**الفصل الثاني (الجانب النظري)**

**إخفاء المعلومات** [بالإنجليزية](https://ar.wikipedia.org/wiki/%D9%84%D8%BA%D8%A9_%D8%A5%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A%D8%A9): (steganography) هو علم وفن إخفاء [الرسائل](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B1%D8%B3%D8%A7%D8%A6%D9%84) بطريقة لايعرف بوجودها سوى [المرسل](https://ar.wikipedia.org/w/index.php?title=%D8%A7%D9%84%D9%85%D8%B1%D8%B3%D9%84&action=edit&redlink=1) [والمستقبل](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84). قد تظهر الرسائل المخفاه بشكل آخر: صورة، مقالة صحفية، قائمة تسوق.

[الحبر المخفي](https://ar.wikipedia.org/wiki/%D8%AD%D8%A8%D8%B1_%D8%B3%D8%B1%D9%8A) أستخدم قديما لإخفاء الرسائل بحيث تبدو الورقة بيضاء فارغة.

تختلف [التعمية](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%AA%D8%B9%D9%85%D9%8A%D8%A9) بالأخفاء عن [التشفير](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%AA%D8%B4%D9%81%D9%8A%D8%B1) في أن الرسالة لاتظهر. بينما الرسالة المشفرة تثير الشبهة وتجذب الانتباه, قد تكون غير أجرامية في البلدان التي تحظر التشفير. لهذا التشفير يحمي المحتوى بينما التعمية بالأخفاء تحمي الرسالة وأطراف  التواصل.

[إخفاء المعلومات](https://ar.wikipedia.org/wiki/%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) هو فن وعلم من كتابة الرسائل المخفية بطريقة لا أحد غير المرسل والمتلقي يشتبه في وجود الرسالة، وهو شكل من أشكال [الأمن من خلال الغموض](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D9%85%D9%86_%D8%AE%D9%84%D8%A7%D9%84_%D8%A7%D9%84%D8%BA%D9%85%D9%88%D8%B6). و [ستيغانوغرافي](https://ar.wikipedia.org/wiki/%D8%B3%D8%AA%D9%8A%D8%BA%D8%A7%D9%86%D9%88%D8%BA%D8%B1%D8%A7%D9%81%D9%8A) الكلمة من أصل يوناني وتعني “الكتابة المخفية”. وكان أول استخدام للمصطلح سجلت في 1499 من قبل [يوهانس تريثموس](https://ar.wikipedia.org/wiki/%D9%8A%D9%88%D9%87%D8%A7%D9%86%D8%B3_%D8%AA%D8%B1%D9%8A%D8%AB%D9%85%D9%88%D8%B3) في كتابه بعنوان [يوهانس تريثيموس](https://ar.wikipedia.org/wiki/%D9%8A%D9%88%D9%87%D8%A7%D9%86%D8%B3_%D8%AA%D8%B1%D9%8A%D8%AB%D9%8A%D9%85%D9%88%D8%B3)، وهو أطروحة عن التشفير وإخفاء المعلومات متنكرا في زي كتاب عن [السحر](https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B3%D8%AD%D8%B1). عموما المثال التقليدي هو رسالة مخبأة بالحبر السري أو غير المرئي بين السطور. الكتابة بالحبر السري كان بداية الكتابة المخفية.

أساس علم إخفاء البيانات (Steganography)

كلمة Steganography في الأساس مشتقة من كلمة يونانية تعني “الكتابة المخفية”.

موضوع إرسال رسالة مخفية عن طريق حجب أن هناك شيء مرسل من الأساس هي طريقة (وفكرة) قديمة. ولها قصة تاريخية بدأت أيام الإمبراطورية اليونانية القديمة عندما كانت تكتب الرسائل على رؤوس العبيد آنذاك بعد حلق شعر العبد، حيث يكتب على رأسه رسالة سرية معينة، وعندما يعود شعره للنمو مرة أخرى تختبئ الرسالة السرية تحت شعره الكثيف، وعندها، يتم إرساله للطرف الثاني يقوم بدوره بحلق رأس العبد مرة أخرى حتى يستطيع قرأة الرسالة، وهكذا كانت بدايات استخدام هذة الطريقة لإخفاء رسالة أو معلومة ما تحت غطاء أو شيء ما حتى لا يكون هناك علم أن أي إتصال سري يتم مابين إثنين أو أكثر.

الفرق بين إخفاء البيانات (Steganography) والتشفير (Encryption)

ربما سمعت سابقًا بمصطلح التشفير (Encryption أو Cryptography) وهو – باختصار – تشفير المعلومة لتصبح غير مفهومة وغير قابلة للقرآة إلا من قبل الشخص الذي يمتلك مفتاح التشفير لفك الشفرة وكل من يحصل على هذا المفتاح. التشفير يكون دائمًا لغرض حماية وأمن المعلومات وأسباب تشفير المعلومات كثيرة، منها: تبادل بيانات سرية بين شركات معينة، بين دوائر حكومية معينة، وغيرها. في المقابل، عند الرغبة في إخفاء المعلومات (Steganography) فإننا نقوم بتضمين المعلومات داخل وسيط ما وتحت غطاء معين بحيث لا تظهر هذه الرسالة لمن يستعرض الوسيط الأساسي (سواءً كان صورة أو فيديو) لأنها مخفية تمامًا داخله، وهذا أشبه ما يكون بالتواصل من وراء الكواليس.

بالتالي، نستطيع القول أن الفرق الأساسي بين التشفير وإخفاء المعلومات هو أنه عند تشفير (Encryption أو Cryptography) معلومة ما، يستطيع الطرف الثالث معرفة أن هناك إتصال يتم مابين طرفين (شخصين أو جهتين) لكنه لا يستطيع فهم المعلومات لأنها مشفرة. أما في حالة إخفاء المعلومات (Steganography)، لا يعلم الطرف الثالث بأن هناك شيء مخفي في الخفاء أو أن هناك إتصال بين إثنين يتم من وراء الكواليس لأنه تم استخدام وسيط ما لإخفاء هذا الإتصال تمامًا.

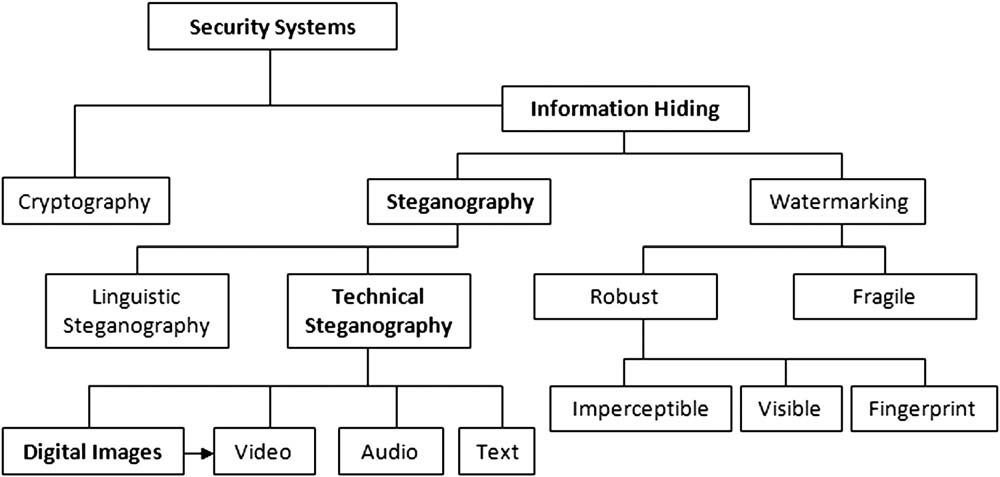
**الوسائط المستخدمة في إخفاء البيانات (Steganography)**

**الوسائط المستخدمة في إخفاء البيانات**

**أبرز الوسائط التي تستخدم في إخفاء المعلومات أربعة وهي:**

* الملفات النصية.
* الصور.
* الملفات الصوتية.
* مقاطع الفيديو.

## أنواع وطرق حجب البيانات

الشكل التالي يوضح عدة أنواع وطرق لحجب البيانات والتي من بينها التشفير (Encryption أو Cryptography) و إخفاء البيانات (Steganography)، وكما هو موضّح، هنالك أقسام فرعية تحت كل نوع.

## أنماط إخفاء البيانات (Types of Steganography)

### Pure Steganography

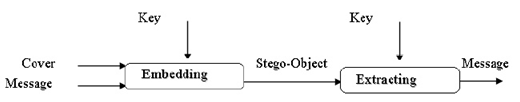
وهو النوع أو النمط العادي والخام من الأنماط المستخدمة لإخفاء المعلومات، هنا يتم تضمين المعلومات أو الرسالة الخفية داخل الوسيط بشكل مباشر وبدون كلمة سرية (شكل ١).



**شكل ١: الآلية المتبعة في النوع العادي أو الخام من إخفاء المعلومات**

### Secret Key Steganography

يعني إخفاء المعلومات بإستخدام مفتاح أو كلمة سرية تضاف للرسالة المخفية عند إخفائها داخل الوسيط المستهدف. وهكذا لا يمكن إسترجاع أو قراءة الرسالة المخفية من قبل الطرف الثاني إلا بمعرفة الكلمة السرية، وبإضافة الكلمة السرية لعملية الإخفاء تكون العملية آمنة ومعقدة أكثر (شكل ٢).



**شكل ٢: الآلية المتبعة في إخفاء المعلومات مع إستخدام كلمة سرية**

### Public Key Steganography

ويعني إخفاء المعلومات بإستخدام مفتاح عام، والعملية هنا تشبة العملية المتبعة في التشفير عن طريق إستخدام مفتاحين، الأول مفتاح “عام” ويستخدمه الشخص الأول عند عملية إخفاء المعلومة، ويتم إستخدام المفتاح الثاني “الخاص” من قبل الشخص المستقبل عند إسترجاعه للمعلومة المخفية، مع العلم أن المفتاح الخاص له علاقة مباشرة مع المفتاح العام (شكل ٣).

## 3

**شكل ٣: الآلية المتبعة في إخفاء المعلومات مع إستخدام كلمة سرية**

## 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 صورة ما، في حين أن أي شخص ينظر لهذة الصورة يرى أنها طبيعية جداً ولا يخطر بباله أنها في الحقيقة تحوي شيئاً ما بداخلها.  
الصورة التالية (صورة القطة) تم إستخدامها كغطاء لحجب المعلومة ولإخفاء أن هناك تبادل معلومات يتم بين شخصين في الخفاء. هل يمكنك ملاحظة الفرق؟  
[](http://educadme.wpengine.netdna-cdn.com/wp-content/uploads/cat.jpg)

هذا ويتم استخدام خورازميات 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: Jsteg و Outguess و JPHide، وغيرهم من البرامج التي يمكن تحميلها من الإنترنت.

**شكل 4: الآلية المتبعة في إخفاء المعلومات مع إستخدام كلمة سرية**

### Public Key Steganography

ويعني إخفاء المعلومات بإستخدام مفتاح عام، والعملية هنا تشبة العملية المتبعة في التشفير عن طريق إستخدام مفتاحين، الأول مفتاح “عام” ويستخدمه الشخص الأول عند عملية إخفاء المعلومة، ويتم إستخدام المفتاح الثاني “الخاص” من قبل الشخص المستقبل عند إسترجاعه للمعلومة المخفية، مع العلم أن المفتاح الخاص له علاقة مباشرة مع المفتاح العام (شكل ٣).

## 3

**شكل5: الآلية المتبعة في إخفاء المعلومات مع إستخدام كلمة سرية**

## 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 صورة ما، في حين أن أي شخص ينظر لهذة الصورة يرى أنها طبيعية جداً ولا يخطر بباله أنها في الحقيقة تحوي شيئاً ما بداخلها.  
الصورة التالية (صورة القطة) تم إستخدامها كغطاء لحجب المعلومة ولإخفاء أن هناك تبادل معلومات يتم بين شخصين في الخفاء. هل يمكنك ملاحظة الفرق؟  
[](http://educadme.wpengine.netdna-cdn.com/wp-content/uploads/cat.jpg)

هذا ويتم استخدام خورازميات 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: Jsteg و Outguess و JPHide، وغيرهم من البرامج التي يمكن تحميلها من الإنترنت.