INTEGRITAT DE LES IMATGES ESTÀTIQUES

Frederik Temmermans (1, 2), Fred Truyen (3), Ann Dooms (4), Peter Schelkens (1, 2), Bruno Vandermeulen (5)

1. Vrije Universiteit Brussel (VUB), Departament d'Electrònica i Informàtica (ETRO), Pleinlaan 2, B-1050 Brussel·les, Bèlgica - 2. imec, Kapeldreef 75, B-3001 Lovaina, Bèlgica - 3. KU Leuven, CS Digital, Blijde-Inkomststraat 21, B-3000 Lovaina, Bèlgica - 4. Vrije Universiteit Brussel (VUB), Departament de Matemàtiques (DWIS), Pleinlaan 2, B-1050 Brussel·les, Bèlgica - 5. KU Leuven, Laboratori Digital, Digitalització i Préstec de Documents, Serveis Centrals de Biblioteques, Mgr. Ladeuzeplein 21, B-3000 Lovaina, Bèlgica

Introducció

Com podem assegurar-nos que la còpia digital que estem produint, copiant, distribuint i emmagatzemant és fidel a l'original? Aquesta és la pregunta que intentem abordar en aquest article. Les tecnologies digitals han fet que la creació, edició, distribució i emmagatzematge d'imatges sigui molt accessible per al públic en general. No obstant això, la facilitat de la manipulació digital comporta uns inconvenients clars. D'una banda, estimula una creativitat interminable (penseu en Photoshop), però de l'altra estem cada vegada menys segurs de si la còpia digital que estem veient és una còpia exacta de la imatge digital original.

És fàcil pensar en situacions en què aquesta qüestió tingui una importància similar. Les fotos manipulades de notícies han portat a la difusió de notícies i rumors falsos on la força ineludible d'una imatge (que sempre sembla aportar un cert tipus d'evidència «directa», fins i tot quan està fortament mediatitzada) ha donat una força aterridora a la desinformació. Les fotos dels historials mèdics, en què es basen les pòlisses d'assegurances, també són susceptibles de frau. Però en aquest article ens agradaria centrar-nos en la imatge digital en el món de l'arxiu. Volem plantejar el context pràctic, així com les tècniques matemàtiques i els esforços d'estandardització que poden ajudar a elevar els fluxos de treball d'integritat de les imatges.

L'article s'organitza de la manera següent. La secció 2 aprofundeix en el significat pràctic i els desafiaments de la integritat de les imatges en el context dels arxius digitals. La secció 3 presenta una sèrie de solucions matemàtiques aplicables per detectar la manipulació o provar l'autenticitat. La secció 4 se centra en els esforços que du a terme el comitè de normalització JPEG per oferir funcionalitats al nivell dels fitxers d'imatges per donar suport als casos d'ús de la integritat de les imatges i millorar la interoperabilitat. La secció 5 presenta les tecnologies de registres distribuïts i de cadenes de blocs i il·lustra com es poden fer servir en un context d'integritat de les imatges.

RESUMEN

La necesidad de contar con métodos fiables que permitan demostrar la integridad de las imágenes digitales es cada vez más importante. Las imágenes se pueden manipular fácilmente para dar una falsa impresión de realidad, lo que se suma al problema de las noticias falsas. Las imágenes son consideradas además obras de creación y pueden estar sujetas a derechos de autor. En consecuencia, ser capaz de probar cuando, donde o cómo se capturó una imagen concreta, va adquiriendo importancia. La tecnología *Blockchain* (cadena de bloques) ofrece una solución para crear registros distribuidos a prueba de manipulaciones. Sin embargo, la adopción de la tecnología *blockchain* para la integridad de la imagen digital plantea varios retos. Este artículo pasa por varios casos de uso sobre integridad de imagen y presenta soluciones técnicas.

SUMMARY

The need for reliable methods that can proof the integrity of digital images increases rapidly these days. Images can easily be tampered with to give a false impression of reality, adding to the problem of fake news. Images are also creative works and may be subject to copyrights. Consequently, being able to proof when, where or how a specific picture was taken gains importance. Blockchain technology provides a solution for creating tamper proof distributed ledgers. However, adopting blockchain technology for digital image integrity poses several challenges. This paper walks through several image integrity use cases and presents technical solutions.

Integritat de les imatges en el context dels arxius digitals

Un dels aspectes més importants de la noció d'arxiu és que el document que s'hi diposita pot ser recuperat intacte i inalterat anys després. La missió fonamental d'un arxiver és garantir que això sigui possible. Aquesta confiança fonamental en el paper custodiador de l'arxiver és el que dóna a la imatge la seva base social i institucional. No tindria cap sentit mantenir registres si no estiguéssim segurs que quan es recuperin estaran inalterats.

Quan els arxius s'exposen a la digitalització, han de ser conscients de l'enorme impacte que pot tenir la digitalització en aquesta missió fonamental. Aquesta qüestió constitueix el nucli del que està en joc quan es digitalitza el contingut dels arxius. La digitalització es pot dur a terme per diversos motius relacionats amb la missió d'un arxiu: per a l'accés, per a la comunicació, per a la preservació i per a la recerca.

Segons el tipus material i l'objectiu, la digitalització requereix nivells de qualitat i/o fidelitat diferents. És una bona pràctica que els arxius digitalitzin el seu contingut en la resolució més avançada i amb fidelitat alta, de manera que pugui servir per a la majoria dels usos. No obstant això, els requisits poden ser molt divergents. Per facilitar la comunicació i l'accés, és suficient (i important) que l'aparença visual de l'objecte estigui representada fidelment i que els usuaris tinguin una percepció correcta de les seves propietats, sovint convertides en estàndards de publicació web. L'usuari necessita tenir una impressió correcta de la feina. Això vol dir que el flux de treball de digitalització ha d'abordar qüestions com ara la gestió del color, la garantia de la qualitat, etc. Algunes vegades es fan intervencions manuals, per exemple, amb programes d'edició fotogràfica, per corregir els nivells, el contrast o l'equilibri.

No obstant això, les exigències de la digitalització canvien radicalment en funció dels objectius de la preservació. En cas que l'original estigui en perill de no ser preservat a causa de l'estat físic en què es troba o per motiu de limitacions econòmiques, la preservació mitjançant la digitalització implicaria capturar tantes propietats físiques i materials de l'original com sigui tècnicament possible, fent servir un procediment estandarditzat com a base i referència. A més, se'n poder fer més captures amb una il·luminació concreta, com la llum rasant, o tècniques específiques, com imatges multiespectrals o amb llums múltiples, per revelar propietats que no són visibles o que ho són poc mitjançant la digitalització estàndard. Es tracta d'un enfocament més orientat a les dades que a l'usuari. Les tecnologies de digitalització sempre han conegut limitacions. Això vol dir que és preferible la precisió numèrica[1] a la fidelitat perceptiva de la representació. Com més estandarditzada sigui la digitalització (captures amb procediments rigorosos, un control ple, un flux de treball de garantia de la qualitat i documentació dels paràmetres de la captura), més fàcil serà reprocessar el treball quan les noves tecnologies o els nous coneixements especialitzats permetin corregir un biaix conegut de la tecnologia de digitalització usada durant la captura. Per a la recerca, és perfectament possible realitzar digitalitzacions més enllà de l'estat d'avantguarda amb configuracions experimentals en funció del tema de recerca. No obstant això, en aquest article no parlarem de la fidelitat de la reproducció digital del document original, sinó que ens centrarem en la reproducció, precisió i fidelitat de la còpia digital.

Qualsevol accés a una imatge digital original equival a produir una còpia digital d'aquesta imatge. Podem treure una fotografia en paper d'una caixa d'arxius i lliurar-la a un investigador. Ell o ella tindrà l'original en mà. Això no ho podem fer amb una imatge digital. L'únic que podem fer és copiar el flux de dades i mostrar-lo en un altre mitjà, ja sigui una pantalla, una impressió, un arxiu nou. Per a una imatge digital, assegurar-nos que tenim accés a la imatge original significa simplement que volem que la sèrie de bits de la imatge original sigui exactament la mateixa que la sèrie de bits de la còpia.

Però això és només una part del problema. Se suposa que no podem anar-nos-en de l'arxiu amb l'original en paper. Podríem fer una fotocòpia o un facsímil, però això implica un cost i és molt fàcil discernir l'original de la còpia. També es pot tornar a reconstruir l'original amb la còpia. Però fer una còpia d'un original digital és molt fàcil i implica molt poc d'esforç i/o cost. Normalment, l'arxiu reproduït és idèntic a l'original. No conté cap referència al flux de bits de l'original, és simplement idèntic a aquest.

Això significa que una vegada que una còpia digital d'un original digital surt de l'arxiu, es pot estendre com un virus i se'n podrien fer i compartir milers de còpies. No obstant això, igual que amb els virus, pot haver-hi errors de còpia (sovint per culpa de les manipulacions de la imatge: retallar, redimensionar o remostrejar) i, al final, hi ha una gran varietat de còpies menys o més divergents de l'original. Això s'ha descrit com el «síndrome de la lletera groga»[2]. Quan busquem per Internet imatges d'aquesta famosa pintura, hi trobem un gran nombre de còpies amb característiques diferents. Per descomptat, la imatge apareix en mides diferents, però també hi ha una àmplia varietat de va-

1. Per exemple, el Color Checker SG d'X-rite.

2. https://yellowmilkmaidsyndrome.tumblr.com/, https://pro.europeana.eu/post/the-yellow-milkmaid-syndrome-paintings-with-identity-problems

riacions en el color, nitidesa, retallades, escales no proporcionals i distorsions similars.

Una altra qüestió és la distribució no neutral. Quan els usuaris comparteixen imatges a Internet i pugen un arxiu al servidor d'una plataforma de mitjans socials o d'un servei d'intercanvi d'imatges, sovint creuen que és una simple còpia d'arxiu. No obstant això, en molts casos la imatge realment és reprocessada i reproduïda. Això té un impacte en una sèrie d'aspectes de la imatge. En alguns casos, desapareixen les metadades originals[3]. En el cas dels arxius codificats en format jpeg comú, se solen fer servir metadades Exif[4] i IPTC/XMP[5] per incloure informació com el creador de la imatge, el propietari dels drets d'autor, etc. Quan la plataforma torna a renderitzar la imatge, és possible que aquesta informació s'hagi eliminat. De fet, hi ha una tendència a fer-ho per protegir la privacitat dels usuaris que pugen fotos.[6].

A més, la renderització de la imatge pot fer servir un nivell de compressió i/o una profunditat diferent, o fins i tot autocorregir o simplement modificar la llum o el balanç de color. Això significa que fer circular una imatge a través d'una sèrie de plataformes d'intercanvi d'Internet augmentarà gradualment la divergència entre la còpia i l'original. Per tant, una còpia d'una còpia no és sempre una còpia de l'original.

La font i el context d'un objecte digital són altres aspectes que cal tenir en compte. Els objectes o documents no sempre contenen informació contextual suficient per poder identificar adequadament el seu significat. Una fotografia d'una troballa arqueològica pot ser inútil sense la informació addicional sobre on s'ha fet, qui l'ha feta i quan. També és possible que vulgueu saber en quina capa terrestre s'ha trobat l'objecte. Moltes representacions digitals d'aquests objectes o documents van acompanyades de metadades descriptives per tal d'aclarir aquest context. Aquestes metadades s'emmagatzemen normalment en sistemes d'informació de fora de l'arxiu mateix. El model que se segueix habitualment és el CIDOC-CRM[7]. Per a un arxiver, és pràctica habitual agrupar els objectes d'arxiu segons l'ordre original: per exemple, cinc fotografies d'un sobre s'han de considerar una «col·lecció» que ha d'estar unida. Si volem digitalitzar un llegat fotogràfic, per exemple, una col·lecció trobada en una caixa d'un estudi fotogràfic, sembla raonable indicar que unes fotos estaven juntes en un sobre i les altres estaven en un àlbum de fotos i que totes estaven en la caixa. No cal explicar que la història del sobre, l'àlbum de fotos i la caixa pot dir-nos més sobre les fotos de dins.

Imatge retocada amb Photoshop d'un llançament de míssils iranians el juliol de 2008.

Imatge original del llançament de míssils de prova.

No obstant això, aquest tipus d'informació contextual, que va molt més enllà de la informació que s'emmagatzema dins del contenidor de la imatge a través d'estàndards com EXIF i IPTC/XMP, pel fet que s'emmagatzema a banda de l'arxiu d'imatge, se sol perdre quan l'arxiu es copia al llarg del seu recorregut per l'esfera d'Internet. Salvaguardar la integritat de les metadades contingudes en els arxius no és suficient

3. Vegeu la prova de metadades de mitjans socials d'IPTC: http://www.embeddedmetadata.org/social-media-test-results.php

4. https://www.photometadata.org/META-Resources-metadata-types-standards-Exif

5. https://www.photometadata.org/META-Resources-metadata-types-standards-XMP

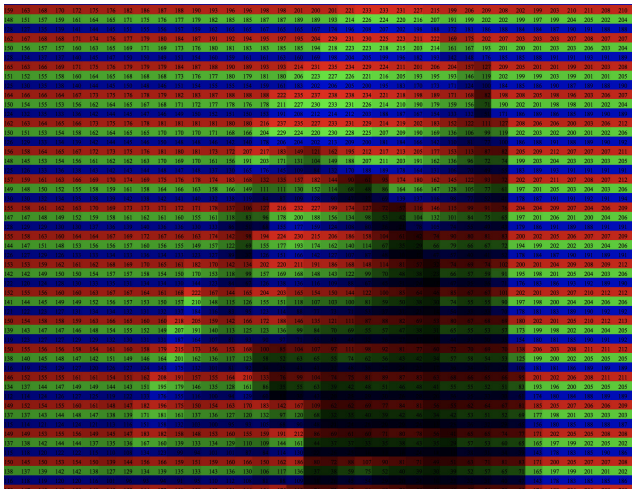
6. M. Smith, C. Szongott, B. Henne i G. von Voigt, "Big data privacy issues in public social media," 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Campione d'*2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, Campione d'Italia, 2012, pàg. 1-6. DOI: 10.1109/DEST.2012.6227909. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6227909&isnumber=6227884. S. Tayeb i altres., "Toward metadata removal to preserve privacy of social media users," *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2018, pàg. 287-293. DOI: 10.1109/CCWC.2018.8301741. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8301741&isnumber=8301613

7. http://www.cidoc-crm.org/

per contrarestar aquesta pèrdua de traçabilitat. Per poder tornar a rastrejar l'origen i, per tant, la font i el context d'aquestes imatges es requereixen tecnologies que permetin a) cercar imatges similars a Internet i b) comparar arxius per trobar-hi dependències. Recorda la difícil tasca de *stemmatology*, en la qual els estudiosos tracten de reconstruir la transmissió dels texts, per exemple, en manuscrits medievals.

En el cas de la fotografia, hi ha una complicació addicional que és que pel fet que un fotògraf pot prendre moltes fotos d'una escena, i en temps moderns pot fer-ho a gairebé la mateixa velocitat de l'obturador, així, originals diferents poden mostrar menys variacions que les còpies d'un únic original. Per tant, és important trobar tècniques que permetin almenys determinar la dependència exacta entre còpies digitals. Hi ha una aplicació més senzilla que separa les còpies digitals preses d'un negatiu original de les fetes a partir de les possibles impressions.

La lletera, de Johannes Vermeer, Rijksmuseum.



Primer plànol de La lletera com a taula Excel amb els colors d'acord amb els respectius números.

Solucions matemàtiques

La tecnologia digital facilita l'edició de les imatges. Tots coneixem els retocs de Photoshop en revistes de moda i fem servir diàriament els filtres d'Instagram. No obstant això, l'edició digital no és sempre innocent i una qüestió de pura estètica. Un exemple és que el juliol de 2008 vam ser víctimes d'una notícia falsa amb imatges digitals. El portal iranià Sepah News havia enviat una imatge manipulada (ni tan sols bona) d'un llançament de míssils de prova que va enganyar totes les agències de notícies d'arreu del món. Aviat es va veure que el tercer míssil era un copia i enganxa del segon i el quart.

Això va demostrar la necessitat de fer servir eines per detectar automàticament la manipulació de les imatges, ja que la inspecció visual humana és molt tediosa i no sempre reeixida (un observador humà pot ser enganyat fàcilment)[8]. La idea principal de la detecció automàtica és considerar una representació numèrica de la imatge digital i traduir els problemes de detecció de manipulacions en transformacions matemàtiques per detectar certs patrons o desviacions dins de la sèrie numèrica.

Una imatge digital que apareix en una pantalla es compon de petits blocs de colors compostos per llum vermella, verda i blava. Aquests blocs s'anomenen píxels, una contracció dels mots en anglès *picture* (imatge) i *elements* (elements). La pantalla rep instruccions sobre on il·luminar els colors i amb quina intensitat a través d'una taula gran amb números, generalment entre el 0 i el 255. Per cada píxel hi ha 256 possibilitats (descrites amb 8 bits) per a vermell, verd i blau, que aporten la rica paleta de color de les anomenades *imatges RGB,* que són capaces d'aproximar-se a la nostra realitat d'una manera bastant acceptable.

Podeu veure la gran varietat de números que representen una imatge per exemple en Excel o amb programes informàtics avançats com Matlab.

Ara presentarem breument algunes solucions matemàtiques per comprovar o verificar la integritat d'una imatge. Aquesta llista dista molt de ser exhaustiva, però se centra en les tècniques més importants.

8. Un altre exemple perillós en la recerca mèdica: http://jcb.rupress.org/content/166/1/11.full

Yezhov apareix clarament a l'esquerra de Stalin.

La foto va ser modificada posteriorment per censors soviètics.

Detectar la clonació

Un ordinador és capaç de detectar les edicions de copia i enganxa, anomenades *clonació*, d'una imatge com la dels míssils, però pot ser molt complicat. De fet, s'han de comparar els grups de números de la imatge per a cada mida possible, una tasca massa tediosa. A més, un clon d'una part d'una imatge no està format necessàriament pels mateixos números. Fins i tot l'alteració geomètrica més mínima portarà a numeracions de color diferents (a causa de les interpolacions de la malla discreta). A més, també podem esperar alteracions de color lleugeres fetes a propòsit.

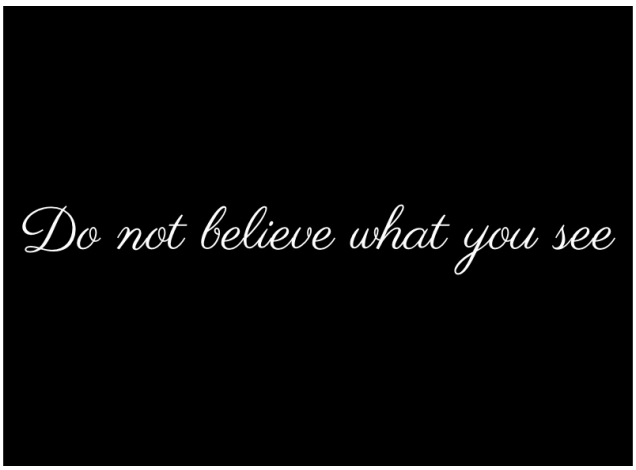
Una solució consisteix a guiar l'ordinador per buscar "punts especials", els voltants del quals tinguin un "comportament interessant, com ara un contrast de color alt. Normalment, són punts que es troben a la vora d'un objecte, com la vora dels fums marrons, que contrasten amb el cel de la foto del míssil. Aquests punts es poden detectar fent càlculs relativament fàcils sobre els números de color (per exemple, una gran diferència). L'espai de cerca per comparar grups de píxels amb una estructura similar es limita a les àrees del voltant d'aquests punts especials.

Detectar insercions i supressions

Tots coneixem exemples històrics famosos de manipulacions analògiques amb fotos en què s'eliminaven persones no desitjades. Aquests fotògrafs eren autèntics artistes, però avui dia no es requereix destresa per alterar les fotos digitals. Hi ha moltes eines que permeten esborrar o emmascarar objectes

no desitjats i pot ser fins i tot més fàcil inserir-ne de nous. Fa poc es va usar la IA, concretament l'aprenentatge profund, per intercanviar caps de persones que apareixen parlant en vídeos amb una sincronització de llavis gairebé perfecta. No obstant això, amb la inspecció visual sovint podem detectar si hi ha ombres o problemes que no coincideixen amb la geometria (per exemple, punts de fuga diferents) o si simplement el contingut no té sentit. Malauradament, és bastant difícil automatitzar aquest procés amb un ordinador, ja que realment no pot "veure" el que es descriu.

No obstant això, sovint es poden recuperar proves digitals d'aquest tipus de manipulacions explotant el format d'arxiu. El material visual distribuït a Internet està gairebé sempre subjecte a compressió. Això redueix la quantitat de dades que l'arxiu ocupa originalment per enviar imatges més ràpidament a través d'Internet o per reduir l'espai d'emmagatzematge. Un algoritme de compressió busca informació "innecessària" en una imatge. Elimina petits detalls invisibles a simple vista i ho combina amb un emmagatzematge eficient de la informació restant.



Resultat del procés de detecció en La lletera modificada

Potser el millor format de compressió és el format JPEG original. L'algorisme divideix primer una imatge en petits blocs de 8 x 8 píxels i després s'hi "aproxima" a través d'una combinació ponderada d'una sèrie de blocs bàsics. Cada un d'aquests blocs representa un patró rítmic determinat (per exemple, franges horitzontals, verticals i diagonals). Finalment, s'arrodoneixen els números d'aquesta combinació, un procés anomenat quantificació. Com més gran sigui l'arrodoniment, major serà la compressió, però pitjor serà la qualitat. Per tant, emmagatzemar la mateixa foto en el mode de compressió JPEG moltes vegades (el que coneixem com a codificació multigeneracional) en reduirà la qualitat. És aquest efecte el que pot proporcionar-nos proves digitals per a les insercions i supressions. Inspeccionar l'histograma dels valors arrodonits d'una imatge JPEG pot revelar parts de la imatge amb "comportaments" de compressió diferents.

Verificar la integritat/autenticitat

Ens podem preguntar si hi ha realment alguna manera de verificar la integritat d'una imatge. Com que una imatge es torna a desar sovint en un format de fitxer diferent, és convenient disposar d'una tecnologia que sigui independent del format. Les marques d'aigua digitals impliquen un tipus de tècniques que incrusten dades en una imatge i hi fan petites alteracions, imperceptibles en els valors del color, moltes vegades només en certs llocs i amb dependència d'una clau secreta (que fa que formi part de la criptografia, l'art de la comunicació secreta). D'aquesta manera, podem ocultar un missatge (secret) dins la imatge mateixa.

Marques d'aigua fràgils i sòlides

L'exemple més senzill de marca d'aigua canvia la paritat d'alguns números de color. Imagineu alteracions en la taula de colors de *La lletera* que convertissin els números parells en imparells i a l'inrevés i donessin lloc a alteracions del color lleugeres i invisibles. Les posicions en què ocorren els canvis depenen, en aquest cas, del missatge que vulguem incrustar-hi. Per llegir el missatge, l'ordinador comprova per a cada número de la taula si és parell o imparell (prenent la resta de la divisió per 2) i quan és parell mostra un píxel negre i quan és imparell, un de blanc. D'aquesta manera podem amagar de manera invisible un missatge blanc i negre dins d'una altra imatge.

Canviar la paritat es redueix a alterar l'últim bit de la representació de 8 bits del número. Per això aquesta tècnica es coneix com a modificació del bit de menys pes. En realitat podem fer servir més bits per incrustar missatges més complexos, però això repercutirà en la perceptibilitat. En qualsevol cas, aquesta tècnica es pot fer servir per incrustar-hi una marca d'autenticitat. Quan es manipuli la imatge, la marca es veurà danyada o fins i tot es perdrà. Per això la tècnica és una *marca d'aigua fràgil*.

El problema amb aquest tipus de marques d'aigua és que els canvis de format probablement arruïnaran també la marca. Quan un canvi de format no es consideri un canvi en la integritat, s'hauran d'emprar altres tècniques de marcat d'aigua que siguin sòlides per als canvis de format i, concretament, una compressió lleugera. No obstant això, això implica sovint que les petites alteracions de la imatge passin també desapercebudes. La *marca d'aigua sòlida* més versàtil

d'aquesta categoria és la tècnica de modulació de l'índex de quantificació, que permet equilibrar les propietats requerides.

Resum perceptiu

En aquest context, com hem explicat anteriorment, també requerim una eina per cercar imatges similars, un cop més, independentment del format d'arxiu. Igual que ocorria amb la detecció de la clonació, és evident que és massa tediós comparar tots els valors de píxel de totes les imatges possibles. Seria més fàcil si poguéssim reduir tota la informació de la imatge a algun tipus de resum numèric de la informació visual. Aquesta tècnica s'anomena resum perceptiu (o marcatge). Aquest principi es fa servir també per buscar àudios i constitueix la base de Shazam i altres.

En una imatge, igual que abans, l'ordinador pot buscar "punts especials" o altres tipus de característiques visuals fent algun tipus d'abstracció de la imatge, i després aplicar-hi un algoritme que redueixi la quantitat d'informació a un codi de longitud fixa amb el requisit que les variacions lleugeres del contingut de la imatge es correspongui amb variació lleugera del codi (a diferència dels resums criptogràfics). Llavors aquest codi pot comparar-se fàcilment amb una base de dades de codis existents computats a partir d'imatges que ja coneix.

La tècnica del resum perceptiu també es pot combinar amb el marcatge d'aigua per comprovar la integritat: podem incrustar el resum perceptiu de la imatge original com una marca d'aigua sòlida. El receptor pot llavors calcular el resum perceptiu i comparar-lo amb la marca extreta. La dificultat d'aquesta combinació resideix en el fet que la incrustació de la marca d'aigua no ha d'alterar el resum.

Actualment, però, l'obstacle més important a l'hora d'emprar aquestes tècniques rau en la manca de normalització.

Esforços de normalització

El comitè JPEG

JPEG és l'acrònim de *Joint Photographic Experts Group* (Grup Conjunt d'Experts en Fotografia). La majoria de la gent coneix el JPEG pel format JPEG original (ITU-T T.81|ISO/IEC 10918-1), també conegut com a JPEG -1. Aquest format va aparèixer el 1992 després d'un procés de desenvolupament iniciat el 1986. Avui, 25 anys després, segueix sent el format d'imatge més dominant i, en conseqüència, un dels estàndards multimèdia més reeixits mai definits.

És menys sabut que el comitè JPEG que hi ha darrera d'aquest estàndard popular segueix sent molt actiu avui en dia i ha implantat altres estàndards reeixits, com el JPEG 2000 (ITU-T T.800ISO/IEC 15444-1), que s'ha adoptat en diversos mercats com el del diagnòstic per la imatge, el cinema digital, els sistemes d'informació geogràfica i el sector artístic.

JPEG és oficialment un grup de treball del Subcomitè (SC) 29 del Comitè Tècnic Conjunt (JTC) 1. El JTC 1 reuneix experts d'ISO i IEC per actuar com un únic organisme de normalització. Per tant, JPEG és, en la pràctica, una abreviatura per a ISO/IEC JTC 1/SC 29/WG 1. Per complicar encara més les coses, JPEG és també un comitè conjunt del JTC 1 i del Grup d'Estudi de la ITU-T 16 (SG 16) de la ITU. Per tant, molts (però no tots) dels estàndards JPEG tenen una doble designació, una de l'ISO/IEC i una altra de la ITU-T.

Atès que cada aplicació té els seus propis requisits específics, hi ha disponibles diversos formats d'arxius d'imatges que es poden triar en funció de les necessitats particulars. Actualment s'estan duent a terme diverses iniciatives de normalització com el JPEG XS, el JPEG Full i el JPEG XL. Podeu obtenir més informació al respecte a jpeg.org.

Arquitectura de JPEG Systems

Tot i que cada format té el seu propi propòsit, tots aquests formats tenen unes característiques comunes. És per això que el JPEG va iniciar l'activitat de JPEG Systems (ISO/IEC 19566) amb l'objectiu principal d'alinear les característiques de sistema dels estàndards JPEG.

El format original d'arxiu JPEG va definir els «segments de marcadors APP» que permeten inserir blocs d'informació dins d'una imatge JPEG sense cap impacte en el procés de descodificació. Això permet a tercers implementar noves característiques o incrustar informació addicional en les imatges. Un exemple típic és l'ús del segment APP3 per incrustar metadades EXIF.

El JPEG 2000, d'altra banda, fa servir un format de caixa més modern. Bàsicament, el format de caixa és una estructura flexible que permet organitzar informació addicional o característiques encapsulades en una estructura jeràrquica binària. El format de caixa es fa servir també en altres formats com JPEG XR (ISO/IEC 15444-2:2004/AMD3:2015) i MPEG-4 (ISO/IEC 14496-12).

Aquesta diversitat de formats va dificultar la definició de noves característiques que es poguessin fer servir sistemàticament independentment del format d'arxiu. Per això JPEG va començar a treballar en una arquitectura JPEG Systems. L'objectiu de l'arquitectura JPEG Systems és permetre la definició de noves funcionalitats que es puguin adoptar amb qualsevol format d'arxiu JPEG. En aquest sentit, el primer pas va

ser alinear el segment de marcadors APP i el enfocaments basat en caixes proporcionant un mecanisme per incorporar les caixes en els segments de marcadors APP. Les noves característiques poden centrar-se en la definició de les caixes i una arquitectura d'abstracció addicional especifica com incrustar-les en el format d'arxiu específic. Aquest mecanisme per incrustar caixes en arxius JPEG-1 es defineix en el JPEG XT. Concretament, per a aquesta extensió es fa servir el segment de marcadors APP 11.

Antigament es feien servir diversos mètodes per incrustar metadades en imatges JPEG. Lamentablement, no tots estaven normalitzats, i això creava un escenari fragmentat que podia portar a incoherències o pèrdua de metadades quan es transferien imatges d'una aplicació a una altra.

Tot i que JPSearch va introduir una manera uniforme d'incorporar tot tipus de metadades, també té algunes restriccions addicionals. Per exemple, és precís que una imatge incrusti almenys un esquema de metadades de JPSearch. A més, JPSearch es va definir anys abans que JPEG Systems i JPEG XT i fa servir segments marcadors APP 3 amb un format personalitzat per incrustar metadades. Per això el JPEG va decidir definir el JPEG Universal Metadata Box Format (JUMBF). El JUMBF permet incorporar tot tipus de metadades en tots els formats d'arxius JPEG basats en caixes, així com el format JPEG original, fent servir l'enfocament JPEG XT abans esmentat.

Moltes característiques d'imatge noves (per exemple, 360) es basen principalment en metadades i combinen sovint metadades i dades d'imatge associades. Per tant, a més d'una sintaxi d'incrustació, el JUMBF proporciona un mecanisme de referència a les metadades a través de les URL. Això permet fer referències de metadades textuals (com XML) a metadades d'imatges associades.

JPEG Universal Metadata Box Format (JUMBF)

JUMBF defineix una caixa genèrica que pot encapsular qualsevol tipus de metadata (textual o binària) i proporciona un mecanisme de referència a través d'un esquema URL.

La caixa JUMBF és una supercapsa, és a dir, una capsa que només pot contenir altres capses. Cada capsa JUMBF ha d'incorporar una capsa de Descripció JUMBF (JUMBD). La capsa de Descripció proporciona informació addicional sobre el tipus de metadades que hi ha incrustades, pot associar una etiqueta de referència a les metadades i indica si les característiques específiques, com les referències, estan habilitades.

Per indicar el tipus de metadades incrustades, la descripció JUMBF conté un camp "Tipus", que és un ID únic universal (UUID). El Tipus determina quines altres capses es permeten després de la caixa JUMBD dins de la capsa matriu JUMBF.

L'especificació JUMBF defineix Tipus de metadades comunes com XML, JSON, caixes UUID i fluxos de codis d'imatge. El altres estàndards o les aplicacions de tercers poden definir els seus propis tipus per a casos d'ús específics. Per exemple, el JPEG 360 (ISO/IEC 19566-6) defineix un Tipus 360 per incrustar 360 metadades i dades d'imatge associades. Aquest mateix enfocament el segueix JPEG Privacy and Security.

És bastant comú que les noves extensions es basin en una combinació de metadades textuals i dades binàries d'imatges. En aquests casos, hi ha la necessitat d'una manera de fer referència a les dades binàries d'imatge des de les metadades textuals. Per tant, JUMBF permet associar una etiqueta de text al seu contingut. JUMBF defineix un esquema URL que es pot fer servir per fer referències des de dins de la imatge, fer una referència externa o fer la sol·licitud directament a les metadades incrustades més que a la imatge encapsulada. Com a alternativa a les etiquetes textuals, JUMBF admet també identificadors binaris com una alternativa més eficient als formats binaris que requereixen referències.

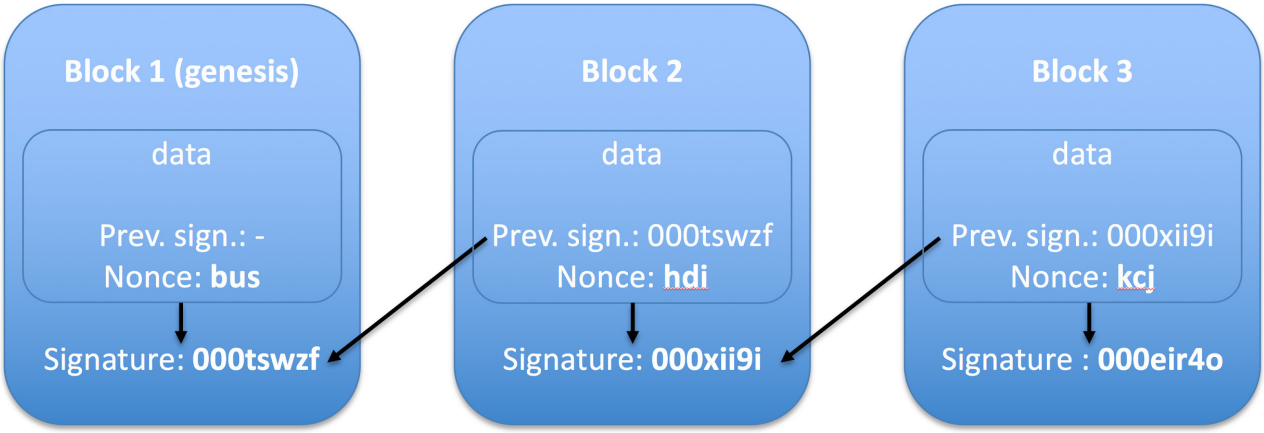
JPEG Privacy and Security

Partint de la base de l'arquitectura JUMBF, JPEG Privacy and Security defineix eines per protegir imatges, comprovar-ne la integritat i incrustar informació sobre els drets d'autor. En la pràctica, cada cas d'ús necessita unes eines específiques de protecció. Per exemple, en alguns casos podrien ser més adequades les marques d'aigua invisibles o el marcatge que l'encriptació tradicional. No obstant això, és important assenyalar que el JPEG no té la intenció de normalitzar cap de les tecnologies subjacents, sinó que pretén formalitzar la manera en què aquestes són senyalitzades i aplicades a les imatges JPEG. Per tant, els usuaris tindran la flexibilitat per triar i adoptar les eines més adequades per als seus casos concrets. A l'hora de definir la sintaxi de senyalització, s'oferirà retrocompatibilitat amb els fluxos de codis JPEG i JPEG 2000, així com amb altres estàndards i marcs existents (per exemple, els de SC 27, SC 29 i W3C).

Entre les funcionalitats de protecció hi ha:

– eines de protecció per protegir independentment parts de qualsevol tipus d'imatges JPEG i/o metadades associades i assegurar al mateix temps la compatibilitat amb les versions anteriors i posteriors de les tecnologies de codificació JPEG;

– control dels nivells jeràrquics d'accés i dels múltiples nivells de protecció per a metadades i protecció d'imatges;



Exemple il·lustratiu d'una cadena de blocs. Cada bloc conté la signatura del bloc anterior i un valor aleatori. En aquest cas, els valors aleatoris se seleccionen de manera que la signatura del bloc comença amb tres zeros.

– sistemes de *carving* (reconstrucció) d'arxius (per exemple, punts de resincronització).

Quant a les funcionalitats d'autenticitat, permet:

– comprovar la integritat de les dades d'imatge i/o les metadades incrustades;

– evitar l'eliminació de metadades, especialment la informació sobre els drets d'autor;

– versionar i/o registrar els canvis d'una imatge i/o de les metadades associades i solucions per mantenir la incorporació de procedència de la incrustació;

– incrustar informació traçable per permetre la identificació i avaluació de la imatge matriu i identificar les versions derivades o modificades de la imatge matriu.

JPEG Privacy and Security té com a objectiu oferir funcionalitats orientades a la integritat de les imatges. Normalment, perquè sigui fiable, s'haurà de dependre d'un tercer organisme de registre o d'una combinació amb una tècnica invasiva com el marcatge invisible. No obstant això, la cadena de blocs és una tecnologia prometedora que podria oferir una solució alternativa que no depengués d'un tercer o de tècniques invasives.

Registres distribuïts i cadena de blocs

La tecnologia de la cadena de blocs va aparèixer per primera vegada en un informe titulat "Bitcoin: A Peer-to-Peer Electronic Cash System" sota l'autoria de Satoshi Nakamoto. El nom de Satoshi Nakamoto és un acrònim i mai s'ha revelat la persona real que hi ha al darrere. Aquesta tecnologia és coneguda principalment pel seus ús de criptomonedes com Bitcoin, tot i que es fa servir per a una gran varietat d'aplicacions. Entre els exemples hi ha el registre de propietat intel·lectual i obres creatives, el registre de diamants i obres d'art, contractes intel·ligents, aplicacions multimèdia.

El nucli d'una aplicació de cadena de blocs és un registre distribuït. És a dir, un registre que no s'emmagatzema en un servidor centralitzat sinó que es comparteix entre una xarxa d'ordinadors. Tots els membres de la xarxa tenen una còpia del registre i les còpies s'actualitzen simultàniament (d'igual a igual). A més, la cadena de blocs està dissenyada de manera que la xarxa d'ordinadors accepta l'estat real del registre i que és immutable. Els registres poden contenir tot tipus de dades. En el cas de Bitcoin, el registre consisteix en un llistat d'operacions amb el remitent, el receptor i la quantitat.

Les cadenes de blocs ofereixen una font fiable d'informació sense la necessitat d'un organisme central. L'absència d'un organisme central comporta uns avantatges obvis enormes, però aquesta tecnologia té també certs inconvenients. Per entendre'ls millor, cal explicar breument amb una mica més detall com funcionen les cadenes de blocs.

El bloc fonamental de la cadena de bloc és un bloc binari de dades que conté tot tipus de dades així com una signatura digital del seu contingut. La signatura digital és una seqüència única de bits que es calcula a partir del contingut. Si un bit del contingut canvia, la signatura resultant serà totalment diferent. En el cas de la cadena de blocs, el contingut és un llistat d'operacions entre remitents i receptors. El registre és una seqüència (cadena) consecutiva de blocs en què els blocs nous s'afegeixen contínuament al final.

Per fer immutable la cadena i el contingut corresponent, la signatura del bloc anterior s'afegeix sempre al contingut del bloc següent. Per tant, si el contingut d'un bloc canviés, s'hauria d'actualitzar també tota la cadena de blocs consecutius. En cas contrari, la cadena seria invalidada. El primer bloc de la cadena no té cap referència prèvia i, per tant, s'anomena «gènesi».

Per descomptat, un delinqüent podria tractar d'actualitzar totes les signatures i referències de la cadena. Per això, les cadenes de blocs solen fer servir un principi anomenat «prova de treball». Això vol dir que per crear un bloc nou, s'ha de fer una certa quantitat de treball (computacional). Amb aquesta finalitat, s'afegeix un valor aleatori al contingut de cada bloc. El valor aleatori no és més que una seqüència aleatòria de bits, però s'ha de seleccionar de manera que la signatura resultant del contingut i el valor aleatori compleixin combinats unes condicions determinades. Per exemple, una condició pot ser que la signatura comenci amb un determinat nombre de zeros per ser acceptada. L'única manera d'aconseguir-ho és anar provant els valors seleccionats a l'atzar fins trobar-ne un que compleixi aquesta condició. Per tant, el temps de computació necessari es pot calcular estadísticament. El desafiament pot augmentar en complexitat per compensar l'augment del poder computacional. El procés de trobar valors aleatoris i validar un bloc és una competència anomenada mineria. Normalment, els miners són recompensats a manera d'incentiu. En el cas dels miners de Bitcoin, es recompensen amb Bitcoins noves, d'aquí el nom mineria.

Si un delinqüent vol fer una modificació del registre, haurà de tornar a fer els càlculs per a tots els blocs consecutius. Com que la comunitat està treballant al mateix temps en blocs nous, necessitaria més del 50 % del poder computacional que en tota la xarxa, quelcom que es considera estadísticament impossible. Per exemple, en el cas de Bitcoin, la capacitat combinada del servidor de la xarxa Bitcoin és major que l'equivalent a 100 vegades la capacitat del servidor de Google[9].

Gràcies a la naturalesa de distribució comunitària i a la immutabilitat estadísticament comprovada, la cadena de blocs és una tecnologia molt valuosa. Evita la necessitat de recórrer a organismes de confiança i es pot adoptar en molts àmbits. No obstant això, també hi ha desavantatges importants.

La mineria requereix enormes quantitats de poder de computació (i energia) i té un impacte ambiental considerable. S'estima que el consum d'energia de Bitcoin durant l'escriptura és de 73 TWh/any [10]. Equival gairebé al consum anual total d'energia d'Àustria (72 TWh/any). Hi ha moltes recerques actives que intenten proposar alternatives com la «prova de participació». No obstant això, a hores d'ara, no hi ha cap alternativa demostrada a la prova de treball que no depengui d'un tercer o que tingui altres vulnerabilitats. A més, la càrrega de treball requerida dóna lloc a un retard considerable entre la sol·licitud d'una operació i el seu registre.

9. https://www.ccn.com/bitcoin-100-times-powerful-google/
10. https://digiconomist.net/bitcoin-energy-consumption

En el context de les imatges, les cadenes de blocs es poden fer servir per registrar imatges completes, empremtes d'imatges o informació de drets d'autor sense dependre d'un tercer organisme de registre o de tècniques de marcatge invasiu. Els sistemes basats en cadenes de blocs han estat proposats també com a mètode per retribuir els fotògrafs (per exemple, KodakCoin)[11]). No obstant això, tenint en compte l'enorme quantitat d'imatges que es produeixen diàriament, hem de tenir en compte els requeriments energètics i l'impacte ambiental que se'n deriven. Un altre desafiament és trobar un incentiu adequat perquè els miners facin sostenible aquest model. Tot i que s'han adoptat cadenes de blocs privades per a casos d'ús similars, aquestes cadenes privades depenen d'un tercer i, per tant, atenuen un dels principals avantatges. Finalment, és important ser conscients dels enormes riscos de privacitat de registrar imatges senceres en una cadena de blocs. Com que les cadenes de blocs són distribuïdes i immutables per naturalesa, les lleis de privacitat, com ara el dret a ser oblidat, serien impossibles d'aplicar. Per descomptat, en comptes de registrar una imatge completa, se'n pot registrar una empremta. Però aquesta empremta hauria de ser prou sòlida com per permetre un registre fiable de la imatge autèntica. Ara bé, hi ha moltes investigacions centrades a proposar solucions a aquestes qüestions. Per tant, encara podria haver-hi un futur prometedor perquè les cadenes de blocs puguin resoldre el cas complex de la integritat de les imatges.

El comitè de normalització del JPEG també ha reconegut el potencial de les cadenes de blocs en el context multimèdia i, per tant, està investigant les necessitats de normalització pel que fa a la tecnologia de les cadenes de blocs dins de JPEG, tal com indica un informe publicat recentment[12].

Conclusions

En relació amb la integrat de les imatges en el context dels arxius digital, hem identificats les qüestions següents que requereixen una atenció especial. El problema principal té a veure amb la missió arxivística per salvaguardar un objecte dipositat o un document intacte i inalterat. Aquesta missió es veu afectada per l'esforç que suposa la digitalització. A més del fet que la digitalització mateixa requereix obtenir una còpia amb una fidelitat i una precisió suficients,

11. https://www.kodak.com/US/en/kodakone/default.htm
12. ISO/IEC JT1/SC29/WG1 N80019 - Towards a Standardized Framework for Media Blockchain (https://jpeg.org/items/20180721_blockchain_whitepaper.html)

les còpies d'un original digital també requereixen una atenció en aquest aspecte. Hem constatat les possibles variacions que es poden produir entre còpies digitals degudes a errors de còpia i a manipulacions d'arxius i l'impacte del reprocessament dels arxius mentre transiten aplicacions. A més de les propietats d'imatge mateixes, també corren perill de ser alterades o esborrades les metadades incrustades, de vegades a causa de les imperioses preocupacions en matèria de privacitat. També hem ressaltat que més enllà d'aquestes metadades incrustades, també hi ha el vincle entre l'arxiu digital i les metadades contextuals, que sovint s'emmagatzemen en sistemes d'informació. La possible pèrdua del context fa necessària la possibilitat de reconstruir els orígens d'un arxiu d'imatge i les seves dependències vers altres còpies digitals.

Hem parlat de diverses tècniques matemàtiques que poden ajudar a identificar els canvis realitzats en el contingut d'una imatge o incrustar informació traçable aplicant marques d'aigua invisibles. A més de les solucions matemàtiques, és essencial obtenir la interoperabilitat mitjançant la normalització. JPEG Privacy and Security proporcionarà una sèrie d'eines per protegir el contingut i les metadades de les imatges, així com per comprovar-ne l'autenticitat, la procedència i la integritat. Concretament, pel que fa a la comprovació de la integritat de les imatges, la cadena de blocs és una tecnologia prometedora que pot eludir la necessitat d'un tercer organisme de registre o de tècniques invasives. No obstant això, l'aplicació d'aquesta tecnologia en un context multimèdia comporta una sèrie de reptes que cal afrontar. És per això que JPEG ha iniciat també una recerca sobre les necessitats de normalització relatives a les cadenes de blocs.

El text en anglès d'aquesta ponència es pot consultar a:
http://www.girona.cat/sgdap/cat/jornades_actes.php