Esteganografia (més exercicis)

A continuació es detallaran diversos mètodes d'ocultament d'informació en fotografies fent servir tècniques d'edició digital.

1.-a) Obre amb el GIMP la fotografia "cel.jpg" proporcionada pel professor. Com que en aquest exercici s'utilitzarà el truc d'emprar les transparències de la imatge per amagar-hi un missatge i el format JPG no admet transparències, el primer que hauràs de fer serà afegir a cada píxel de la foto, a més dels seus canals RGB ja existents, un nou canal: el canal "Alpha" (és a dir, el canal que indicarà el grau de transparència que tindrà el píxel en qüestió). Això es fa anant al menú "Capes->Transparència->Afegeix canal alfa"

> NOTA: Òbviament, caldrà tenir en compte al final de tot de guardar la imatge resultant en un altre format diferent de JPG que sí que admeti les transparències afegides, com és el cas del format PNG. Quan arribi el moment ja ho indicarem pertinentment en un apartat posterior d'aquest exercici.

b) Gràcies a haver fet el pas anterior, ara, en crear una nova capa, aquesta podrà ser transparent. Això és justament el que hauràs de fer en aquest apartat: crea una nova capa en la imatge que sigui totalment transparent. Això es fa anant al menú "Capes->Capa nova..." i al quadre emergent que apareix, triar en l'opció anomenada "Omple amb..." el valor "Transparència"

c) Tenint la capa transparent activada com la capa on treballar (això és fàcil comprovar-ho al diàleg incrustat "Capes" que hauries de tenir visible a la dreta de la finestra del GIMP), escriu-hi un missatge qualsevol fent servir l'eina de text present al quadre d'eines visible a l'esquerra de la finestra del GIMP (el color, la mida i la font de lletra pot ser qualsevol). Un cop finalitzada l'escriptura, tria una altra eina qualsevol del quadre d'eines per tal de sortir del mode d'edició de text i, finalment, molt important, clica sobre el botó que apareix a la part inferior del diàleg incrustat "Capes" que realitza la fusió de la capa activa (en aquest cas, la del text escrit...cada text al GIMP és generat automàticament en una capa pròpia) amb la capa inferior (en aquest cas, la capa transparent) per tal d'integrar el text dins de la capa transparent i així ésser tota ella una sola.

d) Sel·lecciona ara només les parts NO trasparents de la capa transparent (és a dir, les lletres del missatge de text). Això es fa, tenint la capa transparent encara com a capa activada on treballar, anant al menú "Capes->Transparència->Alfa a selecció"

e) Canvia la capa activada de treball per a què ara sigui la de la foto original. Tria del quadre d'eines del GIMP l'eina "Goma d'esborrar" i modifica en el seu panel d'opcions el valor d'"Opacitat" per a que sigui molt baix (entre 1 i 5, no més!).

> NOTA: L'eina "Goma d'esborrar" és similar al pinzell, només que pinta "transparent"; com més alt sigui el seu valor d'opacitat, més transparent pintarà. Per tant, el que hem fet aquí és configurar-la per a què el que es pinti amb ella sigui només una mica transparent però no gaire (de fet, imperceptible, que és el que es pretén).

f) Encara treballant a la capa de la foto original, pinta tota la zona que coincideixi amb les lletres del missatge secret.

> NOTA: El que hem fet en l'apartat anterior és afegir una mica de transparència (però no massa, degut al baix nivell d'opacitat de l'eina goma d'esborrar) a tots els píxels de la capa activa de treball que coincideixin amb la zona sel·leccionada, la qual són precisament les lletres del missatge secret. Cal saber que, tot i que la zona sel·leccionada pertanyi a una altra capa diferent de la capa de treball, les eines de dibuix del GIMP tenen en compte sempre la sel·lecció que hi hagi per definir els seus límits d'actuació, estigui aquesta sel·lecció definida en la pròpia capa de treball o no.

g) Elimina la capa on s'ha escrit el missatge secret (ja que ja no és necessària) i guarda la imatge final en format PNG (ja que si no, com ja s'ha comentat, el canal "Alpha" no es guardaria i, per tant, tot aquest truc que estem fent no serviria de res). Això es fa anant al menú "Fitxer->Anomena i exporta" i indicant al nom de la imatge a guardar l'extensió ".png".

h) Obre la imatge resultant amb un visor de fotografies qualsevol: hauries de comprovar que a simple vista no es nota res estrany ja que el missatge incrustat dins de la imatge hauria de ser invisible (degut a què els píxels que formen el missatge són una mica més transparents que la resta de la imatge però no prou per distingir-se)

1BIS.-a) Per veure el missate ocult segons el mètode indicat a l'exercici anterior, després d'obrir la imatge esteganogràfica amb el GIMP, vés al menú "Colors->Components->Descompon" i, al quadre emergent que apareix, tria en l'opció "Model de color" el valor "Alfa".

> NOTA: El que hem fet en l'apartat anterior és extreure en una nova imatge a part (que apareixerà en una nova pestanya del GIMP) el valor del canal "Alpha" dels pixels de la imatge original. És a dir, obtindrem una nova imatge on tots els píxels opacs de la imatge original es visualitzen en aquesta nova imatge amb el color blanc i els píxels de la imatge original amb certa quantitat de transparència es visualitzen en aquesta nova imatge amb tons de gris més o menys foscos fins arribar al negre, que indicarà que aquell pixel en concret era totalment transparent a la imatge original.

b) És probable que la imatge que aparegui en fer l'apartat anterior es vegi completament blanca degut a què el grau de transparència que hem fet servir amb l'eina "Goma d'esborrar" no és massa elevat (aquesta era la gràcia de què el missatge passés desapercebut). Per a mostrar els píxels amb una mica de transparència hem de modificar el llindar visible en aquesta nova imatge. Això es fa anant al manú "Colors->Llindar..." i desplaçant el trianglet de color negre a les posicions necessàries a dreta o esquerra fins que el missatge sigui finalment visible.

2.-a) Obre amb el GIMP la fotografia "cel.jpg" proporcionada pel professor i fes servir l'eina "Pipeta" present al quadre d'eines visible a l'esquerra de la finestra del GIMP per tal d'obtenir el color d'una zona de la imatge corresponent al cel clar. Veuràs com aquest color s'ha activat com a color de primer pla.

b) Clica sobre el quadradet de "color de primer pla" per a què aparegui el quadre emergent de tria de colors i modifica el color actualment sel·leccionat (és a dir, el triat a l'apartat anterior) per a què sigui molt semblant però diferent (el més fàcil és que modifiquis el valor indicat a la caixa "Notació HTML" per un altre valor hexadecimal proper i pulsis enter).

c) Pulsa el botó de "D'acord" del quadre emergent anterior i ara tria l'eina de text del quadre d'eines per escriure en alguna zona de cel clar de la imatge un text qualsevol (la mida i la font són indiferents, però no hauries de ser capaç de veure res degut a què el color del text és molt semblant al del color de fons, tal com s'ha indicat a l'apartat anterior). Un cop finalitzada l'escriptura, tria una altra eina qualsevol del quadre d'eines per tal de sortir del mode d'edició de text

d) Guarda la imatge final amb un altre nom anant al menú "Fitxer->Anomena i exporta" i indicant al nou nom de la imatge. Obre la imatge resultant amb un visor de fotografies qualsevol: hauries de comprovar que a simple vista no es nota res estrany

2BIS.-a) Per veure el missate ocult segons el mètode indicat a l'exercici anterior, després d'obrir la imatge esteganogràfica amb el GIMP, vés al menú "Filtres->Detecció de vores" i allà tria alguns dels diferents filtres que surten llistats ("Diferència de gaussians", "Vora...", "Laplace", "Neó..."). Al quadre emergent que t'apareixerà, desplaça les opcions que se't mostrin per tal de modificar els valors del filtre concret triat: en algun moment se t'haurà de mostrar el missatge secret

> NOTA: Els filtres de detecció de vores el que fan és detectar amb diferents mètodes la diferència de colors entre els píxels, marcant visualment la "frontera" entre els diferents colors existents en una imatge

3.-a) Una eina online molt interessant per detectar la presència dins d'imatges d'aquests tipus de missatges ocults que juguen amb l'ús de canals de colors dins d'imatges (però no només, perquè també és capaç de detectar contingut LSB i d'altres tipus, com veurem al següent apartat) és https://stegonline.georgeom.net (el codi font de la qual es troba disponible a https://github.com/Ge0rg3/StegOnline/tree/master) . Prova-la per intentar trobar, fent servir les eines "Full Red", "Full Green", "Full Blue" o "Browse Bit Planes" que allà se't proporciona, els missatges secrets inclosos dins de les imatges creades per tu als exercicis 1 i 2.

NOTA: Teniu més informació sobre els diferents mètodes de detecció utilitzats per aquesta eina a https://stegonline.georgeom.net/checklist Moltes d'ells es poden aconseguir amb l'eina Gimp (per exemple, el seu menú "Colors->Inverteix" seria idèntic a l'opció anomenada "Inverse (RGB)" en la web) però és de reconèixer que aquesta web ho posa tot més senzill (com per exemple, l'opció "Show RGBA values", la qual mostra els valor numèric dels píxels, molt útil si aquests valors -passats a ASCII, per exemple- fossin ells mateixos el propi missatge ocult!). Una eina web similar és https://github.com/mindcrypt/visual-forensic-steganography

NOTA: Existeixen també diverses eines natives per detectar també la presència de missatges incrustats en imatges (fent servir diferents mètodes, alguns ja coneguts, com la detecció de LSBs (amb nombre de bits variables, però) o d'inversió de bits, o mitjançant la separació de canals RGBA, la detecció de colors semblants o la inspecció de paletes de colors en imatges indexades, o via detecció de dades Zlib incrustades i/o de metadades i cadenes, o via detecció d'ocultacions fetes amb eines específiques con OpenStego o altres, etc). En aquest sentit tenim l'eina **Zsteg** (https://github.com/zed-0xff/zsteg , escrita en Ruby), útil només per imatges PNG/BMP o **Stegoveritas** (https://github.com/bannsec/stegoVeritas , escrita en Python), útil per múltiples formats de imatge o Stegano (https://wiki.cedricbonhomme.org/security:steganography, escrita en Python), la qual també pot fer-se servir com eina d'ocultació esteganogràfica "a l'ús", o **Aletheia** (https://github.com/daniellerch/aletheia, escrita en Python) la qual també detecta missatge oculs en diferents formats d'imatges fent servir diferents mètodes, entre els quals, a més dels mencionats anteriorment, també s'inclouen uns quants basats en "machine learning" (de fet, aquesta eina necessita un nombre elevat de llibreries AI instal·lades per funcionar...una introducció al seu funcionament es pot trobar a https://daniellerch.me/stego/aletheia/intro-es

b) Puja a la web anterior la fotografia "penguin.jpg, proporcionada pel professor, la qual té un contingut incrustat mitjançant LSB. Tria l'opció "Extract Files/Data" i juga amb el nombre de bits (I canals a extreure) per aconseguir obtenir aquest contingut.

NOTA: Fixa't que la web també té opcions similars a les comandes conegudes *binwalk*, *strings* o *exiftool* D'altra

4.-a) Llegeix primer https://www.fotoforensics.com/tutorial.php?tt=ela (i també les pestanyes "Evaluating" i "Sample") per tal de, un cop pujada a través del formulari https://www.fotoforensics.com una fotografia JPEG qualsevol que tinguis a mà, puguis deduir si aquesta ha sigut modificada digitalment o no.

NOTA: La pàgina https://www.fotoforensics.com/tutorial.php conté moltíssima informació molt valuosa per conèixer l'estructura interna dels diversos formats de fotografia digital i descobrir múltiples conceptes, tècniques, trucs i eines per esbrinar si una determinada fotografia ha sigut manipulada un cop presa. Visita molt recomanable!

aII) Realitza els diferents exercicis llistats a https://www.fotoforensics.com/messages.php?challenge=1 (els quals contenen cadascun d'ells una petita ajuda incorporada si la necessites)

b) Vés a https://29a.ch/photo-forensics/#help i esbrina per a què serveix l'eina "Error Level Analysis" d'aquesta eina online. Tot seguit utilitza-la amb una fotografia qualsevol (pots ser alguna de les utilitzades en apartats anterior o qualsevol altra descarregada d'Internet) i observa el resultat

bII) ¿Per a què serveixen les eines "Clone detector", "Noise Analysis" i "Luminance Gradient" de la web anterior?. Prova-les també.

NOTA: Una eina nativa similar a les webs anteriors és **Ghiro** (http://www.getghiro.org), la qual, però, es pot provar online també a http://www.imageforensic.org