علـــى حـــد ســـواء بمـــا هـــو مخفـــي لمحتـــوى الرســـالة فضـــلا عـــن الاحـــرف والمفـــاتيح (وغيرهـــا مـــن المعلومـــات) المطلوبـــة لفـــك الشـــفرة او استرداد الرسالة .

كما مبين في الشكل (٢-٣)



الشكل (٢-٣) متعددة المستويات المعلومات نموذج اخفاء

٤) إخفاء البيانات من خلال إخفاء متعدد المستويات SSEC :

هذه الدراسة مقترحة من قبل Indradip , Bhattacharyya Sanyal Gautam and Banerjee (Souvik) استخدم الجمع بين ميزات كل من النص والصورة القائمة على تقنية إخفاء المعلومات عن توصيل المعلومات بشكل أكثر امانا بين موقعين. أدرجت فكرة المفتاح السري للمصادقة عند كل الطرفين من أجل تحقيق مستوى عال من الامن. ونتيجة لزيادة تحسين مستوى الامان، تم ترميز المعلومات من خلال القيم SSCE وجزاء لا يتجزأ في نص الغلاف الوارد باستخدام طريقة إخفاء المعلومات النص المقترح لتشكيل النص المخفي. وقد استخدمت هذه التقنية الترميز عند كل الطرفين من أجل تحقيق مستوى عال من الامن ،

التـــالي تـــم تضـــمين الـــنص المخفـــي مـــن خـــلال طريقـــة PMM فـــي صـــورة الغـــلاف لتشـــكيل صـــورة المخفيـــة. فـــي الجانـــب المســـتقبل وقـــد تـــم تنفيذ العملية العكسية إليًا ترجع المعلومات الاصلية.

٥) خوارزمية إخفاء المعلومات لإخفاء رسالة سرية داخل صورة:

هـــذه الدراســـة مقترحـــة مـــن قبـــل (Suk Teoh and Ibrahim Rosziat Kuan

اســـتخدام خوارزميـــة رمـــوز الثنائيـــة وبكســـل داخـــل صـــورة وتقتـــرح هـــذه الورقـــة خوارزميـــة جديـــدة لإخفـــاء البيانـــات الـــداخل صـــور باســـتخدام تقنيـــة إخفـــاء المعلومـــات لتصـــميم خوارزميـــة لإخفـــاء كـــل البيانـــات المدخلـــة داخـــل الصـــورة لحمايـــة خصوصـــية البيانـــات، بعـــد ذلـــك يـــتم تطويرهـــا يقـــوم هـــذا النظـــام علـــى خوارزميـــة جديـــده لإخفـــاء المعلومـــات، هـــذا النظـــام المقتـــرح يـــوفر منصـــة صـــور للمســـتخدم لإدخـــال الصـــور ومربـــع نـــص لإدراج النصـــوص، يمكـــن للمســـتخدم إرســـال صـــورة stego الـــى مســـتخدمو كمبيـــوترا اخـــر بحيـــث المســـتقبل قـــادرا علـــى اســـترجاع و قـــراءة البيانـــات التـــي كانـــت مخفيـــة فـــي الصـــورة بواســـطة استخدام النظام المقترح نفسه .

٢-٥ الوسائط المستخدمة في إخفاء البيانات

١ .الملفات النصية:

عن طريق إخفاء الرسالة المراد إرسالها باستخدام النصوص، وتتم هذه الطريقة إما بطريقة نصية، مثل: يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفية أو بطريقة نحوية أو لفظية، ويعتبر هذا النوع من الاخفاء من أصعب أنواع الاخفاء.

٢ .الملفات الصوتية:

عن طريق إخفاء الرسالة المراد إرسالها باستخدام داخل إشارة صوتية يمكن أن تكون في مجال الزمن أو مجال الطيف.

٣ .مقاطع الفيديو:

يعتبر الاخفاء باستخدام ملفات الفيديو جزاء مشتقا من الاخفاء باستخدام الصور، وذلك لان ملفات الفيديو عبارة عن صورة مجتمعة، لأجل هذا تقنيات بالصور يمكن استخدامها في هذه الطريقة.

٤ .الصور:

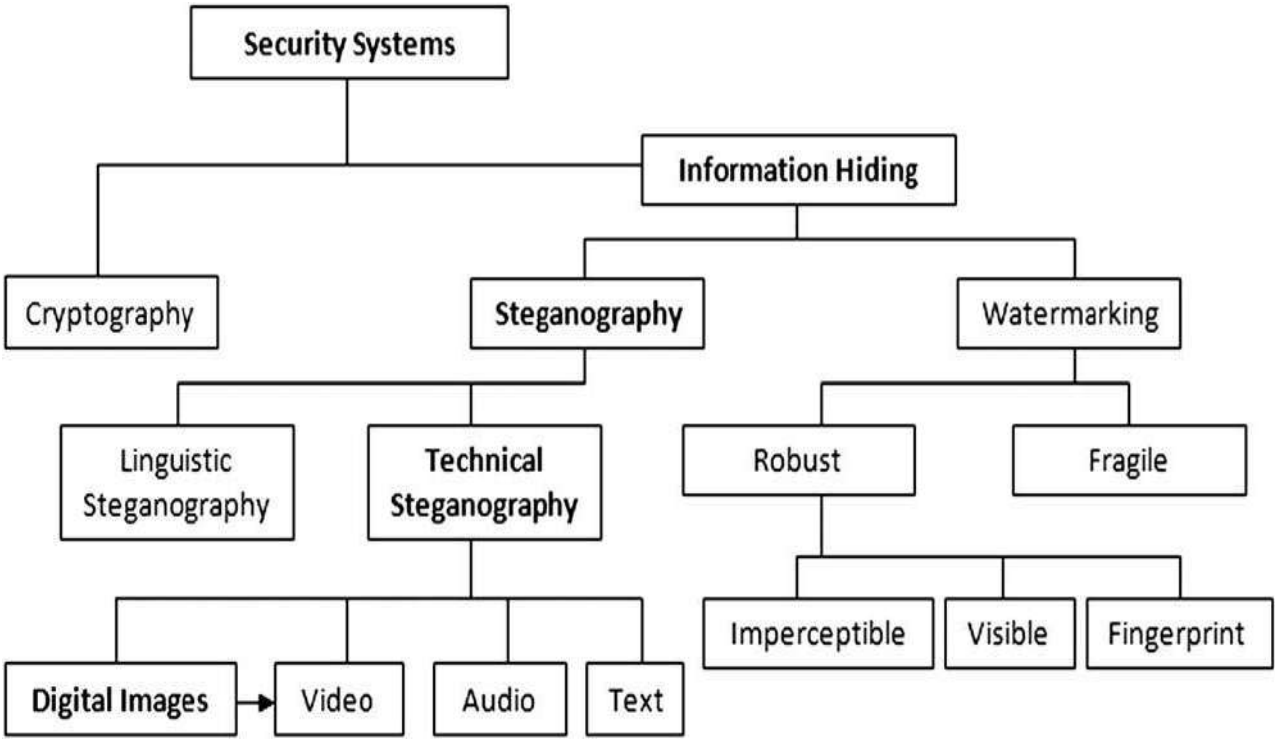
عن طريق إخفاء الرسالة المراد إرسالها باستخدام ملف صوري، يعد هذا النوع من الاخفاء من أكثر الأنواع انتشارا في الاستخدام لما تتميز به الصورة من صفات تجعلها الوسط المثالي للإخفاء.

ويتم تطبيق هذه النوع من الاخفاء باستخدام احد الطرق التالية:

- الإخفاء باستخدام التحويل الزاوي المتقطع (Transformation Cosine) Discrete
- الاخفاء باستخدام التحويل الموجي (Transform Wavelet Discrete)
- الإخفاء باستخدام الإدخال في البت الأقل أهمية (Bit Significant Least)

٢-٦ أنواع وطرق حجب البيانات

الشكل التالي (٢-٤) يوضح عدة أنواع وطرق لحجب البيانات والتي من بينها التشفير (Encryptionأو Cryptography)وإخفاء البيانات (Steganography) وكما هو موضّح، هنالك اقسام فرعية تحت كل نوع.



شكل(٢-٤) طرق إخفاء البيانات

٢-٧ أنماط إخفاء البيانات (Types of Steganography)

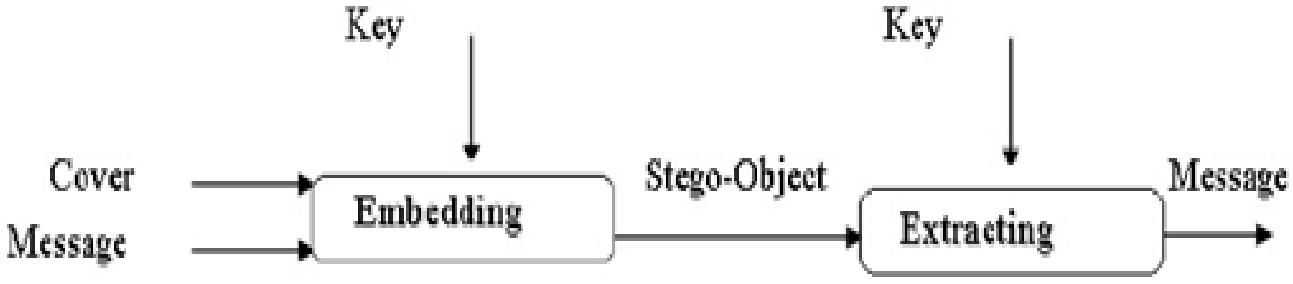
١. Pure Steganography

وهو النوع أو النمط العادي والخام من الأنماط المستخدمة لإخفاء المعلومات، هنا يتم تضمين المعلومات أو الرسالة الخفية داخل الوسيط بشكل مباشر وبدون كلمة سرية (شكل٢-٥):

شكل(٢-٥)الآلية المتبعة في النوع العادي أو الخام من إخفاء المعلومات

٢. Secret Key Steganography

يعني إخفاء المعلومات باستخدام مفتاح أو كلمة سرية تضاف للرسالة المخفية عند إخفائها داخل الوسيط المستهدف. وهكذا لا يمكن استرجاع أو قراءة الرسالة المخفية من قبل الطرف الثاني إلا بمعرفة الكلمة السرية، وبإضافة الكلمة السرية لعملية الإخفاء تكون العملية آمنة ومعقدة أكثر كما مبين في الشكل (٢-٦):

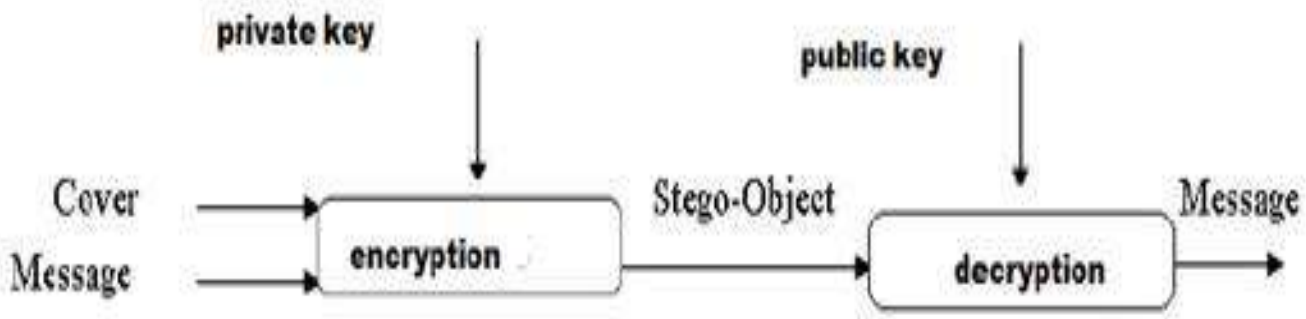


شكل(٢ -٦): الآلية المتبعة في إخفاء المعلومات مع استخدام كلمة سرية

٣. Public Key Steganography

ويعني إخفاء المعلومات باستخدام مفتاح عام، والعملية هنا تشبه العملية المتبعة في التشفير عن طريق استخدام مفتاحين، الأول مفتاح "عام" ويستخدمه الشخص الأول عند عملية إخفاء المعلومة، ويتم استخدام المفتاح الثاني "الخاص" من قبل الشخص المستقبل عند استرجاعه للمعلومة المخفية، مع العلم أن المفتاح الخاص له علاقة مباشرة مع المفتاح العام .

كما مبين في الشكل (٢-٧)



شكل (٢-٧) الآلية المتبعة في إخفاء المعلومات مع استخدام كلمة سرية

٢-٨ التطبيقات المستخدمة في إخفاء البيانات(Steganography)

تستخدم طريقة إخفاء المعلومات (Steganography) في الكثير من التطبيقات المفيدة مثل تعزيز البطاقات التعريفية الذكية، حيث أن طريقة إخفاء المعلومات تلعب دور مهم في إخفاء تفاصيل معينة داخل صور الأفراد، كذلك، في الشبكات في حزم TCP/IP حيث يتم إخفاء أو تضمين كلمة سر غير مكررة داخل صورة ما حتى يتم تحليل حركة مرور الشبكة لمستخدم معين. لتوضيح الفكرة أكثر، لنأخذ على سبيل المثال الصور، يتم إخفاء معلومات معينة داخل

صـــورة مـــا، فـــي حـــين أن أي شـــخص ينظـــر لهـــذه الصـــورة يـــرى أنهـــا طبيعيـــة جـــداً ولا يخطـــر ببالـــه أنهـــا فـــي الحقيقـــة تحـــوي شـــيئاً مـــا بـــداخلها. الشـــكل (٢-٨): (صـــورة القطـــة) تـــم اســـتخدامها كغطـــاء لحجـــب المعلومـــة ولإخفـــاء أن هنـــاك تبـــادل معلومـــات يـــتم بـــين شخصـــين فـــي الخفاء. هل يمكنك ملاحظة الفرق؟

الشكل (٢-٨) استخدام صورة القطة لإخفاء المعلومات

هذا ويتم استخدام خوارزميات مختلفة لإخفاء معلومة معينة داخل الصور، وكل خوارزمية لها خصائصها وميزاتها وعيوبها، وتختلف طريقة العمل من طريقة لأخرى، و من أشهر برامج إخفاء المعلومات في الصور: Jstegو Outguess و JPHide، وغيرهم من البرامج التي يمكن تحميلها من الإنترنت.

وبنفس الفكرة، يمكن استخدام الملفات النصية و الصوتية لإخفاء بيانات أو معلومات معينة، في حين لو قرأت النص المعني (الظاهر) أو سمعت مقطع الصوت لوجدته طبيعيًا جداً.

الطرق و الأساليب التي تستخدم لإخفاء المعلومات كثيرة ومختلفة وكلٌ له مزاياه وعيوبه، كما أن هناك الكثير من الطرق و الأساليب لكشف هذه المعلومات المخفية.

الفصل الثالث

الاستنتاجات

الاستنتاجات

١. اخفاء المعلومات و تشفير المعلومات عبارة عن وسيلتان مختلفتان من وسائل حماية المعلومات.
٢. الاخفاء يعمل على اخفاء وجود المعلومات بينما التشفير يعمل على اخفاء محتويات المعلومات.
٣. النتيجة النهائية لإخفاء المعلومات هي عنصر الاخفاء بينما النتيجة النهائية للتشفير هي النص المشفر.
٤. ليست ثمة خوارزمية محددة لإخفاء بل يعتمد على الطبيعة البشرية بينما يعتمد التشفير على خوارزميات معروفة.
٥. هناك عدة وسائط لإخفاء البيانات منها الفيديو وملفات الصوت ولكن الصورة الرقمية هي الاكثر استخداما .
٦. الغرض من عملية تشفير الصور هو الحفاظ عليها من السرقة او العبث وخصوصا اذا كانت صور خاصة او مهمة ولا نرغب ان يراها احد سوانا.
٧. يحمي التشفير البيانات عند انتقالها عبر الأجهزة.
٨. التشفير يساعد المؤسسات على تامين المعلومات المهمة.
٩. توجد طريقتان للتشفير هما الأكثر شيوعا التشفير المتماثل وغير متماثل.

المصادر

[١] رهام جاسم عيسى ، إنعام محمد سليمان ، " استخدام الخوارزمية الجينية في تشفير بيانات صورية رمادية وإخفاءها في صورة " ، كلية علوم الحاسوب والرياضيات ، جامعة الموصل ، العراق ، (٢٠١٣) .

[٢] شهد عبدالرحمن حسو ايلاف اسامه عبد المجيد " تطبيق نظام التغطية على الصور الملونة من نوع (BMP) " ، كلية علوم الحاسوب والرياضيات ، جامعة الموصل ، العراق ، (٢٠٠٨) .

[٣] شيماء شكيب ، همسة معن ، " طريقة خوارزمية جينية مثلى للإخفاء " ، كلية علوم الحاسوب والرياضيات ، جامعة الموصل ، العراق ، (٢٠١١) .

[4] Steganography Uses and Effects on Society , by Karen Korhorn http://cpsr.org/prevsite/essays/2002/2rr3.htm

[5] l Kekre , H. B. , Archana Athawale , and Pallavi N. Halamkar . " Increased Capacity of Information Hiding in LSBS Method for Text and Image . " International Journal of Electrical , Computer and Systems Engineering 2.4 (2008) : 246-249

[6] Koppola , Rajanikanth Reddy . A High Capacity Data - Hiding Scheme in LSB - Based Image Steganography . Diss . University of Akron , 2009

[7] Al - Najjar , Atef Jawad . " The decoy : multi - level digital multimedia steganography model . " WSEAS International Conference . Proceedings . Mathematics and Computers in Science and Engineering . No. 12. World Scientific and Engineering Academy and Society , (2008)

[8] Bhattacharyya , Souvik . " Data hiding through multi level steganography and SSCE . " Journal of Global Research in Computer Science 2.2 (2011)

[9] Ibrahim , Rosziati , and Teoh Suk Kuan . " Steganography algorithm to hide secret message inside an image . " arXiv preprint arXiv :1112.2809 (2011)

[10] http://www.kutub.info " Retrieved on (May 10 , 2016)

[11] Sayed , " Multi Level Network Steganography " Sudan . University June (2014)

[12] http://www.boosla.com " Retrieved on (Aug 20 , 2016)

[13]https://educad.me/67189/%D8%A5%D8%AE%D9%81%D8%A7%D8%A1%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%85%D9%82%D8%AF%D9%85%D8%A9/