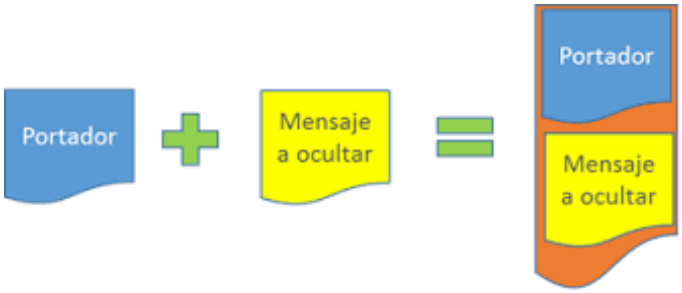
UD3.2. Esteganografia

La esteganografia (del grec steganos, "cobert" o "ocult", i graphos, "escriptura") tracta l'estudi i aplicació de tècniques que permeten ocultar missatges o objectes, dins d'uns altres, anomenats portadors, per a ser enviats i de manera que no es perceba el fet. És a dir, procura ocultar missatges dins d'altres objectes i d'aquesta manera establir un canal encobert de comunicació, de manera que el propi acte de la comunicació passe inadvertit per a observadors que tenen accés a aqueix canal.



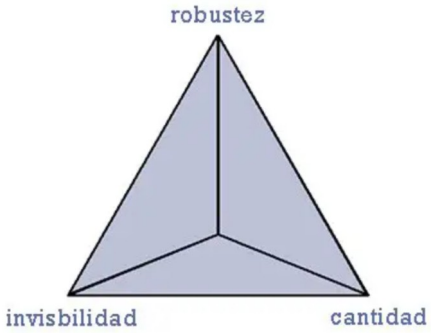
Amb esteganografia i criptografia, en ambdues, s'intenta ocultar un missatge per a ser enviat, però són fonamentalment diferents, donat que la criptografia només xifra els missatges, mantenint-los visibles però irrecognoscibles (apareixen com una seqüència de caràcters il·legibles) i per a veure el seu contingut original és necessari conéixer una clau. En la esteganografia, l'arxiu o objecte que conté el missatge ocult s'observarà idèntic a l'original, i per a conéixer el seu missatge contingut serà necessari conéixer la clau i l'algorisme (programari) amb el qual es va ocultar.

Encara que habitualment solem considerar la esteganografia com una tècnica per a ocultar informació dins d'imatges, la veritat és que existeixen molts altres tipus:

Esteganografia pura: No existeix estegano-clau, i per tant, es pressuposa que l'observador és incapaç de reconéixer una informació oculta mitjançant estegano d'un missatge normal. S'aplica llavors seguretat basada en la foscor, i el millor exemple és aquest mini repte hacking que es pot trobar **ací** , on la imatge té oculta una altra imatge que qualsevol pot obtindre obrint el camuflatge (la primera imatge) amb un descompressor qualsevol.

- Podem situar les dades ocultes (disfressats) en:
- En les METADADES de la imatge (visor de pdf, exiftool, ...)
- Com a fitxer "annex" o "pegat", concatenant informació (amb compressió)
- Amagat en el Thumbnail d'un fitxer, imatge, video...
- En la mateixa imatge (a simple vista, amb LSB, amb canal Alpha

Esteganografia de clau secreta: En aquest cas, la estegano-funció depén d'una clau que han de conéixer tant l'emissor com el receptor. Un exemple senzill seria un text ocult sota un altre text generat aleatòriament a partir d'un capítol d'un llibre que els dos (emissor i receptor) coneguen i una contrasenya que dictarà el com desxifrar el missatge camuflat.



La esteganografia té per tant una terna en l'equilibri de la qual radica la funció per a la qual s'ha desenvolupat. Habitualment, les tècniques de esteganografia que permeten ocultar major informació (quantitat) són menys robustes i passen menys desapercebudes (invisibilitat). Per contra, a major robustesa, normalment menor quantitat d'informació oculta.

Tècniques mes utilitzades en esteganografia.

- En documents
- En imatges
- En àudio
- En vídeo
- En arxius de qualsevol tipus.
- Altres. Una nova tècnica esteganogràfica implica l'injectar retards (coneguts per la seua traducció a l'anglés com "delays") imperceptibles als paquets enviats sobre la xarxa des del teclat. Els retards en el tecleig dels comandos en alguns usos (telnet o programari d'escriptori remot) poden significar un retard en paquets, i els retards en els paquets es poden utilitzar per a codificar dades.

Activitat: ESTEGANO-1
Busca en este document, informació amagada.
pista (no està en esta pàgina)

Activitat: ESTEGANO-2
En una mv Kali Linux, instal·la la utilitat **Steghide** i busca informació de com s'utilitza.
Descriu les seues opcions i prova-les. Utilitza la imatge d'aquest enllaç i crea un fitxer de text anomenat secret.txt. Dins del fitxer escriu el teu nom i data de naixement. Amaga este fitxer dins de la imatge de l'enllaç.

Activitat: ESTEGANO-3
En una mv Windows 10 , baixa la utilitat FileFriend d' http://www.filefriend.net/
Utilitza l'opció d'amagar un fitxer dins d'un altre

Activitat: ESTEGANO-4
Instal·la la utilitat exiftool i explora el fitxer del enllaç . Busca la «password»