



CScorza

LA DIGITAL IMAGE FORENSICS NELL'OSINT

L'uso della Digital Image Forensics per le attività di OPEN SOURCE INTELLIGENCE



OsintItalia

ASSOCIAZIONE di PROMOZIONE SOCIALE

Crediti

LA DIGITAL IMAGE FORENSICS NELL'OSINT

L'uso della Digital Image Forensics per le attività di OPEN SOURCE INTELLIGENCE

Testo scritto e prodotto da **CScorza**

Anno di pubblicazione 2023

Contatti

Linkedin - <https://www.linkedin.com/in/cscorza/>

Telegram – https://t.me/+kP_uYlc6-345Njc8

🕵️ CScorza - Indagini Telematiche "Canale Pubblico"

Github - <https://github.com/CScorza>

Gli articoli di questo libro sono ad accesso aperto e distribuiti sotto Creative Licenza Commons Attribution (CC BY), che consente agli utenti di scaricare, copiare e sviluppare articoli pubblicati, purché l'autore e l'editore siano adeguatamente accreditati, il che garantisce il massimo diffusione e un più ampio impatto delle nostre pubblicazioni



INDICE

Introduzione

- Cos'è la Digital Image Forensics
- Campi di sviluppo della Digital Image Forensics e dell'OSINT Image

PARTE 1

- Temi principali della Digital Image Forensics
 - Fotogrammetria e Misurazione degli Oggetti
 - Confronto Fotografico
- Punti di Repere
- Software per il confronto fotografico e il riconoscimento facciale
- Linux e il Riconoscimento Facciale
 - Analisi del Contenuto
- Analisi dei Metadati o EXIF
- Hash
- Tipi di formato delle immagini
- Tipici problemi di qualità delle immagini
- Tecniche per il Miglioramento delle Immagini

PARTE 2

- Strumenti di Ricerca delle Immagini
- OSINT IMAGE e il SOCIMT
 - Ricerca volti
 - Reverse image search
 - Geolocalizzazione delle immagini
- Banche dati per la ricerca di oggetti specifici
- Estensioni per il Browser nella ricerca delle Immagini
- App utili per l'Image Digital Forensics

PARTE 3

- Strumenti per l'analisi delle Immagini False
 - Error Level Analysis
 - L'uso dei canali colore (RGB) per l'estrapolazioni di dettagli
- L'uso dell'ombra per l'analisi delle immagini

PARTE 4

- Utilizzo forense dei programmi di grafica
 - Linea guida per l'uso di software grafici in modalità forense per non alterare l'integrità dell'immagine.
- Estrapolazione dei Video da Siti Web o da DVR

PARTE 5

- Steganografia
- Watermark
- L'AI la nuova frontiera delle immagini FAKE

TESTI UTILI E BIBBLIOGRAFIA

- Linee Guida utili e testi consigliati
- Bibbliografia

PREFAZIONE

La Digital Image Forensics è una disciplina in costante evoluzione e - in un'era in cui le immagini digitali sono sempre più parte integrante della nostra vita quotidiana - sta assumendo rilevanza in molteplici ambiti investigativi.

In questo senso, il compendio scritto da Emanuele Russo a supporto del Corso introduttivo sulla Digital Image Forensics, che lui stesso ha tenuto a favore dei soci di Osintitalia, rappresenta un eccellente base di partenza; per tutti coloro che vogliono avvicinarsi a questa interessantissima disciplina, ma anche per i più esperti che siamo sicuri potranno trarne utili spunti metodologici.

Emanuele rappresenta in pieno i valori di della nostra associazione. Una realtà che trae la sua forza proprio nei suoi associati.

Grazie quindi Emanuele e complimenti per l'encomiabile opera di divulgazione che stai portando avanti e che metti a disposizione della nostra grande comunità.

Osintitalia APS

OsintItalia¹

L'associazione OsintItalia nasce dall'incontro di un gruppo di giovani professionisti che operano, con competenze diversificate, nell'ambito dell'Open Source Intelligence, meglio conosciuto come OSINT, ossia analisi su fonti aperte, animati da un comune desiderio di utilizzare l'OSINT per aiutare le persone.

Da tale comune interesse è nata l'idea di creare un'associazione di promozione sociale che pone al centro il concetto di OSINT solidale.

In particolare, l'associazione collabora con le Istituzioni nell'ambito di attività che richiedano competenze tecniche in materia di OSINT. Tra gli ambiti in cui potrà essere utilizzata tale disciplina ricadono molte attività, tra cui:

- la ricerca di persone scomparse.
- il supporto contro il cyber bullismo.
- il supporto contro il Revenge Porn.
- il contrasto alla disinformazione digitale (es. fake news).
- il Fraud Investigation con il gruppo "Scam-Monitoring".
- promuovere a livello nazionale e internazionale iniziative di carattere formativo e divulgativo sull'utilizzo dell'OSINT.
- sostenere a livello nazionale e internazionale iniziative di sensibilizzazione volte a diffondere la cultura dell'OSINT sociale e solidale (c.d. "OSINT for good").



¹ Info e iscrizione OsintItalia.it

INTRODUZIONE

Il volume nasce come ausilio al corso di base di OSINTITALIA “Introduzione alla Digital Image Forensics”
Questo testo, non è un manuale della Digital Image Forensics, ma una raccolta di informazioni, tecniche e strumenti, che uniscono la Digital Image Forensics con l’OSINT Image.

Il suo scopo è quello di essere d’ausilio a qualunque “analista” (esperto e non), nella scoperta di nuove tecniche di analisi delle immagini al fine di ricavarne quante più informazioni utili ai fini della sua indagine.
Da qui le prime due domande:

Cos’è la Digital Image Forensics?

Si riferisce al processo di analisi e verifica dell’autenticità di immagini digitali.

Questo campo implica tecniche e strumenti per rilevare manipolazioni, falsificazioni o alterazioni in immagini digitali e per stabilire la fonte originale e la storia di un’immagine digitale.

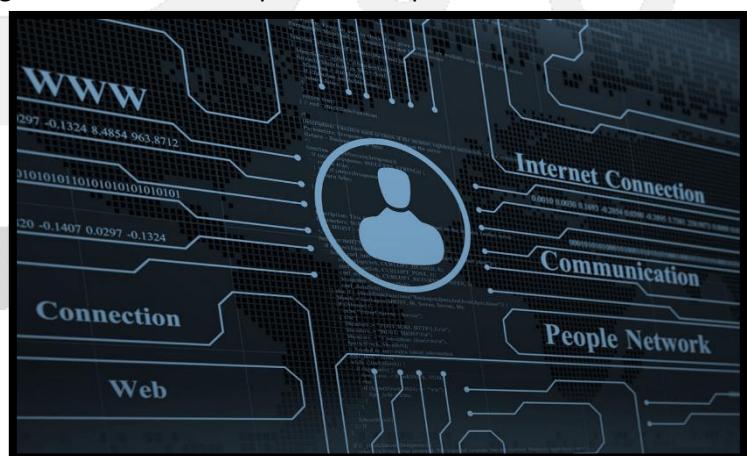
L’obiettivo della Digital Image Forensics, è fornire prove affidabili e robuste a fini legali, forensi e scientifici.

Le tecniche comunemente utilizzate includono l’analisi degli errori di immagine, il confronto di immagini, l’analisi delle caratteristiche e l’analisi dei metadati.



Cos’è l’Open Source Intelligence Image?

Si riferisce all’utilizzo di informazioni disponibili pubblicamente per raccogliere informazioni sulle immagini, ad esempio sulla loro origine, autenticità o storia. Questa tecnica viene utilizzata in molti campi, tra cui la criminologia, la difesa e la sicurezza, per raccogliere informazioni importanti che possono aiutare a prendere decisioni informate.



Iniziando da un’anteprima dell’Analisi visiva per poi passare sempre più nel dettaglio della Forensics e dell’OSINT, con software e tecniche varie, il lettore verrà accompagnato in un percorso guidato da esempi pratici e vere e proprie guide dei vari software, al capire fine di capire cosa si cela dietro una foto e quale delle decine di informazioni si possono ricavare. In oltre un capitolo viene dedicato a quelle che sono le linee guida, in uso e che sono fondamentali per non alterare l’immagine e quindi la sua autenticità

Buona Lettura

PARTE 1

TEMI PRINCIPALI DELL' IMAGE DIGITAL FORENSICS

L' Digital Image Forensics si può suddividere:

- Fotogrammetria e Misurazione delle Immagini
- Confronto fotografico
- Analisi del Contenuto
- Autenticazione dell'immagine

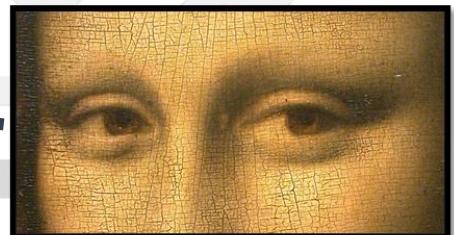
La Tecnica prima del Software

Uno degli aspetti principali della Digital Image Forensics e dell'OSINT Image è “*l'Analisi Visiva*”, cioè l'analisi che possiamo compiere usando il senso della vista.

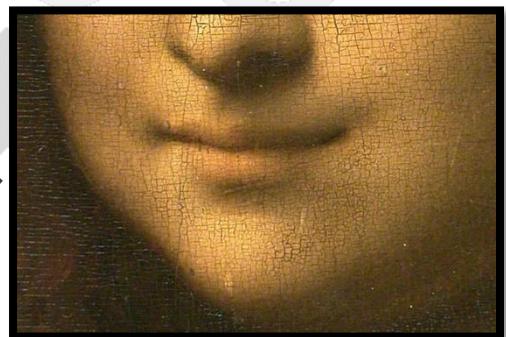


La Gioconda
Fonte: Wikipedia

Utilizzando l'Opera d'Arte della Gioconda possiamo apprezzare ancor di più questa tecnica, analizzando ogni dettaglio del quadro, utilizzando solo gli occhi dell'operatore.



Riflette la sua bellezza interiore e altri che la descrivono come una donna astuta e sottile.



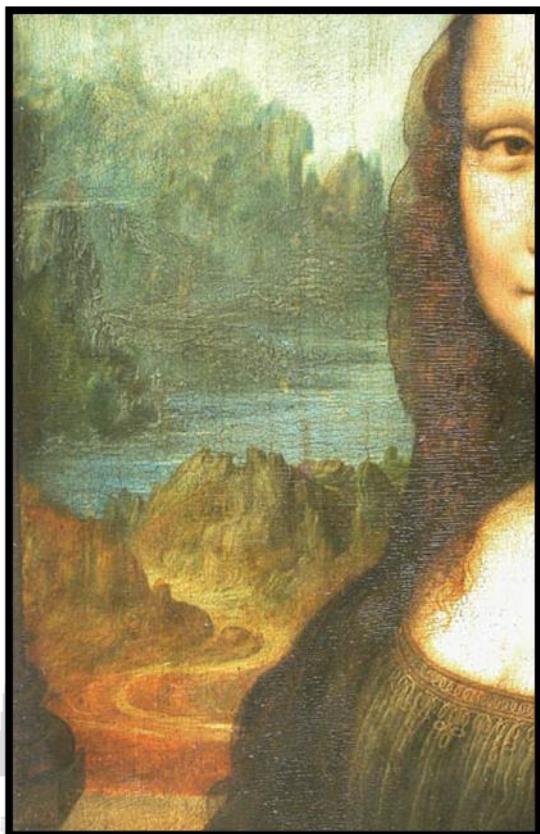
Alcune interpretazioni sostengono che la bocca rappresenta la sfumatura tra la dolcezza e la malizia.



Rappresentano la femminilità e la dolcezza della donna ritratta.

Nei gesti, nel volto e nell'abbigliamento possiamo notare, il periodo storico e stagionale, lo stato d'animo, l'età, la conformità del viso e delle mani, etc.

Dando uno sguardo allo sfondo del quadro, possiamo notare invece:



- A sinistra una serie di colline e montagne che si ergono all'orizzonte.

Le colline sono coperte di vegetazione e alberi, mentre le montagne sono coperte di neve. In primo piano, si vede un corso d'acqua che attraversa una zona pianeggiante coperta di vegetazione e alberi.

- A destra del quadro, il paesaggio mostra una serie di colline e montagne più lontane rispetto a quelle viste nella parte sinistra.

Anche in questo caso, le colline sono coperte di vegetazione e alberi, mentre le montagne sono coperte di neve. In primo piano, si vede un villaggio situato in cima ad una collina, con alcune case e una chiesa.



Comune di Bobbio, Provincia di Piacenza (Emilia Romagna), luogo dove si pensa che Leonardo da Vinci abbia preso ispirazione.

Foto:
Wikipedia



LA FOTOGRAMMETRIA E LA MISURAZIONE DEGLI OGGETTI

La fotogrammetria è una tecnologia che utilizza fotografie per creare modelli tridimensionali di oggetti o ambienti.

Questa tecnica si basa sulla misurazione della posizione e della forma degli oggetti sulle foto, utilizzando tecniche di elaborazione delle immagini attraverso software ed applicazioni.

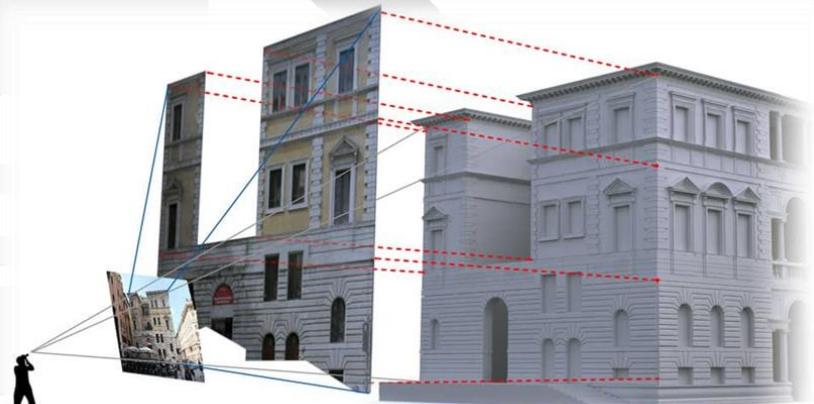
La fotogrammetria viene utilizzata in molti campi, tra cui la topografia, la geologia, l'architettura e la ricostruzione di incidenti.

La fotogrammetria consente di ottenere misurazioni precise e accurate di oggetti su foto, che possono essere utilizzate per creare modelli tridimensionali dettagliati, mappe digitali e analisi geospaziali.

La Fotogrammetria e l'OSINT Image

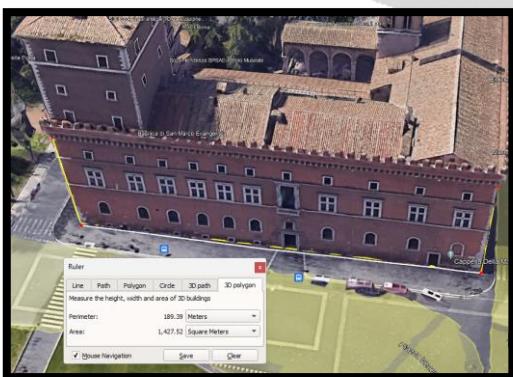
Sono due tecnologie complementari che possono essere utilizzate insieme per raccogliere e analizzare informazioni sulle immagini. La fotogrammetria consente di ottenere misurazioni precise e accurate di oggetti sulle foto, che possono essere utilizzate per creare modelli tridimensionali dettagliati, oppure fare confronti tra due target, etc.

Misurazione di un coltello attraverso degli oggetti che hanno delle misure standard note (Come righelli, Pacchetti di sigarette, penne etc)



*Da un Immagine all'elaborazione in 3D con le misure in proporzione di un palazzo
microgeo.it/fotogrammetria/*

Di seguito due strumenti (con le relative Istruzioni) per effettuare misure.



Google Earth

Google Earth (*Multipiattaforma*)

1. Apri **Google Earth Pro** e trova l'edificio che desideri misurare
2. Clicca sul pulsante "**Strumenti**" e seleziona "**Misura**"
3. Fai clic sulla posizione in cui vuoi iniziare la misura e trascina il mouse per disegnare una linea/poligono
4. Le misure ottenute, possono essere impostati secondo il sistema preferito.

ImageMeter Pro (Android)

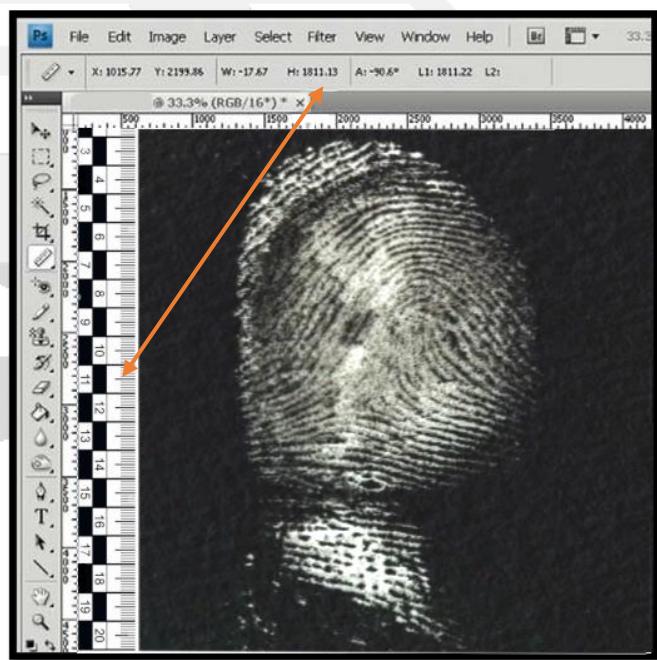
1. Apri l'app: Avvia l'app **ImageMeter Pro**² sul tuo dispositivo Android.
2. Seleziona la modalità di misura:
 - Tocca il pulsante "**Misura**" per accedere alla modalità di misura.
 - Seleziona "**Misura linea**" per misurare la lunghezza di un oggetto, "**Misura angolo**" per misurare l'angolo tra due linee o "**Misura area**" per misurare la superficie di un oggetto.
3. Scatta una foto o seleziona un'immagine:
 - Tocca il pulsante "**Scatta foto**" per scattare una foto dell'oggetto che desideri misurare, oppure tocca "**Selezione immagine**" per selezionare un'immagine dalla tua galleria.
4. Disegna la linea di misura:
 - Disegna una linea che segua l'oggetto che desideri misurare. La lunghezza della linea verrà visualizzata in tempo reale in alto sullo schermo.
5. Regola la precisione:
 - Tocca il pulsante "**Impostazioni**" per accedere alle impostazioni dell'app, quindi seleziona "**Unità di misura**" per regolare la precisione delle misure.
6. Salva e condividi la misura:
 - Tocca il pulsante "**Salva**" per salvare la misura, oppure tocca "**Condividi**" per condividere la misura con altre persone tramite e-mail, messaggi o altre app di condivisione.
7. Ripetere i passaggi da 3 a 6 per effettuare ulteriori misure.



Palazzo Venezia
Fonte: artribune.com

Ulteriori strumenti per effettuare strumenti sulle immagini:

- [Adobe Photoshop](#)
- [Gimp - GNU Image Manipulation Program](#)
- [ImageJ/Fiji – ImageJ Pro](#)



Photoshop Elements

² Approfondimento:

[ImageMeter PRO](#)

<https://github.com/CScorza/Image-OSINT-Forensics>

CONFRONTO FOTOGRAFICO

Il confronto fotografico è un processo che implica la comparazione di due o più immagini per determinare le differenze tra di esse.

Questo processo può essere utile in molte applicazioni, come la verifica dell'autenticità di un'immagine, il confronto tra due soggetti, ed altro.

Il confronto fotografico può essere effettuato:

- Manualmente
- E con software specializzati.

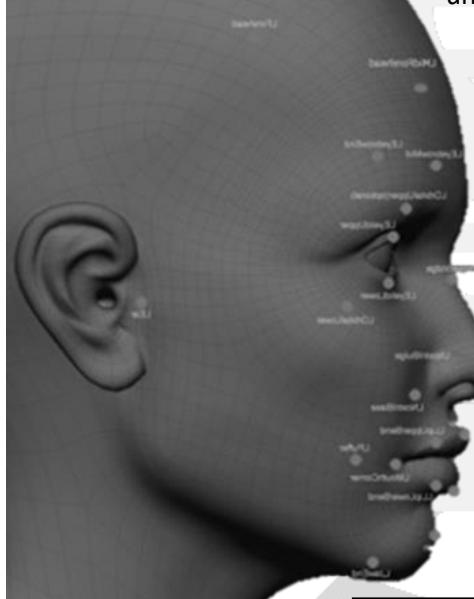


Fonte: mole24.it

IL RICONOSCIMENTO FACCIALE E L'ANALISI FISIONOMICA

Il Riconoscimento Facciale

È una tecnologia che consente di riconoscere i tratti distintivi di una persona a partire da un'immagine o da un video.



L'Analisi Fisionomica

E' l'insieme delle caratteristiche somatiche e facciali di un individuo, utilizzata per identificare o descrivere una persona.

L'analisi fisionomica è l'arte di interpretare queste caratteristiche per scopi di identificazione e/o descrizione.

Uno dei sistemi più usati per effettuare questa analisi, è il **"Sistema Bertillon"**, creato da un Criminologo Francese **Alphonse Bertillon**, nato a Parigi nel 1853 e fondatore nel 1870 del primo laboratorio di identificazione criminale ed inventore dell'antropometria giudiziaria, chiamata **"Bertillonage"** o **"Sistema Bertillon"**³, un sistema di riconoscimento biometrico adottato in tutta Europa e negli Stati Uniti.



Fonte: Wikipedia

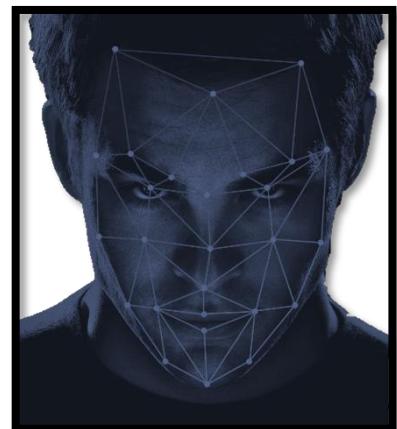


³ <https://gallica.bnf.fr/ark:/12148/bpt6k30435611>

IL RICONOSCIMENTO FACCIALE E L'INTELLIGENZA ARTIFICIALE

Il **Sistema Bertillon** utilizzava una serie di misurazioni fisiche precise, tra cui la lunghezza del braccio, la lunghezza del piede e la circonferenza della testa, per creare un "profilo fisico" unico di un individuo. Questo profilo poteva quindi essere utilizzato per identificare i criminali che erano già stati arrestati in precedenza. Le misurazioni che in questo libro vengono trattate, vengono dette "Punti di Repere sul volto". Utilizzati ancora oggi per il confronto fotografico tramite IA (intelligenza artificiale).

La maggior parte dei sistemi di riconoscimento, funzionano con codici numerici chiamati "*faceprints*". Tali sistemi identificano un determinato numero di punti chiave o "nodali" su un volto umano. In questo contesto, i punti chiave o nodali sono punti di riferimento utilizzati per misurare le variabili del volto di una persona, come la lunghezza o la larghezza del naso, la profondità degli occhi e la forma degli zigomi.



PUNTI DI REPERE SUL VOLTO "FACEPRINTS"

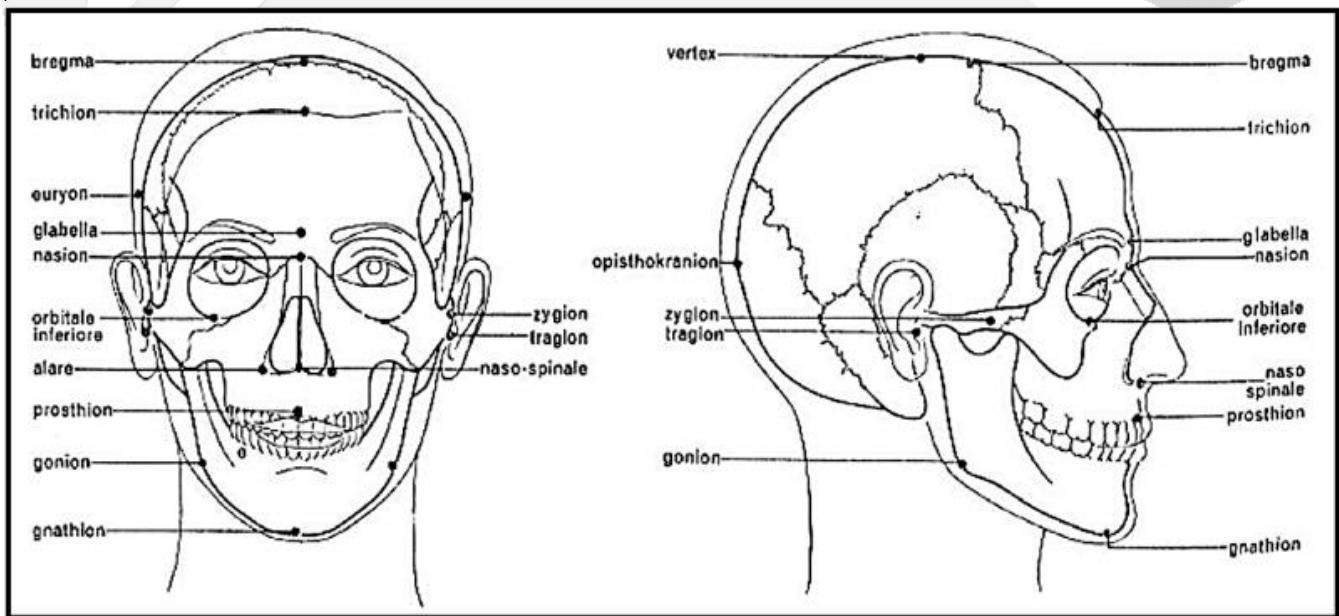
I punti di riferimento sul volto sono specifici tratti anatomici o caratteristiche sul viso che vengono utilizzati per identificare e confrontare le immagini di volti diversi.

Questi punti di riferimento detti "**Punti di Repere**" includono la posizione degli occhi, del naso, della bocca e delle orecchie, nonché la forma e la dimensione del mento e delle guance.

Questi punti di riferimento sul volto sono spesso utilizzati nel confronto fotografico per identificare la somiglianza tra due volti e per determinare se due immagini rappresentano la stessa persona.

Ad esempio, se stai confrontando due immagini di volti, potresti utilizzare la posizione degli occhi, del naso e della bocca come punti di riferimento per determinare se i volti sono simili o no.

⁴

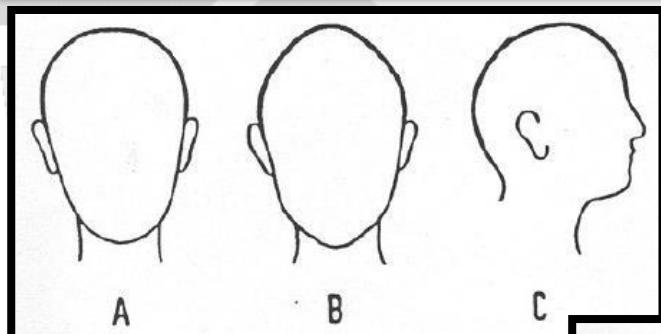
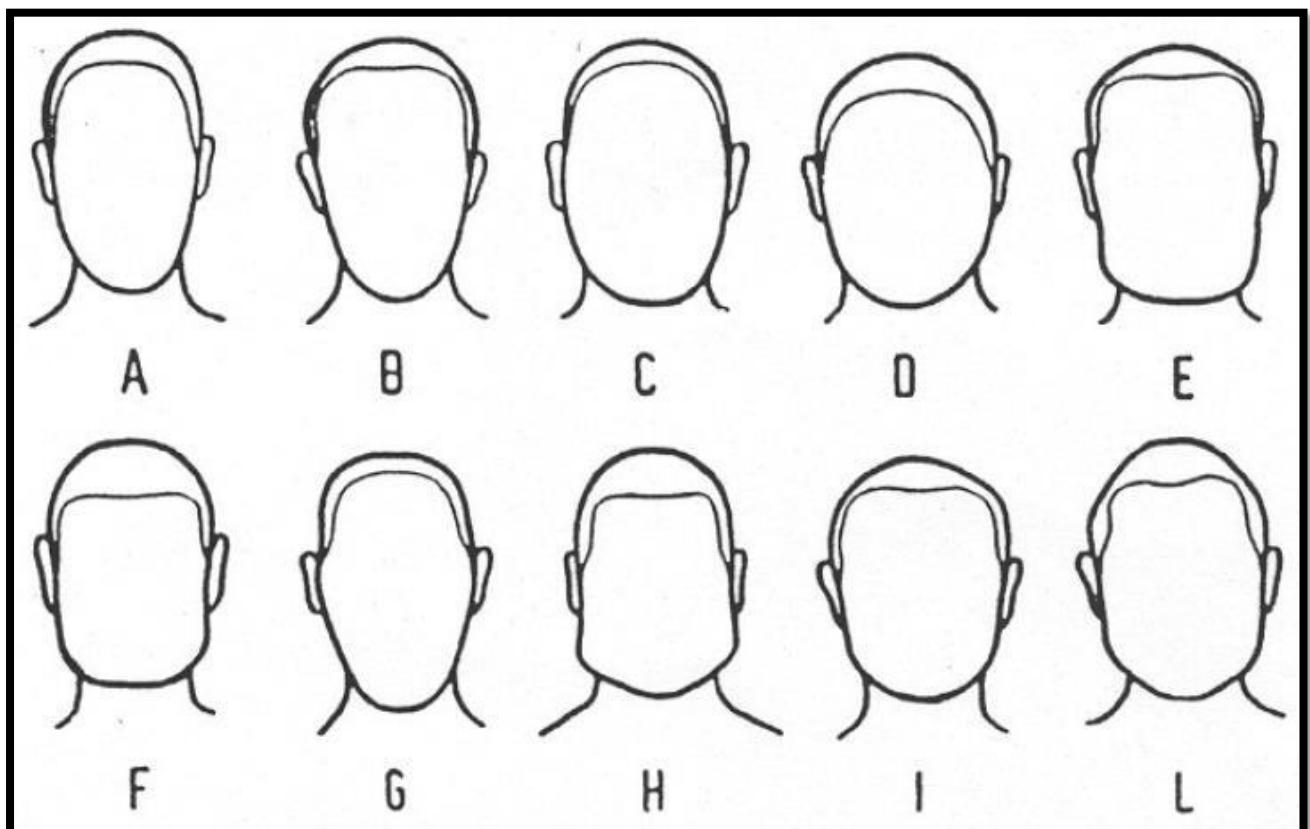


⁴ [https://bista.sites.dmi.unipg.it/didattica/sicurezza-pg/seminari2010-11/sic-immagini/Biometria%20applicata%20alla%20sicurezza%20\(in%20particolare%20biometria%20facciale\)%20-%20Corapi%20Gessica%20e%20Fusco%20Federica%20\(presenazione\).pdf](https://bista.sites.dmi.unipg.it/didattica/sicurezza-pg/seminari2010-11/sic-immagini/Biometria%20applicata%20alla%20sicurezza%20(in%20particolare%20biometria%20facciale)%20-%20Corapi%20Gessica%20e%20Fusco%20Federica%20(presenazione).pdf)

Approfondimento:

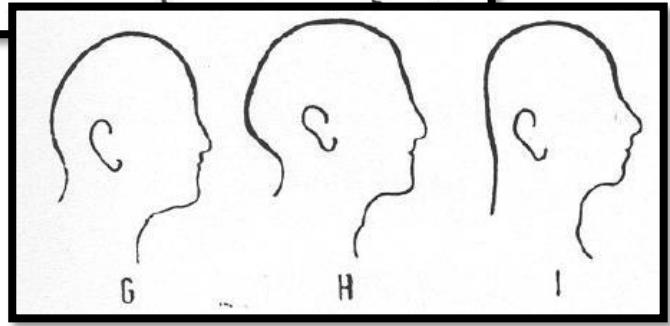
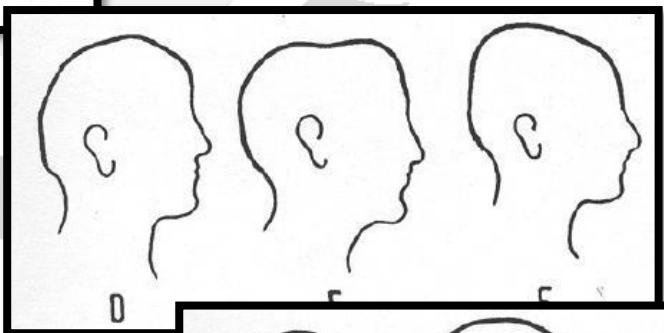
<https://www.ai4business.it/sicurezza/riconoscimento-facciale/>

I DIESCI TIPI MORFOLOGICI FACCIALI

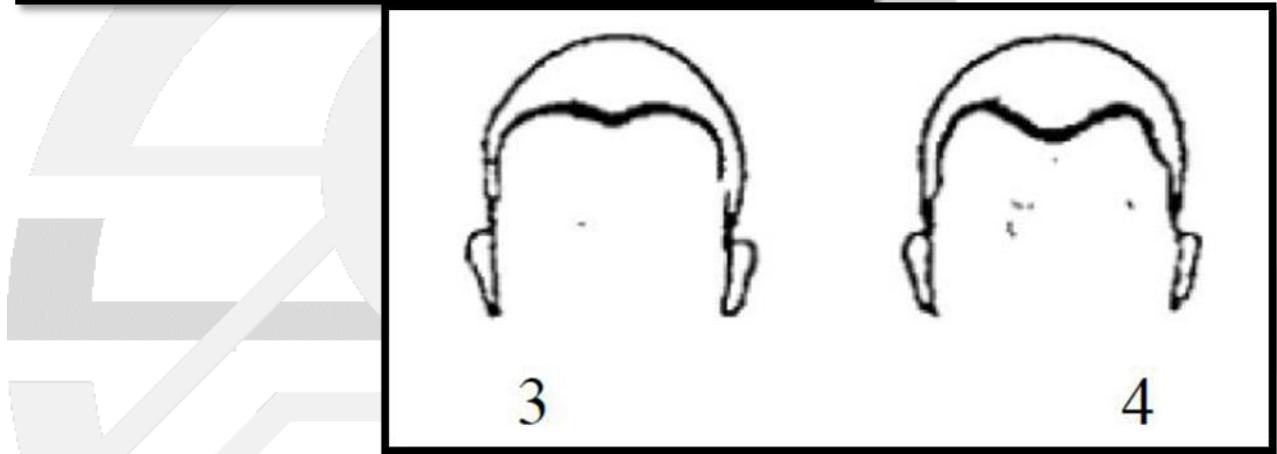
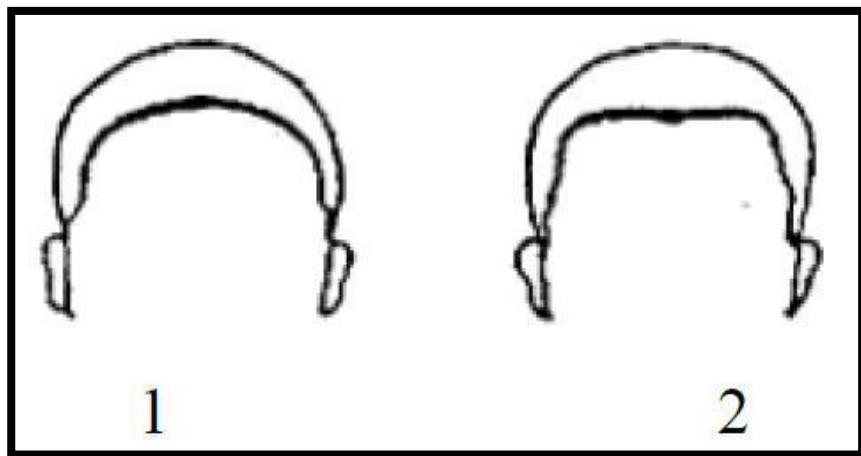


FORME DELLA TESTA

- A) testa di fronte curva;
- B) testa carenata;
- C) testa di profilo, curva;
- D) a linea spezzata;
- E) insellata;
- F) con vertice posteriore;
- G) con vertice anteriore;
- H) con occipite sporgente;
- I) ad occipite appiattito.



TIPI DI LINEA DI INTERSEZIONE DEI CAPELLI SULLA FRONTE



L'attaccatura dei capelli in riferimento al punto antropometrico **Trichion**.

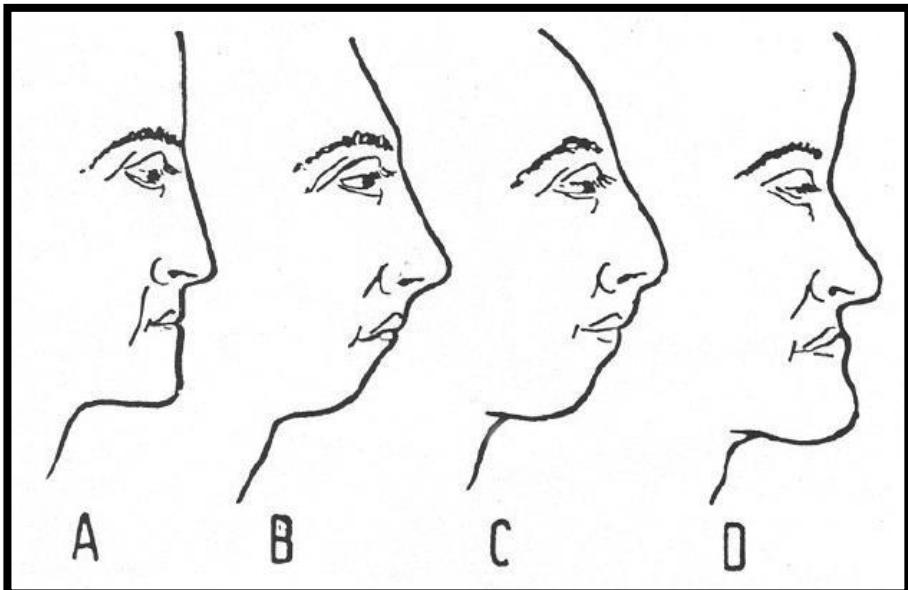
I soggetti privi di **Trichion** sono caratterizzati da:

- 1) attaccatura curvilinea;
- 2) attaccatura rettilinea.

Quelli con **Trichion** in:

- 3) stretto;
- 4) largo.

PROFILO GLOBALE DEL VOLTO

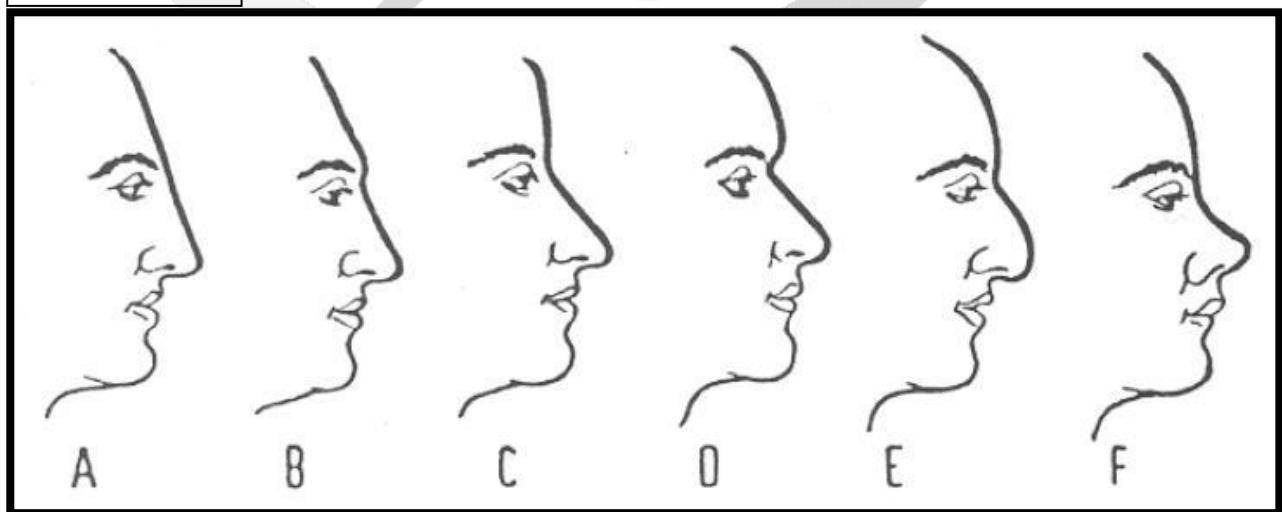


- A) faccia rettilinea;
- B) faccia piramidale;
- C) faccia semilunare;
- D) faccia rientrante.

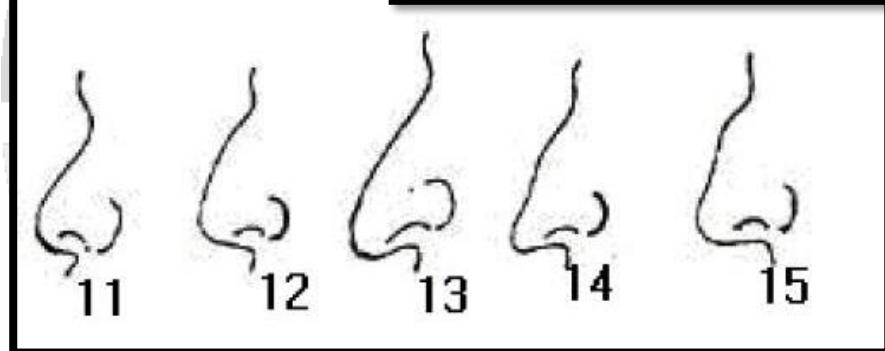
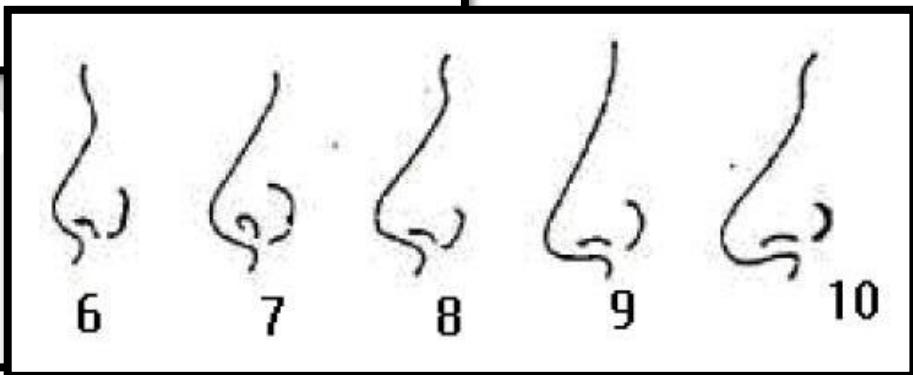
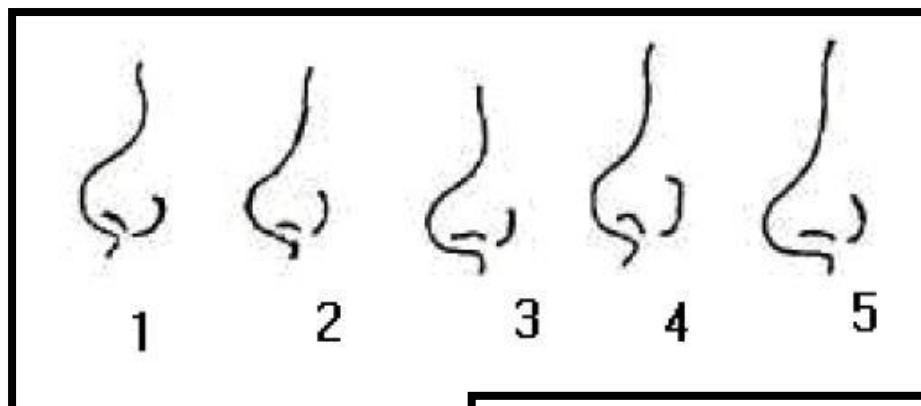
FORME DEL NASO

- A. Continuo
- B. Parallello
- C. Spezzato
- D. Angoloso
- E. Curvilineo
- F. Ondulato

PROFILO FRONTE/NASALE

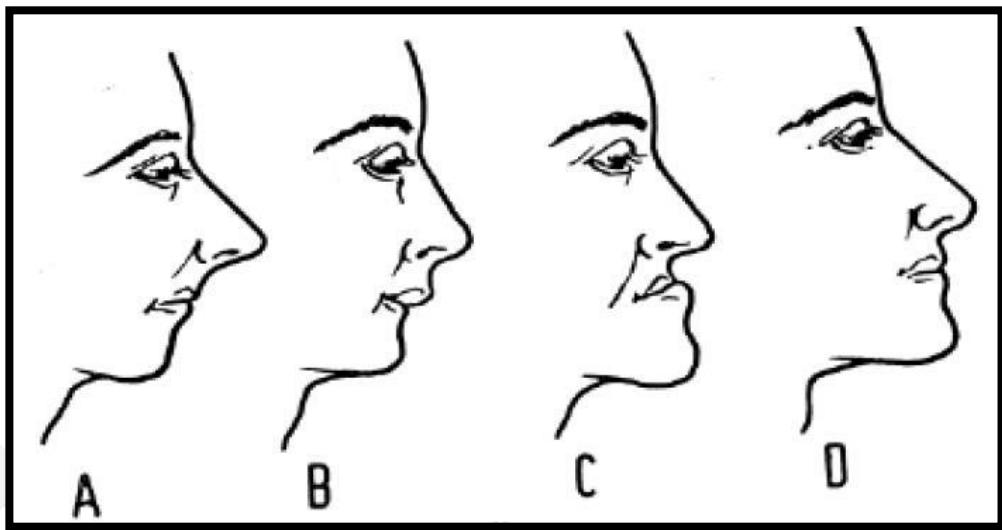


FORME DEL NASO

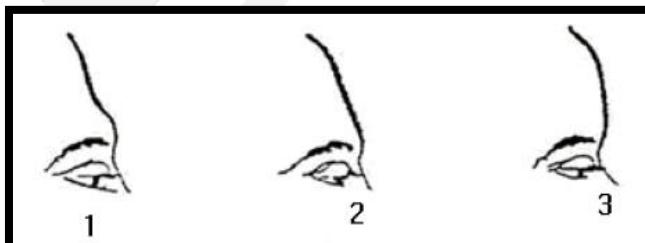


tipo	dorso	radice	punta	base
1	corto	infossata	verso l'alto	in avanti
2	corto	poco alta	verso l'alto	obliqua
3	corto	poco alta	verso avanti	orizzontale
4	media lunghezza	poco alta	verso avanti	in avanti
5	media lunghezza	alta	verso avanti	orizzontale
6	corto	infossata	verso l'alto	in avanti
7	media lunghezza	alta	verso l'alto	in avanti
8	media lunghezza	poco alta	verso avanti	poco in avanti
9	lungo	poco alta	verso avanti	orizzontale
10	lungo	poco alta	verso il basso	indietro
11	corto	infossata	verso l'alto	in avanti
12	media lunghezza	poco alta	verso avanti	poco in avanti
13	lungo	poco alta	verso il basso	indietro
14	lungo	poco alta	verso il basso	orizzontale
15	lungo	poco alta	verso avanti	orizzontale

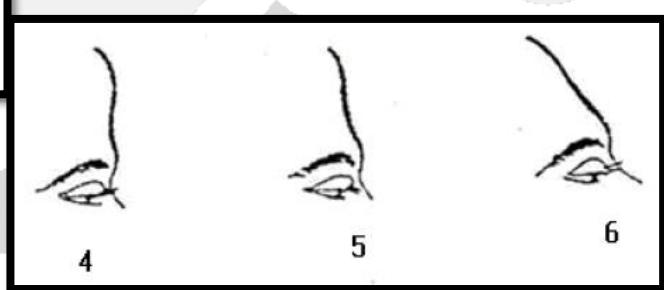
PROFILO NASO-BUCCALE



- A. **Nasale**: la faccia sporge in corrispondenza del naso, mentre il mento è sfuggente;
- B. **Dentale superiore**: il labbro superiore sporge sul mento sfuggente;
- C. **Mandibolare**: il labbro inferiore sporge in avanti rispetto al superiore;
- D. **Totale**: naso e mentoniera sono protesi in avanti per cui la linea verticale che scende dalla parte inferiore della fronte raggiunge il mento tagliando in avanti tutte le altre parti.



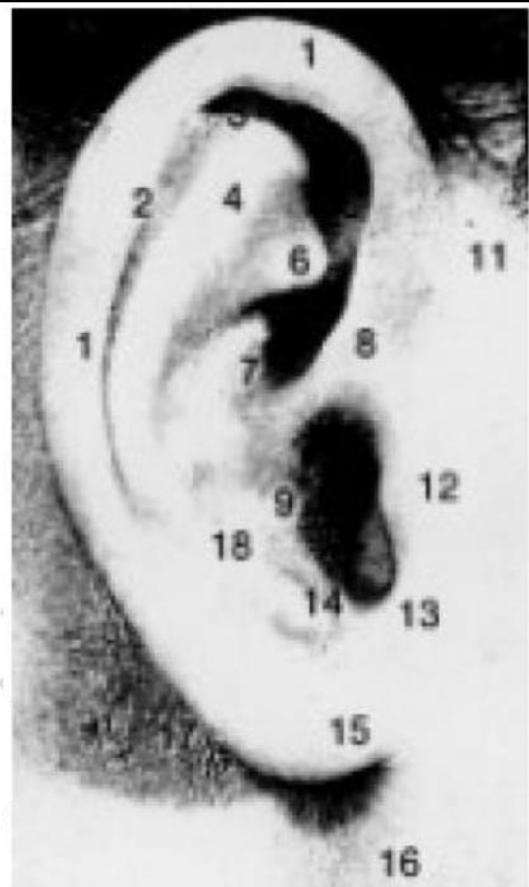
CODIFICA DEL PROFILO DELLA FRONTE



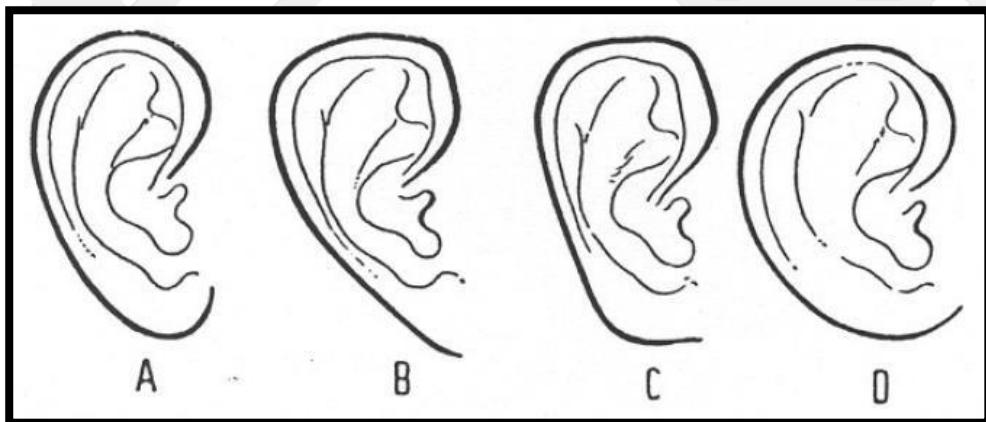
- 1) concava;
- 2) rettilinea;
- 3) convessa;
- 4) Prominente
- 5) intermedia;
- 6) sfuggente.

ORECCHIO ESTERNO

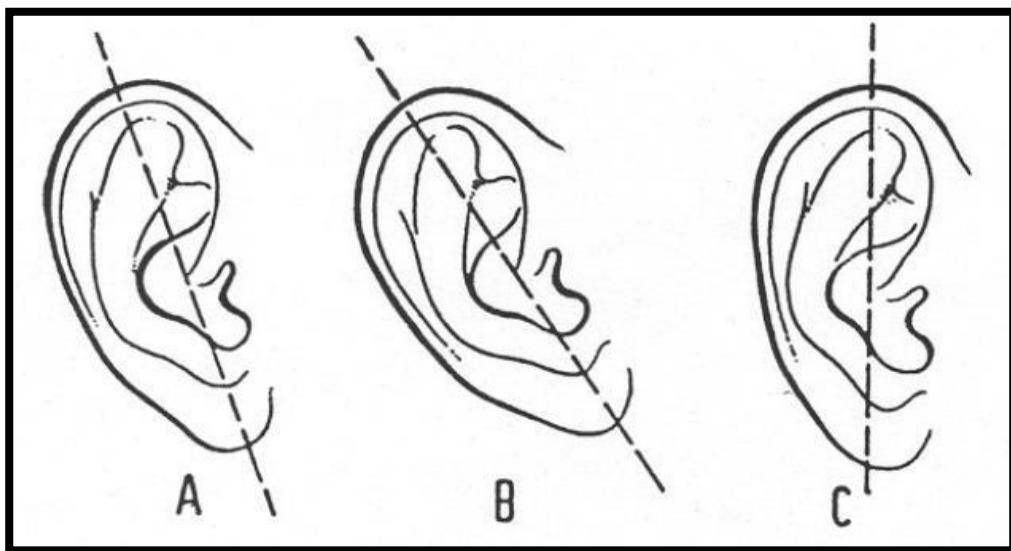
- 1) elice;
- 2) tubercolo auricolare;
- 3) fossa scafoidea;
- 4) radice superiore dell'elice;
- 5) fossa triangolare;
- 6) pilastro inferiore dell'antelice;
- 7) parte superiore della conca;
- 8) radice dell'elice;
- 9) parte inferiore della conca;
- 10) meato acustico esterno;
- 11) nervo auricolo temporale;
- 12) trago;
- 13) incisura intertragica;
- 14) antitrago;
- 15) lobulo;
- 16) antelice.



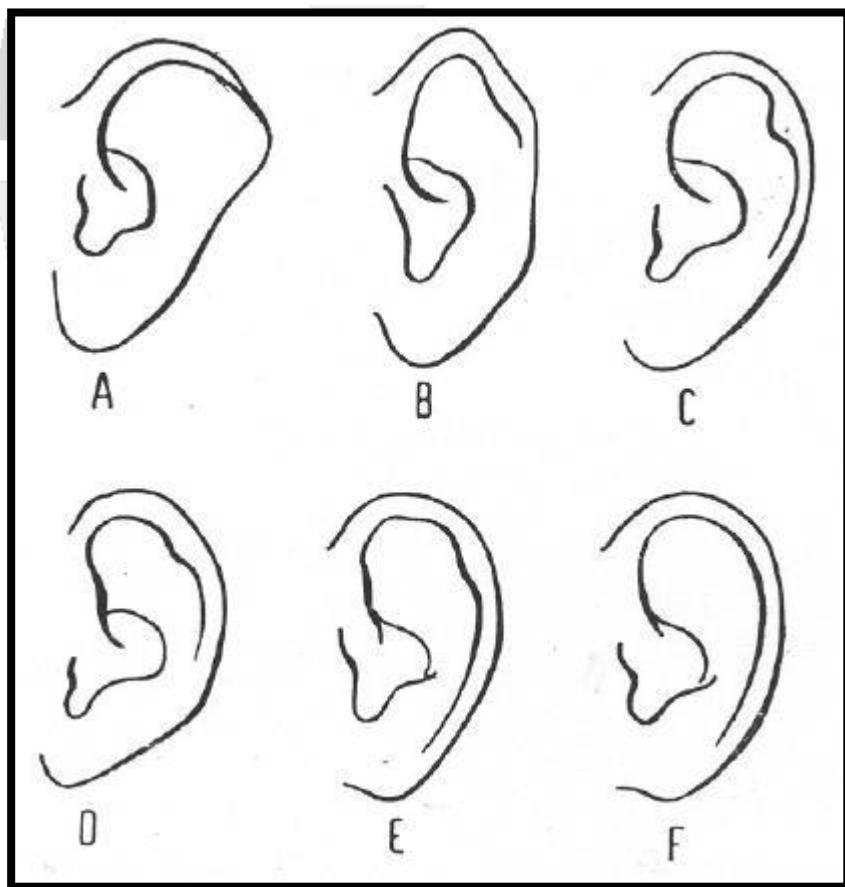
FORMA DELL'ORECCHIO



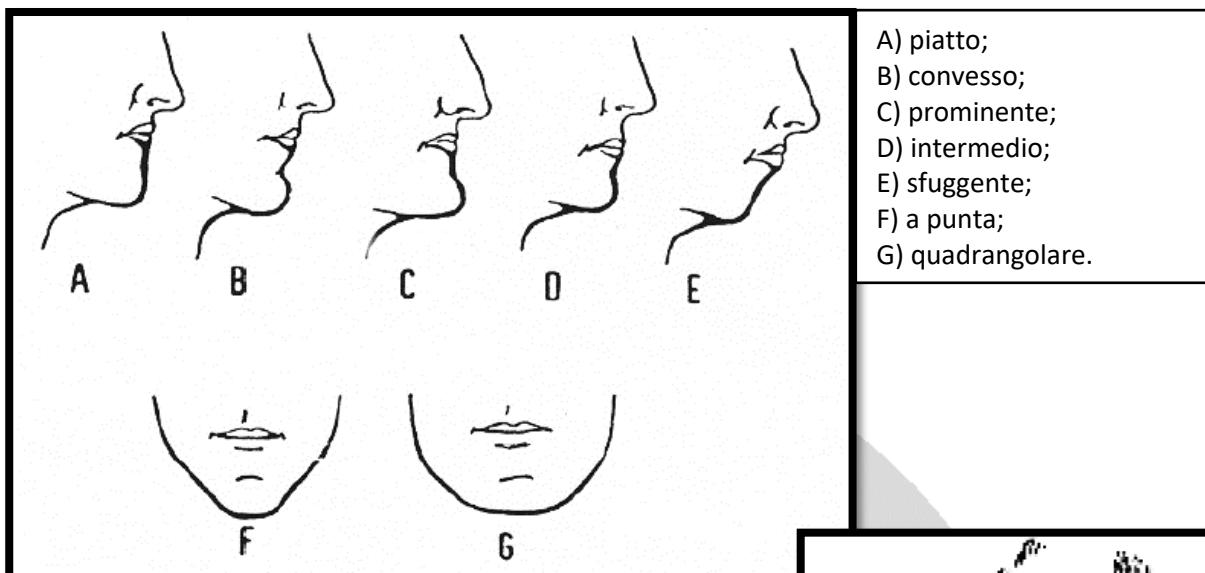
Direzione dell'orecchio



Schema delle diverse forme del tubercolo di Darwin



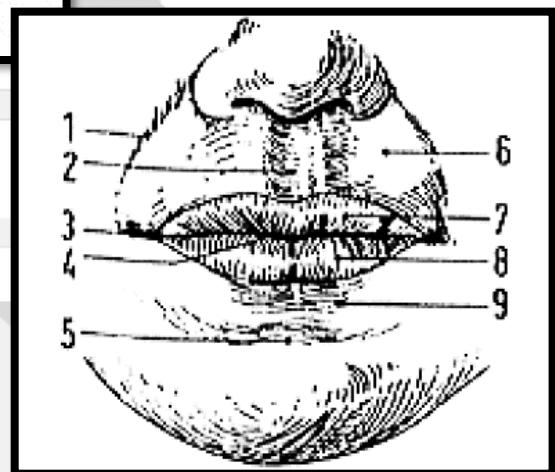
Forma del mento



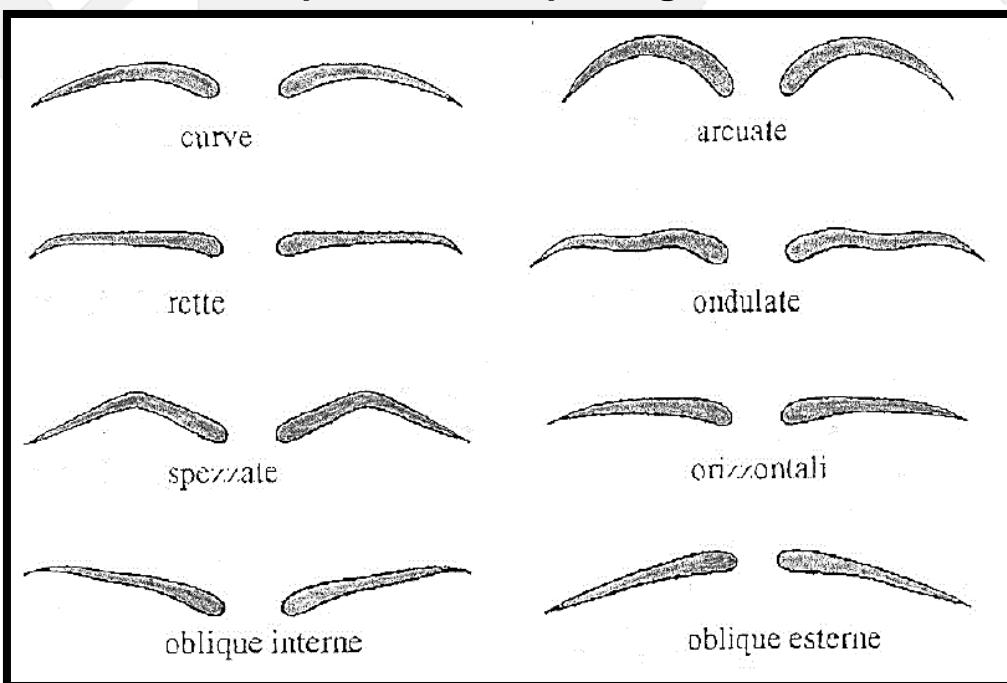
Struttura della bocca

Vale la seguente nomenclatura mostrata:

- 1) solco naso-labiale;
- 2) solco naso-orale;
- 3) angolo della bocca;
- 4) rima buccale;
- 5) solco mento-labiale;
- 6) labbro superiore;
- 7) prolabio superiore;
- 8) prolabio inferiore;
- 9) labbro inferiore.

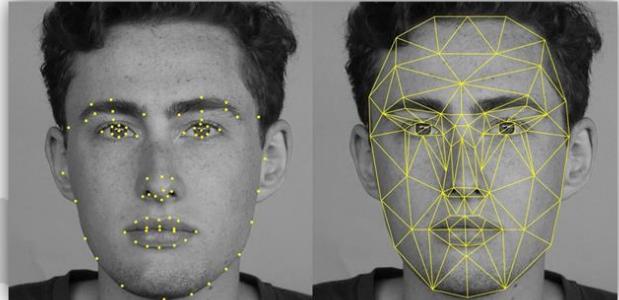


Aspetto delle Sopracciglia



IL RICONOSCIMENTO FACCIALE

Il riconoscimento facciale digitale funziona analizzando i tratti distintivi del viso, come la distanza tra gli occhi, la forma del naso e la posizione della bocca, utilizzando algoritmi di intelligenza artificiale.



Questi algoritmi comparano l'immagine di un volto con un database di immagini precedentemente raccolte per trovare una corrispondenza.

Betaface.com

Il processo di riconoscimento facciale può essere utilizzato in diverse applicazioni, come la sicurezza informatica, la sorveglianza, etc.

Di seguito un elenco di software e API⁵ per il riconoscimento facciale.

- Face++ di Megvii
- Microsoft Azure Face API
- Amazon Rekognition
- IBM Watson Visual Recognition
- OpenCV
- DeepSight di Senstetime
- Cognitec FaceVACS

Siti per il riconoscimento facciale:

- Betaface.com
- Amazon Rekognition
- Microsoft Face API
- IBM Watson Visual Recognition
- Google Cloud Vision API

⁵ API: È l'acronimo di application programming interface in Italiano interfaccia di programmazione delle applicazioni. Un'API è un intermediario software grazie al quale due applicazioni possono comunicare tra loro.

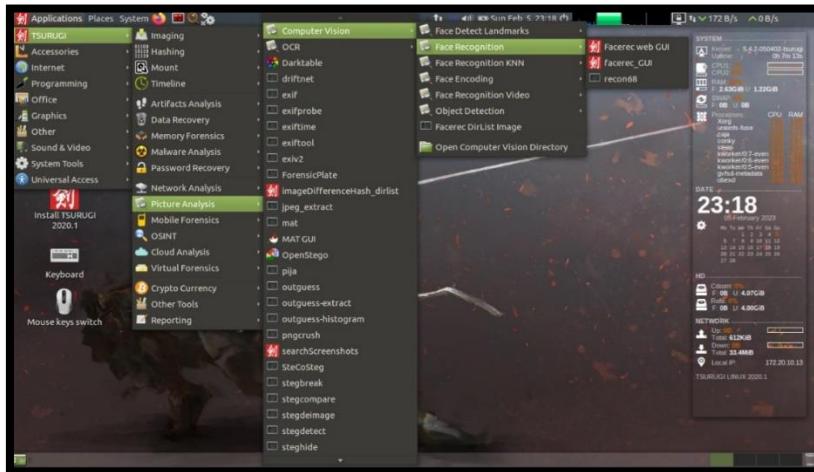
Approfondimento: <https://github.com/CScorza/Image-OSINT-Forensics>

LINUX E IL RICONOSCIMENTO FACCIALE

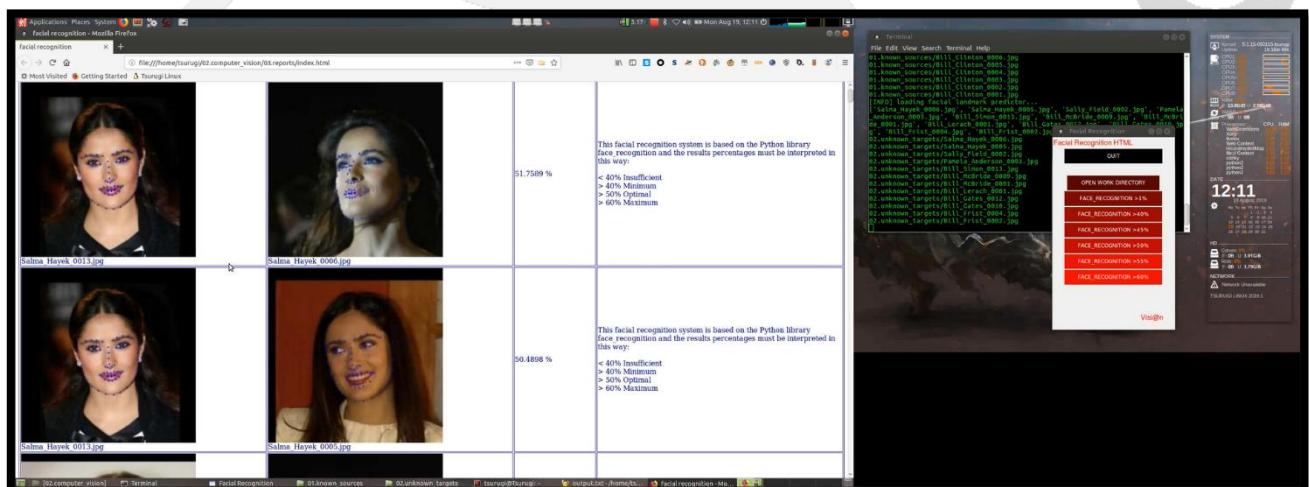
All'interno delle .iso Forensics di Tsurugi, è presente una sezione dedicata al Riconoscimento Facciale.

Il funzionamento degli script scritti in python, fanno riferimento a dei punti del viso e di vari algoritmi, per cercare una persona specifica all'interno di molte immagini inseriti in una cartella, mostrando la corrispondenza esatta in percentuale di somiglianza con un'immagine campione inserita in una seconda cartella.

Di seguito riporta il tutto in un file di Report in html.



iSO scaricabile su Tsurugi-linux.org



Immagini concesse da Visi@n

ANALISI DEL CONTENUTO

Consiste nel processo di estrazione delle informazioni presenti in un'immagine e nell'analisi di tali informazioni al fine di comprenderne il significato o il contesto

Si divide in due Tecniche:

- Analisi Visiva
- Analisi dei Metadati

L'Analisi Visiva

Serve ad individuare gli elementi significativi presenti nell'immagine.

Durante l'analisi, infatti, vengono identificate caratteristiche come forme, colori, texture e oggetti presenti nell'immagine. Queste informazioni possono quindi essere utilizzate per una vasta gamma di scopi, come la classificazione di immagini, la rilevazione di anomalie, la creazione di mappe di riferimento, la rilevazione di tendenze, ma soprattutto per l'attività d'Intelligence.

L'Analisi Visiva può essere suddivisa in tre fasi principali:

Pre-elaborazione:

In questa fase, l'immagine viene preparata per l'elaborazione successiva.

Questo può comportare l'eliminazione di rumore, la correzione della distorsione e l'ottimizzazione della qualità dell'immagine.

Elaborazione:

In questa fase, l'immagine viene sottoposta a una serie di elaborazioni per estrarre le informazioni significative.

Questo può comportare l'utilizzo di filtri, tecniche di rilevamento di oggetti, analisi di soggetti e molto altro.

Interpretazione:

In questa fase, le informazioni estratte dall'immagine vengono utilizzate per effettuare un'interpretazione. Questo può comportare la classificazione dell'immagine in una determinata categoria, la rilevazione di anomalie, la creazione di mappe di riferimento e molto altro.



ANALISI DEI METADATI

I metadati di un'immagine sono informazioni supplementari associate all'immagine stessa, che possono anche essere modificati tramite i vari software e che forniscono informazioni sulle condizioni in cui è stata scattata la foto, sulle impostazioni della fotocamera e su altri dettagli tecnici.

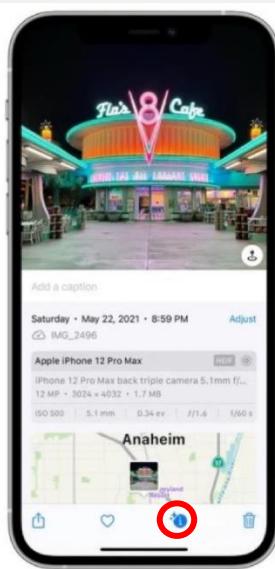
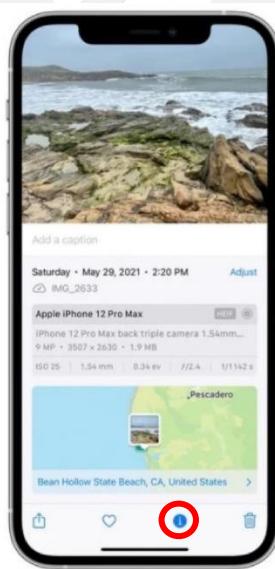
Quindi in sostanza queste informazioni vengono *"inserite"* all'interno della foto digitale al momento dello scatto.

I metadati più comuni associati alle immagini includono:

- **Data e ora dello scatto:** informazioni sul momento in cui è stata scattata l'immagine.
- **Modello di Fotocamera/Smartphone:** il nome e il modello della fotocamera che è stata utilizzata per scattare l'immagine.
- **Impostazioni della fotocamera:** informazioni sulle impostazioni della fotocamera, come la risoluzione, l'esposizione, la luminosità, la nitidezza e la profondità di campo.
- **Localizzazione:** informazioni sulla posizione geografica in cui è stata scattata l'immagine, se disponibili.
- **Autore:** il nome della persona che ha scattato l'immagine.

Questi metadati possono essere visualizzati attraverso le impostazioni della macchina fotografica digitale o attraverso le impostazioni del nostro smartphone e utilizzando software di elaborazione delle immagini o strumenti di gestione dei metadati.

6



Predefinito	Metadati
Predefinito	Nessuno
Nome file	_9110129.ORF
Nome copia	
Cartella	11
Stato metadati	Modificato
Titolo	Closeup of fresh chillies Habanero Orange
Didascalia	Fresh and colorful Orange Habanero peppers freshly picked from the plant
Copyright	Giovanni Bertagna - www.bertagna.it
Stato Copyright	Sconosciuto
Creatore	Giovanni Bertagna
Località	
Valutazione	• • • •
Etichetta	Verde
Ora di acquisizione	16:02:43
Data di acquisizione	11 settembre 2016
Dimensioni	4608 x 3456
Ritaglio	4608 x 3456
Esposizione	1/100 sec a f / 20
Lunghezza focale	43 mm
Sensibilità ISO	ISO 200
Flash	Non utilizzato
Marca	OLYMPUS IMAGIN...
Modello	E-PL5
Obiettivo	OLYMPUS M.12-50...
GPS	



⁶ <https://www.macitynet.it/foto-ios-15-metadati-exif-immagini/>
Approfondimento: <https://github.com/CScorza/Image-OSINT-Forensics>

Qui di seguito alcuni strumenti e software per il rilievo di metadati presenti nelle foto:

Software:

[MEDIAINFO](#)

[JPEGSNOOP](#)

[PHOTOME](#)

(Oltre ai vari software di grafica di Adobe, Gimp, CorelDraw, etc.)

Software Online:

[FOTOFORENSICS](#)

[29a](#)

[IMAGEFORENSIC](#)

[ERRORLEVELANALYSIS](#)

[Imageedited - Is Your Image Edited?](#)

[Metadata2go](#)

[Getghiro](#)

[Exif Jpeg header manipulation tool](#)

[Fake news debunker by InVID & WeVerify](#)

[ExtractMetadata.com](#)

The screenshot shows the JPEGsnoop application window. At the top, there's a menu bar with File, Edit, View, Tools, Options, Help. Below the menu is a toolbar with various icons. The main area displays a large amount of text-based metadata information. It starts with file offsets (0x000022399 to 0x00082C3D7), followed by markers (SOI, EOI, and SOS). Then it moves to searching compression signatures, listing various camera models like Canon EOS 5D Mark II, Nikon D800, and others. Below this is a table comparing EXIF.Maker / Software against EXIF.Model, showing quality and subsamp match columns. The table includes rows for Canon cameras, Sigma, and several mobile devices. At the bottom, there's a note about matching iSO-based editors and a section for ASSESSMENT.

File	
File Type	JPEG
File Type Extension	.jpg
MIME Type	image/jpeg
Image Width	1372
Image Height	2048
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
JFIF	
JFIF Version	1.01
Resolution Unit	cm
X Resolution	29
Y Resolution	29
ICC_Profile	
Profile CMM Type	Little CMS
Profile Version	2.1.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	2012:01:25 03:41:57
Profile File Signature	acsp
Primary Platform	Apple Computer Inc.
CMM Flags	Not Embedded, Independent
Device Manufacturer	
Device Model	
Device Attributes	Reflective, Glossy, Positive, Color
Rendering Intent	Perceptual
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	Little CMS
Profile ID	0
Profile Description	c2
Profile Copyright	FB
Media White Point	0.9642 1 0.82491
Media Black Point	0.01205 0.0125 0.01031
Red Matrix Column	0.43607 0.22249 0.01392
Green Matrix Column	0.38515 0.71687 0.09708
Blue Matrix Column	0.14307 0.06061 0.7141
Red Tone Reproduction Curve	(Binary data 64 bytes)
Green Tone Reproduction Curve	(Binary data 64 bytes)
Blue Tone Reproduction Curve	(Binary data 64 bytes)
Composite	
Image Size	1372x2048
Megapixels	2.8

[FotoForensics.com](#)

[JPEGsnoop](#)

Estensioni Browser di Image Forensics (Ricerca Metadati)

- [SEARCH Investigative and Forensic Toolbar](#)
- [EXIF Viewer Pro](#)
- [Fake news debunker by InVID & WeVerify](#)
- [Fake Profile Detector \(Deepfake, GAN\)](#)

Ricerca Seriale Foto Camera

- [Stolen Camera Finder](#)



HASH (L'impronta del dato)

"Un hash è una funzione matematica che prende in input una stringa di dati di qualsiasi lunghezza e restituisce un output di lunghezza fissa, chiamato hash digest."

Il digest hash è una rappresentazione univoca dell'input originale, il che significa che due input diversi non possono produrre lo stesso output."

Questa proprietà rende i hash utili per molti scopi, tra cui la verifica dell'integrità dei dati, la creazione di dizionari, la codifica di password e molto altro.



79054025
255fb1a2
= 6e4bc422
aef54eb4

Se abbiamo due elementi (File, Immagini, software, etc) da analizzare e capire se sono due copie identiche, possiamo calcolare l'hash del primo file e confrontarlo con l'Hash del secondo file.

Se i due valori risultano identici allora vuol dire che anche i due elementi sono identici.

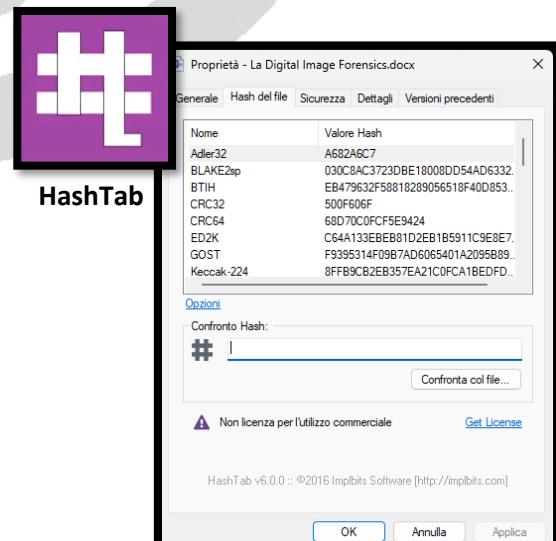
Per questo motivo, a volte viene definita "**impronta digitale**".⁷

Esistono molti tipi di funzioni hash, alcune delle quali sono più comunemente utilizzate di altre. Ecco alcuni dei tipi più popolari:

- **MD5:** Una funzione hash molto comune che produce un output a 128 bit.
- **SHA-1:** Un'altra funzione hash molto comune che produce un output a 160 bit.
- **SHA-2:** Una famiglia di funzioni hash che include diversi algoritmi con output di lunghezza diversa, tra cui SHA-256 e SHA-512.
- **SHA-3:** Una famiglia di funzioni hash recentemente introdotta come successore della famiglia SHA-2.
- **BLAKE2:** Una funzione hash molto veloce che produce un output a 256 bit.

Strumenti e Software per calcolare l'hash:

- | | | |
|---|--|--|
| <ul style="list-style-type: none">• HashCheck• HashMyFiles• CertUtil• md5sum• OnlineHashCrack | <ul style="list-style-type: none">• WinMD5Free• HashTab• HashCalc• QuickHash• PeaUtils | <ul style="list-style-type: none">• Free File Hasher• EasyHash• GtkHash• HashIt• A Soft Murmur |
|---|--|--|



⁷ Approfondimento: <https://github.com/CScorza/Image-OSINT-Forensics>

TIPI DI FORMATO DELLE IMMAGINI

I formati di immagine possono essere classificati in base alla loro capacità di compressione:

Abbiamo 4 gruppi:

- Formato Lossy
- Formato Lossless
- Formato Proprietario
- Formato file RAW

Formato Lossy

Il formato di compressione lossy è un tipo di formato di immagine che comprimerà il file riducendo la qualità dell'immagine. Questo significa che l'immagine decompressa non sarà identica all'immagine originale. Ciò può causare la perdita di dettagli, sfumature di colore e altre informazioni visive.

È da tenere presente che, anche se il formato lossy può essere conveniente per ridurre le dimensioni del file, una volta che l'immagine viene compressa e decompressa più volte, la qualità dell'immagine continuerà a peggiorare. Questo tipo di formati sono utilizzati moltissimo nelle chat di messaggistica, nei social network, email etc.

I formati di riferimento sono:

- **JPEG** (.jpeg, .jpg) - Joint Photographic Experts Group
- **JPEG 2000** (.jp2) - Joint Photographic Experts Group 2000
- **GIF** (.gif) - Graphics Interchange Format



Formato Lossless

I formati lossless utilizzano algoritmi di compressione che mantengono intatte le informazioni sulla quantità di colore, la posizione e le proprietà dei singoli pixel.

Questo tipo di formato è particolarmente utile per le immagini che devono essere modificate o elaborate in seguito, o per le immagini che hanno elementi precisi, come testo o linee, che potrebbero essere alterati da una compressione lossy.

Esempi di formati di immagini lossless includono **PNG**, **GIF** non compresso e **TIFF**.

Questi formati sono supportati da molte applicazioni di elaborazione di immagini e sono comunemente utilizzati in molte situazioni, come la creazione di siti web, la stampa di documenti e la creazione di immagini destinate alla manipolazione.

In generale, un formato di immagini lossless offre una qualità superiore rispetto ai formati di immagini lossy, ma richiede anche una quantità maggiore di spazio di archiviazione.

Questo equilibrio tra qualità e quantità di spazio di archiviazione deve essere valutato attentamente quando si sceglie un formato di immagine per un particolare progetto.



Formati Proprietari

I formati proprietari delle immagini sono formati di file che sono sviluppati e controllati da un'azienda o da un'organizzazione specifica e che possono essere utilizzati solo con le loro applicazioni o software proprietari.

Questi formati sono spesso utilizzati per archiviare immagini digitali in modo efficiente e sicuro, ma possono essere difficili da aprire o utilizzare con altri software o sistemi.

Questi sono un esempio di formati proprietari:

- **PSD** (Adobe Photoshop)
- **AI** (Adobe Illustrator)
- **CDR**(Corel Corporation)
- **DWG** (AutoCAD Drawing)
- **XCF** (eXperimental Computing Facility) – Formato natio di Gimp.



Formato RAW (Grezzo)

Il formato RAW è un formato di file per immagini utilizzato da molte fotocamere digitali ed impostabile nelle applicazioni “Camera” dello smartphone. Si tratta di un formato proprietario che offre una qualità di immagine superiore rispetto ai formati di file più comuni, come i formati Lossy (JPEG o PNG).

Il formato RAW archivia i dati grezzi del sensore della fotocamera, il che significa che non vengono effettuate alcune delle elaborazioni che avvengono in altri formati di file.

Questo dà agli utenti un maggiore controllo sulla post-elaborazione delle immagini e consente di ottenere immagini più nitide e dettagliate.

Tuttavia, il formato RAW ha anche alcuni svantaggi:

- Richiede più spazio di archiviazione rispetto ai formati di file più comuni
- Può essere difficile da aprire o utilizzare con software o sistemi diversi dalla fotocamera che l'ha prodotto.
- Inoltre, il formato RAW richiede una post-elaborazione prima di essere visualizzato o condiviso con altre persone.



In generale, il formato RAW è più adatto per i fotografi professionisti o per gli appassionati che desiderano un maggiore controllo sulla post-elaborazione delle immagini, mentre i formati di file più comuni sono più adatti per l'utilizzo quotidiano e per la condivisione di immagini con altre persone.

La scelta del formato dipende dalle esigenze specifiche di ogni progetto e dalle capacità del software disponibile.

Formati proprietari RAW:

- **Canon:** CRW (Canon RaW, estensione file: *.CR2 e *.CR3);
- **Epson:** ERW (Epson RaW);
- **Foveon:** X3F.
- **Fuji:** RAF (Raw Fuji);
- **Hasselblad:** 3FR.
- **Kodak:** DCR (Digital Camera Raw);
- **Minolta:** MRW (Minolta RaW);
- **Nikon:** NEF (Nikon Electronic Format);
- **Olympus:** ORF (Olympus Raw Format);
- **Pentax:** PEF (Pentax Electronic Format).
- **Sony:** ARW (Alpha RaW).
- **Samsung:** SRW (Samsung RaW)

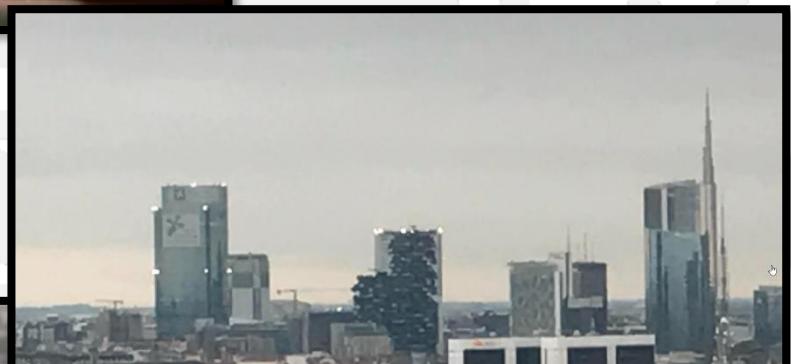
TIPICI PROBLEMI DI QUALITÀ DELLE IMMAGINI

Compressione del file con perdita A seconda della tipologia dell'immagine, essa potrebbe avere una serie di problemi di qualità quali

- Il movimento veloce
- La pixelizzazione dello zoom
- Sfocatura
- Sotto o sovraesposizione
- Illuminazione scarsa
- Compressione del file con perdita



Il movimento veloce



La pixelizzazione dello zoom



Sfocatura

TECNICHE DI MIGLIORAMENTO DELL'IMMAGINE

Ci sono molte tecniche che possono essere utilizzate per migliorare la qualità di un'immagine. Ecco alcune delle tecniche più comuni:

- **Nitidezza - Regolazione della luminosità e del contrasto:** queste tecniche possono essere utilizzate per migliorare la visibilità delle aree scure o troppo luminose dell'immagine.



- **Rimozione del rumore:** questa tecnica viene utilizzata per ridurre il rumore digitale presente in un'immagine, soprattutto quelle scattate con fotocamere a bassa risoluzione o in condizioni di scarsa illuminazione.



AmpedFIVE

- **Correzione della distorsione:** questa tecnica viene utilizzata per correggere le deformazioni presenti in un'immagine, come la distorsione barilottica o la distorsione della fisheye.



- **Ritaglio:** questa tecnica viene utilizzata per ritagliare un'immagine e migliorarne la composizione.
- **Miglioramento del colore:** questa tecnica viene utilizzata per migliorare la saturazione del colore, la gamma di colori e la tonalità dell'immagine.



- **Ridimensionamento/Interpolazione pixel:** Ridimensiona un'immagine o un video a una risoluzione maggiore per identificare ulteriormente i dettagli



Queste sono solo alcune delle tecniche che possono essere utilizzate per migliorare la qualità di un'immagine.

La scelta della tecnica dipende dalle esigenze specifiche di ogni progetto e dalle capacità del software disponibile.

L'USO DEI CANALI COLORE (RGB) PER L'ESTRAPOLAZIONI DI DETTAGLI

In un contesto forense è una tecnica utilizzata per analizzare le immagini e estrarre informazioni supplementari che potrebbero essere importanti, capire se l'immagine è stata manipolata e quindi verificare la sua integrità.

In un'immagine digitale, ogni pixel è rappresentato da un insieme di valori di colore che vengono memorizzati in diversi canali, come il canale rosso, verde e blu (RGB).

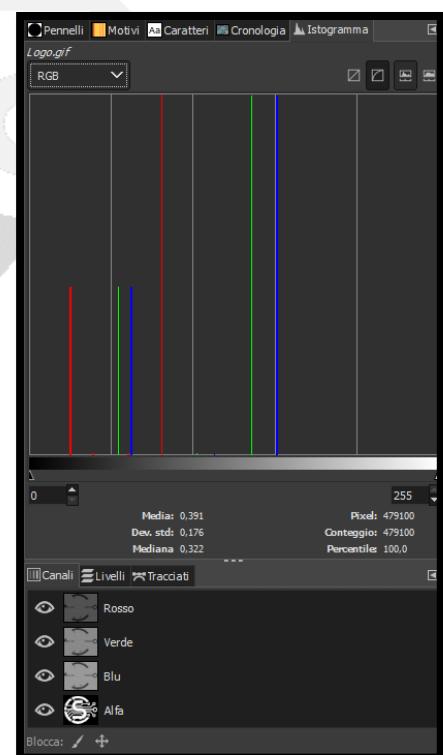
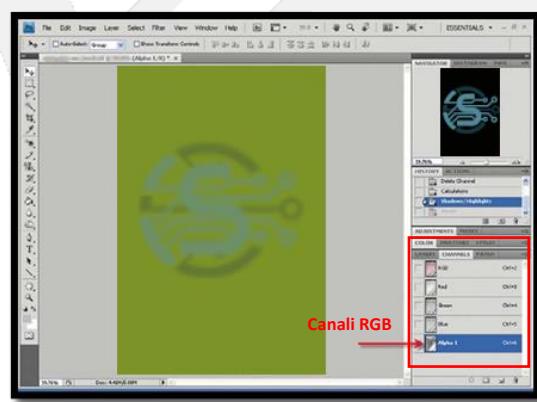
Questi canali possono essere separati e analizzati singolarmente per rivelare informazioni nascoste o dettagli che potrebbero essere altrimenti difficili da vedere nell'immagine originale.

Ad esempio, l'analisi dei canali colore può essere utilizzata per identificare eventuali artefatti digitali, come quelli causati da una compressione delle immagini, che potrebbero indicare una manipolazione dell'immagine.

Passaggi nei principali software grafici:

Per visualizzare i canali RGB su Photoshop, seguite questi passaggi:

1. Aprire l'immagine in Photoshop.
2. Fare clic su "Canale" nel menu a discesa "Finestra".
3. Fare clic su uno dei canali RGB (R, G o B) per visualizzare la sua immagine a scala di grigio.
4. Fare clic sull'altro canale per visualizzare la sua immagine a scala di grigio.
5. Continuare a fare clic sui canali per visualizzare la loro immagine a scala di grigio.



Per visualizzare i canali RGB su GIMP, seguite questi passaggi:

1. Aprire l'immagine in GIMP.
2. Fare clic su "Canali" nel menu a discesa "Finestra".
3. Fare clic su uno dei canali RGB (R, G o B) per visualizzare la sua immagine a scala di grigio.
4. Fare clic sull'altro canale per visualizzare la sua immagine a scala di grigio.
5. Continuare a fare clic sui canali per visualizzare la loro immagine a scala di grigio.

Canali RGB, GIMP

PARTE 2

STRUMENTI DI RICERCA DELLE IMMAGINI

Esistono diversi Motori di ricerca ed Estensioni che possono essere utilizzati per cercare immagini su Internet.

Qui di seguito vedremo come da un'Immagine contenuta sul Desktop o presente sul web, si possa effettuare una serie di ricerche per capire:

- La provenienza dell'immagine;
- Che cosa rappresenta;
- Estrazione del testo e traduzione presente nell'immagine;
- Ricerca Oggetti presenti nell'immagine;
- Ricerca Numeri seriali dei mezzi di trasporto;
- Etc.

Esempi di Motori di Ricerca Generici:

- [Google Images - LENS](#)
- [Yandex Images](#)
- [TinEye](#)
- [Bing Images – Ricerca Visiva](#)
- [Yahoo Image Search](#)
- [Flickr](#)
- [Zapmeta](#)
- [Baidu](#)



L'OSINT IMAGE e il SOCMINT

1

RICERCA DI UN PROFILO FACEBOOK AVENDO UNA FOTO TARGET.

2

3

4

N.B.
Più l'immagine è indicizzata sul web e più la ricerca avrà un esito positivo

RICERCA VOLTI

- [FaceCheck.id](#)
- [PimEyes](#)
- [Pictriev](#)
- [DeepFace \(Android\)](#)



REVERSE IMAGE SEARCH

(In questi motori di ricerca, puoi caricare un'immagine o inserire un URL che si riferisce a un'immagine, e il motore di ricerca ti mostrerà i risultati corrispondenti, come siti web che contengono l'immagine, informazioni sul proprietario dell'immagine o versioni di dimensioni diverse della stessa immagine.)

- [OsintCombine](#)
- [Karmadecay - Reverse image search of Reddit.com](#)
- [Reverse Image Search](#)
- [Berify](#)
- [DupliChecker - Reverse Image Search](#)

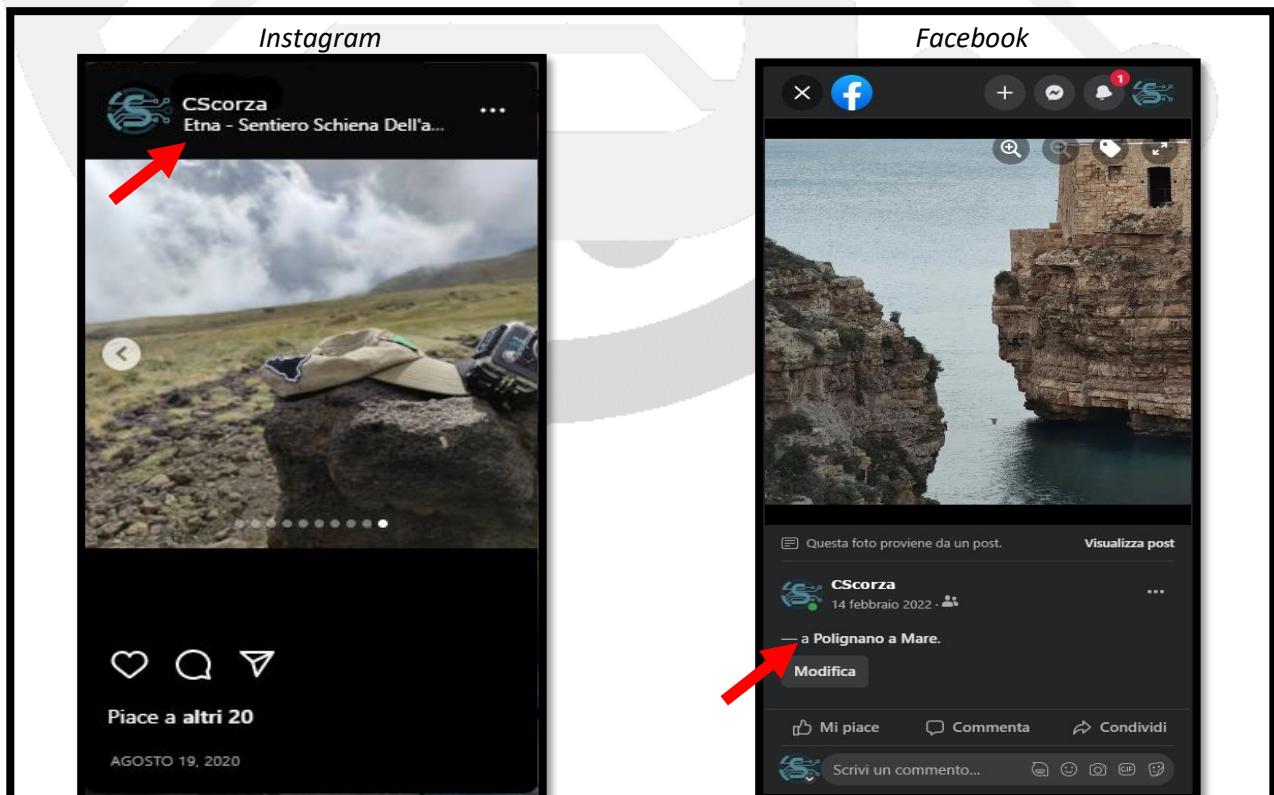
GEOLOCALIZZAZIONE DELLE IMMAGINI

(Ci sono diversi motori di ricerca che possono essere utilizzati per la geolocalizzazione delle immagini, ovvero per trovare informazioni sulla posizione geografica in cui sono state scattate le immagini.)

- [Geolocation Estimation - Image](#)
- [Google Maps](#) (Utilizzo di Google Street View)
- [Google Earth](#) (Utilizzo di Google Street View)
- [SnapChat](#) (Geolocalizzazione Immagini SnapChat)

Geolocalizzazione Immagini dei Social Network

Molti Social network hanno la possibilità di aggiungere la posizione GPS nelle Immagini da pubblicare, come Facebook, Instagram, Twitter, Linkedin e etc..



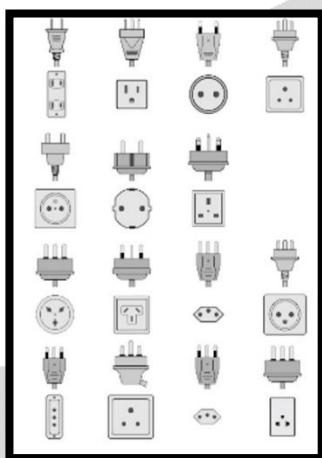
MOTORI DI RICERCA SPECIFICI PER GLI OGGETTI

Ricerca Generici

- [Image Identify](#)

Ricerca Marchi

- [US Sistema di ricerca elettronica dei marchi \(TESS\)](#)
- [UE - eSearch](#)
- [UE - TMview](#)



Ricerca Animali

- [Identificazione Uccelli](#)
- [Identify Dog Breeds Pro \(Android App\)](#)

Ricerca Auto

- [CarNet](#)

Ricerca Armi

- [Enciclopedia delle armi](#)



Ricerca Piante

- [PI@ntNet identify](#)

Ricerca Prese Elettriche

- [World plugs - IEC](#)
- [Sistema di ricerca elettronica dei marchi \(TESS\)](#)

Ricerca Colore

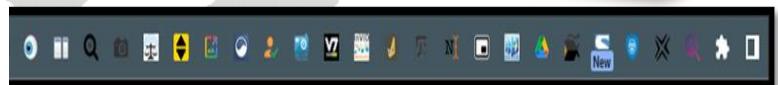
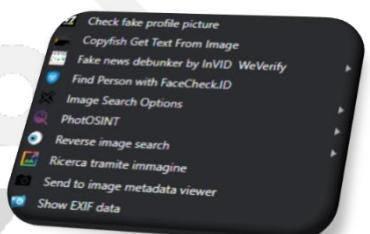
- [Tineye.com - Multicolore](#)



ESTENSIONI PER LA RICERCA DI IMMAGINI

(Google Chrome e FireFox)

- [PhotOSINT](#)
- [RevEye Reverse Image Search](#)
- [Search by Image](#)
- [FaceCheck Reverse Image Search](#)
- [Fast Advanced Google Search](#)
- [View Image](#)



APP SMARTPHONE PER LA RICERCA DELLE IMMAGINI

- Google Lens ([Android](#), [iOS](#))
- Investigatore foto ([iOS](#))
- Forensics Acquisition of Screenshot ([Android](#))
- IAFace ([Android](#))
- Photo Sherlock ([Android](#), [iOS](#))



Approfondimento: <https://github.com/CScorza/Image-OSINT-Forensics>
<https://github.com/CScorza/SOCMIIntelligence>

PARTE 3

STRUMENTI PER L'ANALISI DELLE IMMAGINI FALSE

Error Level Analysis

L'uso di ELA (*Error Level Analysis*) è una tecnica che consente di identificare eventuali modifiche apportate a un'immagine. L'ELA è uno strumento utile per l'analisi forense delle immagini e può essere utilizzato per identificare eventuali manipolazioni, ad esempio per modificare le informazioni presenti in un'immagine.

Questa tecnica si basa sul fatto che le modifiche apportate a un'immagine spesso causano un aumento del livello di errore nell'immagine rispetto alle parti originali.

L'ELA funziona comprimendo l'immagine (portandola al formato Jpeg) e successivamente decomponendo la versione compressa con una qualità diversa da quella originale.

Questo processo crea un'immagine con una qualità inferiore rispetto all'immagine originale, ma con le parti modificate che appaiono come livelli di errore più elevati rispetto alle parti originali.

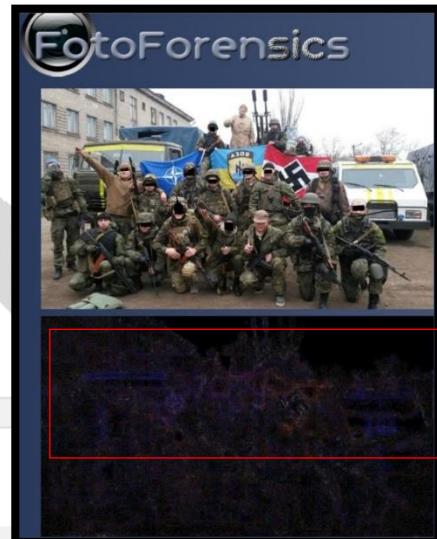
Per utilizzare l'ELA, l'immagine viene compressa con una qualità più bassa rispetto all'originale e successivamente confrontata con l'immagine originale. Le parti dell'immagine che hanno un livello di errore più elevato rispetto all'immagine originale sono considerate come eventuali modifiche apportate.

Questo tipo di tecnica, può essere utilizzata o manualmente con i programmi di grafica più comuni come Photoshop, Gimp etc.

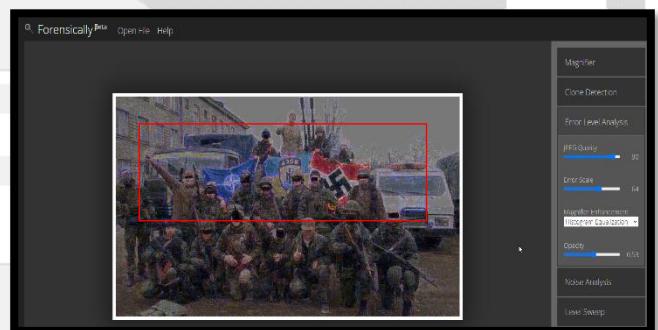
Ma è presente in altri strumenti online, in maniera "automatica":

- [FotoForensics](#)
- [Forensically](#)
- [ImageForensic.org](#)
- [ImageJ + plugin](#)
- [Ghiro](#)

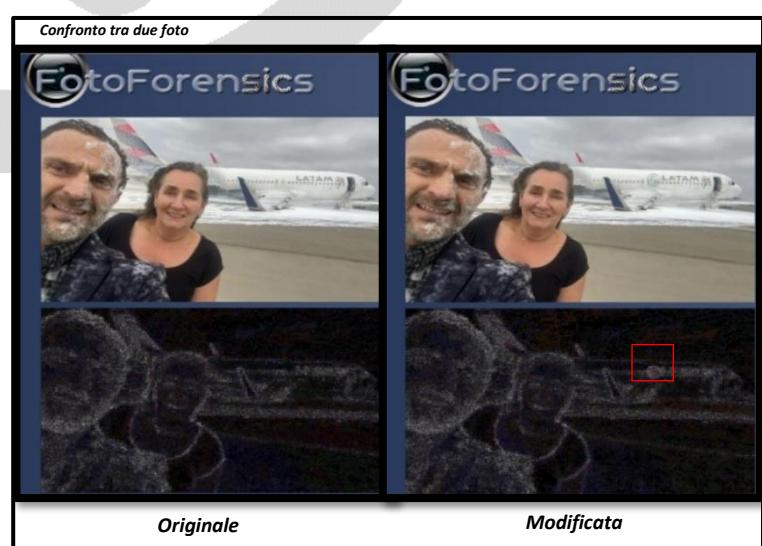
Come possiamo vedere negli esempi proposti (Es.1 ed Es.2), la tecnica "ELA", evidenzia come l'immagine non sia uniforme nell'insieme ma presenza delle parti più "marcate" di altre, che ci fanno supporre che siano state aggiunte successivamente.



Esempio 1



Esempio 2



L'USO DELL'OMBRA PER L'ANALISI DELLE IMMAGINI



Molte volte ci capita di vedere la proiezione dell'ombra nelle nostre immagini e oltre ad una serie di elementi che ci possono definire il periodo stagionale in cui è stata scattata una foto, possiamo utilizzare la tecnica del calcolo dell'ombra per definire anche in maniera approssimata, il mese e la fascia d'oraria in maniera più precisa possibile.

Questo perché la posizione del sole e la sua altezza nel cielo cambia durante il giorno e durante l'anno a causa della rotazione terrestre e della sua orbita intorno al sole. Questo influisce sulla direzione della luce solare e di conseguenza sulla direzione e forma dell'ombra proiettata.

I siti che ci vengono in aiuto in questa tecnica sono:

- [CalcSun](#)
- [Shadow Calculator](#)
- [Sun Path 3D](#)
- [Google Earth](#)

Utilizzando una immagine esempio (Piazza San Pietro - Vatican City), calcoleremo l'ombra proiettata dall'obelisco che si erge al centro della piazza, in 3 Step.



Step.1

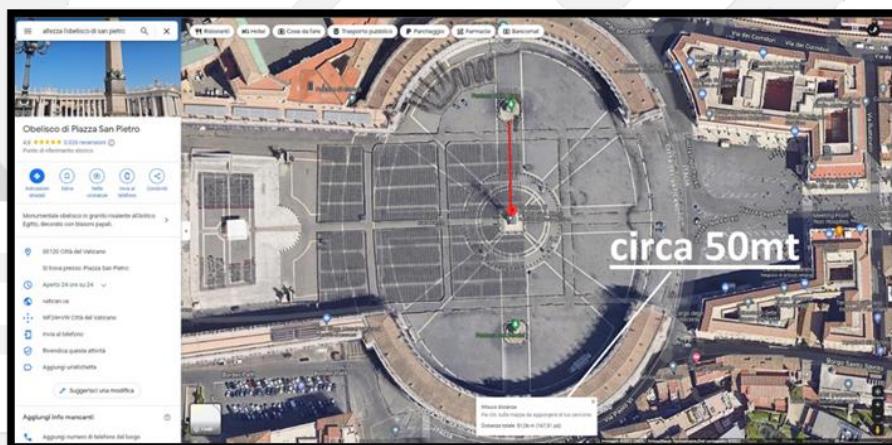
Analisi Visiva

Proiezione dell'Ombra



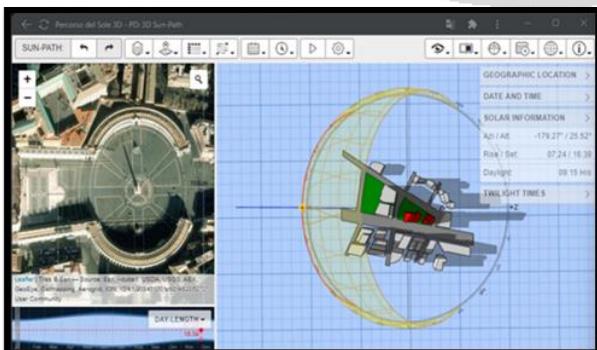
Step.2

Calcolo della lunghezza della Proiezione dell'Ombra, utilizzando la funzione righello di Google Maps o Google Earth.

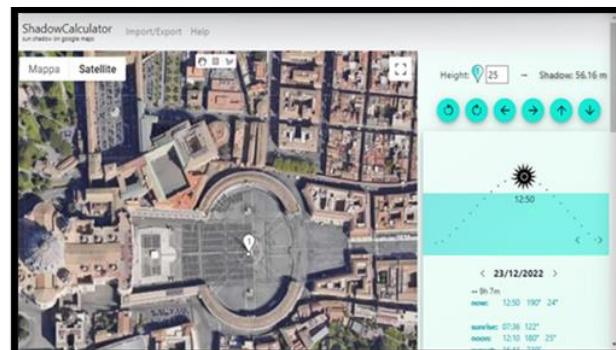


Step.3

Utilizzo di uno dei software elencati precedentemente e dopo aver inserito la misura rilevata “giocare” con le date per stabilire a che ora, giorno, mese e anno, l'ombra si trova a quell'altezza e con quella lunghezza.



[Sun Path 3D](#)



[Shadow Calculator](#)

Parte 4

UTILIZZO FORENSE DEI PROGRAMMI DI GRAFICA

L'uso forense di software di elaborazione delle immagini come Photoshop o GIMP è molto importante per non compromettere la **validità e l'integrità** delle immagini stesse, utilizzate come prove per esempio in un processo giudiziario.

Se venissero utilizzati per modificare o manipolare le immagini, potrebbero influire sull'esito della loro autenticità.

Per questo motivo, è importante utilizzare questi software in modo responsabile e seguire rigorosi standard forensi per garantire che le immagini utilizzate come prove siano autentiche e non manipolate.

Ad esempio, è importante mantenere una documentazione completa di tutte le modifiche effettuate all'immagine, utilizzare formati di file che consentano di verificare l'autenticità dell'immagine e utilizzare tecniche di analisi forense per verificare la integrità dell'immagine.

Di seguito, una *Linea Guida* come premessa prima di aprire il programma di grafica:

1. Mantenere una documentazione completa:

- Mantenere una documentazione dettagliata di tutte le modifiche effettuate all'immagine, inclusi i file originali e i file modificati, è fondamentale per garantire la tracciabilità delle modifiche e preservare la integrità dell'immagine.

2. Utilizzare formati di file affidabili:

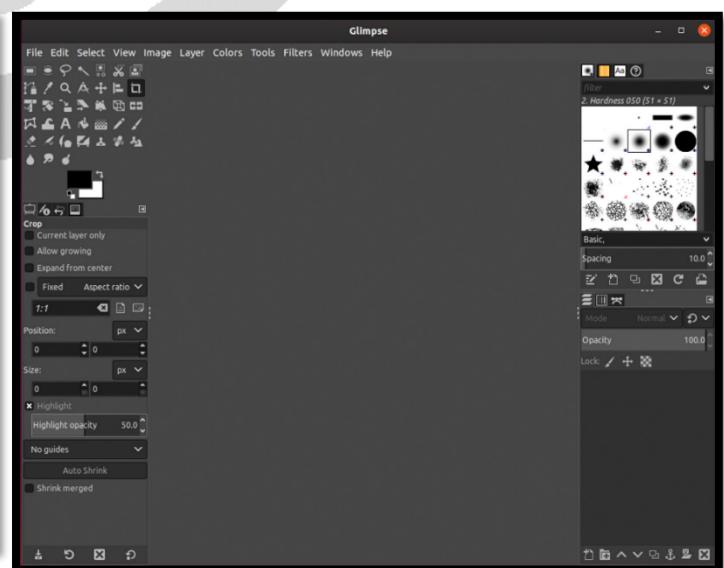
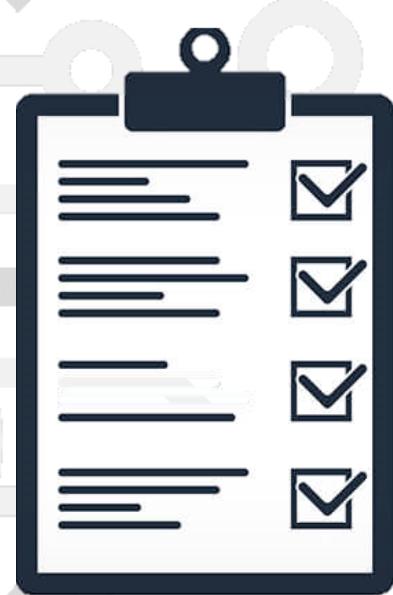
- Utilizzare formati di file che consentano di verificare l'autenticità dell'immagine, come i formati di file non compressi TIFF o RAW è importante per garantire che l'immagine non sia stata manipolata.

3. Evitare di sovrascrivere i file originali:

- È importante evitare di sovrascrivere i file originali con le modifiche effettuate, in modo da preservare la integrità dell'immagine originale.

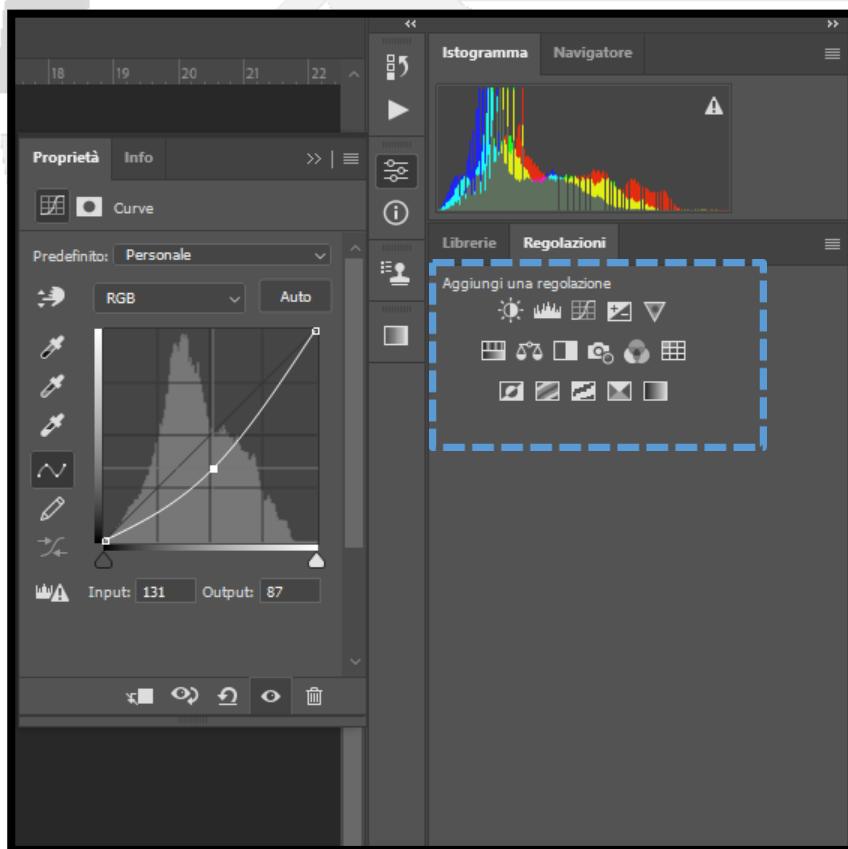
4. Verificare l'integrità dell'immagine:

- Utilizzare tecniche di analisi forense, come l>Error Level Analysis (ELA), per verificare l'integrità dell'immagine e determinare se è stata manipolata.

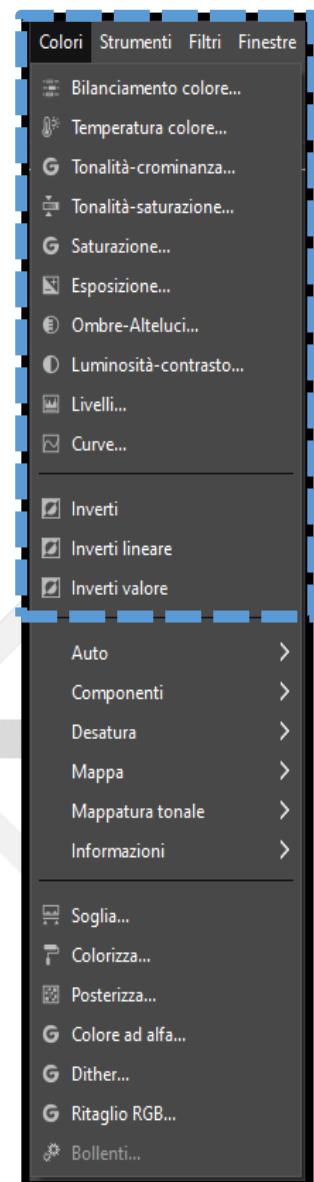


Linea guida per l'uso di software grafici in modalità forense per non alterare l'integrità dell'immagine

1. Apri l'immagine che desideri misurare in (Es .Photoshop o Gimp.)
2. Utilizzare lo strumento "**Allineamento**" per allineare l'immagine in modo che l'oggetto che si desidera misurare sia dritto e parallelo alla griglia.
 - È possibile utilizzare lo strumento "Allineamento" per ruotare e spostare l'immagine in modo che sia perfettamente allineata.
3. Utilizzare lo strumento "**Zoom**" per ingrandire l'immagine in modo da poter vedere i dettagli dell'oggetto che si desidera misurare.
4. Utilizzare lo strumento "**Misura/Righello/Misurino**" per misurare l'oggetto.
 - È possibile utilizzare questo strumento per misurare la lunghezza di un oggetto noto nell'immagine e quindi utilizzare questa informazione per calcolare le dimensioni dell'oggetto che si desidera misurare.
5. Utilizzare lo strumento «**Luminosità/Contrasto**» per regolare la luminosità e il contrasto dell'immagine in modo che l'oggetto che si desidera misurare sia ben visibile.



Photoshop, strumenti utili ai fini forensi



GIMP, strumenti utili ai fini forensi

ESTRAPOLAZIONE DEI VIDEO DA SITIWEB O DA DVR

Questo capitolo serve per aiutare quanti si trova ad dovere estrarre o condividere/ricevere video e hanno paura dell'alterazione della qualità dell'immagini e quindi compromettere le stesse con la perdita di dati.

Molti siti web pubblicano e/o fanno condividere dei video (YouTube, TikTok, Facebook, Instagram etc), e molti di noi condividiamo i video (anche quelli di natura lavorativa che andrebbero condivisi solo tramite E-mail), via chat di messaggistica come WhatsApp o Telegram.

I social media però per una ragione pratica, preferisco comprimere i video che noi condividiamo, in modo da poter essere facilmente condivisa e scaricata velocemente. Questo fa sì che il video cambia il suo formato originale e quindi perde moltissimo di qualità.

Lo stesso potrebbe avvenire a chiunque deve impostare per ragioni di lavoro o altro il proprio DVR o deve estrarre le immagini da esso.

Scaricare un video da un DVR è una procedura delicata che richiede particolare attenzione per evitare di compromettere la qualità delle immagini, quindi dobbiamo impostare il DVR in questo modo:

- **Imposta le impostazioni di scaricamento:** dopo aver selezionato il video, imposta le impostazioni di scaricamento. Scegli il formato di file appropriato (ad esempio, MP4 o AVI) e la risoluzione desiderata. Assicurati che l'impostazione della risoluzione sia la stessa del video originale.
 - **Il formato MP4 (MPEG-4 Part 14):** È molto utilizzato per la distribuzione di video online, poiché offre un'elevata qualità dell'immagine e una buona compressione del file. Inoltre, il formato MP4 supporta diverse risoluzioni video, tra cui 1080p e 4K.
 - **Il formato AVI (Audio Video Interleave):** È stato uno dei primi formati video ad essere sviluppato per computer. Anche se è meno utilizzato rispetto al passato, è ancora uno dei formati video più comuni e supporta diverse risoluzioni video, tra cui 720p e 1080p.



Importante ai fini della traccabilità, identificare il DVR (Serial ID che si trova all'interno delle impostazioni oppure nel retro del case fisico) e l'Hash del file estratto e inserirlo nel report/verbale che poi viene compilato per i vari usi.

Di norma quando viene scaricato un video, viene fornito anche il software proprietario (SmartPlayer), che consente sia della visione del video che anche la *conversione* in altri formati e possibilità di *screenshot*.

Esistono anche altri media player che consentono di vedere i video prodotti dal DVR come VLC, iSpy etc.

Per scaricare video dal web (senza la violazione dei diritti di autore), possiamo utilizzare innumerevoli strumenti e siti, oppure utilizzare lo strumento "ispeziona" del browser.

Ecco una lista di strumenti per il download, conversione e mediaplayer ed editing:



SmartPlayer

Download Video	Conversione Video	Media Player	Editing Video
Freemake.com	Uniconverter.Wondershare.it	VLC Media Player	Adobe Premiere
Online Video Converter.pro	video-converter.com	Dahua Smart Player	Wondershare Filmora
Save-from.net	Convertio.co	DVR Examiner 3	Sony Vegas
Save-from.com	Filmora.wondershare.ne	Azure Video Indexer	DaVinci Resolve
clipconverter.cc		AmpedFIVE DVRC - "pay"	Video Editing Software

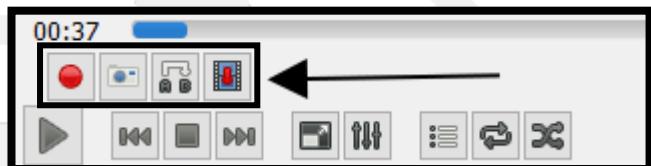
Suggerimenti

VLC

Molti strumenti (specie quelli di editing), hanno la possibilità di visualizzare le immagini per frame. Questo può essere molto utile per trovare il giusto momento in cui la qualità dell'immagine è migliore (magari un volto, una scritta o altro, si vedono in maniera più nittida). Lo troviamo nei media player e nei programmi di editing. In particolare è presente su VLC.



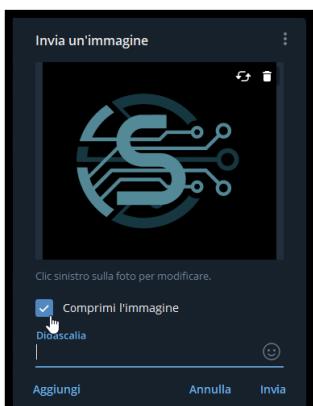
Frame di un video



Strumenti per la gestione dei frame in VLC

Condivisione Video

Quando dobbiamo condividere un file via internet, è sempre preferibile l'E-mail, in modo da contenere quelle che sono i formati originali del file (in questo caso i video), ma se vogliamo utilizzare le chat di messaggistica (Telegram, WhatsApp) per esempio, è importante non condividere il file come immagine normale, ma come un documento. In questo modo non vi è alcuna modifica da parte dell'applicazione a quelle che sono i formati e la risoluzione. Questo perché nel condividere il file, il software comprende modificando la qualità e la risoluzione dell'immagine/video cambiando anche il formato, in modo da essere più leggero e facilmente condivisibile.



Telegram



WhatsApp

PARTE 5

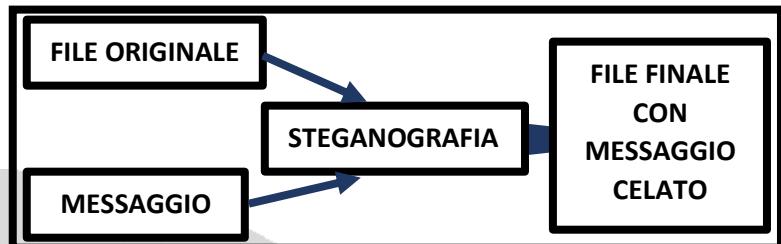
STEGANOGRADIA

La Steganografia⁸ è una tecnica di nascondere informazioni segrete all'interno di altre informazioni apparentemente innocue, come immagini, messaggi di testo, audio o video.

L'obiettivo è mantenere la segretezza delle informazioni trasmesse, rendendo difficile per eventuali osservatori indesiderati di rilevarne l'esistenza.

La steganografia è spesso utilizzata per scopi legittimi, come la protezione dei dati sensibili, ma può anche essere utilizzata per scopi illegali, come il trasferimento di informazioni confidenziali o attività di Cyber Crime.

La Steganografia può essere applicata:



- **Sulle Immagini**

La Steganografia su un'Immagine funziona nascondendo informazioni all'interno dei pixel dell'immagine stessa. Una delle tecniche, consiste nel modificare i bit meno significativi dei pixel in modo che corrispondano ai bit del messaggio da nascondere. In questo modo, le modifiche apportate all'immagine sono quasi impercettibili all'occhio umano, ma il messaggio è comunque contenuto nell'immagine.



- **Sulle Tracce Audio**

La Steganografia su un'Audio funziona nascondendo informazioni all'interno delle tracce audio. Una delle tecniche, consiste nel modificare i bit meno significativi dei campioni audio in modo che corrispondano ai bit del messaggio da nascondere. In questo modo, le modifiche apportate all'audio sono quasi impercettibili all'orecchio umano, ma il messaggio è comunque contenuto nell'audio.

- **Su file di testo.**

La Steganografia su un File funziona nascondendo informazioni all'interno di un file esistente, come un documento di testo. In questo caso, il messaggio viene codificato in modo che possa essere inserito in un file esistente senza alterarne la funzionalità.



Strumenti utili per creare ed rilevare le informazioni celate.

- | | | |
|------------------------------|---|--------------------------------|
| - OpenStego | - Steganos Security Suite | - Stegoveritas |
| - Stegosuite | - Stego Magic | - Stego-Tricks |
| - OutGuess | - QuickStego | |
| - S-Tools | - Stegsolve | |

⁸ Approfondimenti: <https://github.com/CScorza/StegoIntelligence>
<https://cert-aqid.gov.it/news/cose-la-steganografia/>

WATERMARK

Il Watermark⁹ (Letteralmente "*Filigrana*") è un'immagine o un testo trasparente sovrapposto a un'immagine o a un documento che funge da protezione del "copyright" o "identificativo della fonte". Il Watermark può essere utilizzato per prevenire la riproduzione non autorizzata o per identificare l'autore o la fonte di un'immagine o di un documento.

Protezione del copyright:

Il watermark può essere utilizzato per prevenire la riproduzione non autorizzata di un'immagine o di un documento.

Questo perché se qualcuno cerca di copiare o distribuire l'immagine o il documento, il watermark verrà automaticamente incluso nella copia, rendendo chiaro chi ne detiene il copyright.



Identificazione della fonte:

Il watermark può anche essere utilizzato per identificare l'autore o la fonte di un'immagine o di un documento.

Questo può essere utile se si vogliono tenere traccia delle fonti o per verificare che le informazioni siano accurate.



Protezione della qualità:

Il watermark può anche essere utilizzato per prevenire la manipolazione o la modifica non autorizzata di un'immagine o di un documento.

Questo perché se l'immagine o il documento viene modificato, il watermark verrà automaticamente alterato, rendendo evidente che la fonte originale è stata modificata.



Di seguito un elenco di Software Gratuiti ed a pagamento per inserire i Watermark.

Gratuiti:

- [uMark](#)
- [Watermark.ws](#)
- [Visual Watermark](#)
- [FastStone Photo Resizer](#)
- [Clipchamp](#)

A Pagamento

- [Adobe Photoshop](#)
- [Adobe Lightroom](#)
- [Adobe Premier](#)
- [CorelDRAW](#)
- [Watermark Factory](#)

Esempi pratici - Software Gratuiti

⁹ Approfondimento: <https://www.creativosonline.org/it/como-eliminar-marca-de-agua-photoshop.html>
<https://github.com/CScorza/WatermarkIntelligence>

	Immagini - uMark	Documento – Office Word	Video - Clipchamp
1	Scaricare e installare uMark sul computer.	Aprire il documento sul quale si desidera inserire il watermark.	Aprire il sito web di Clipchamp e selezionare "Editor" dalla barra dei menu.
2	Aprire il software e selezionare le immagini su cui si desidera inserire il watermark.	Fare clic sulla scheda "Layout" nella barra dei menu in alto.	Fare clic sul pulsante "Carica video" e selezionare il video su cui si desidera inserire il watermark.
3	Selezionare il tipo di watermark che si desidera utilizzare, come testo o immagine, e personalizzare il watermark utilizzando le opzioni disponibili.	Fare clic sul pulsante "Sfondo pagina" nella sezione "Pagina".	Dopo aver importato il video, fare clic sul pulsante "Testo" nella barra degli strumenti.
4	Regolare la posizione, l'opacità e la dimensione del watermark utilizzando le barre di scorrimento e i controlli disponibili.	Selezionare "Watermark" (Filigrana) dal menu a discesa.	Digitare il testo del watermark nella casella "Testo" e modificare il colore, il tipo di carattere, la dimensione, l'allineamento e altre impostazioni di formattazione come desiderato.
5	Eseguire un'anteprima del watermark sulle immagini selezionate per verificare che soddisfi i requisiti.	Selezionare il tipo di watermark che si desidera utilizzare, come "Testo" o "Immagine", e personalizzare il watermark utilizzando le opzioni disponibili.	Trascinare il watermark nella posizione desiderata sul video e regolare la trasparenza utilizzando la barra di scorrimento "Opacità".
6	Salvare le immagini con il watermark utilizzando il comando "Salva" o "Esporta" nel software.	Regolare la posizione, la trasparenza e la dimensione del watermark utilizzando le barre di scorrimento e i controlli disponibili.	Anteprima il watermark sul video per verificare che soddisfi i requisiti. Fare clic sul pulsante "Esporta" per scaricare il video con il watermark.

Guida all'inserimento del Watermark su Photoshop

1	Aprire l'immagine su cui si desidera inserire il watermark.
2	Creare un nuovo livello utilizzando il comando "Livello" nella barra dei menu in alto e selezionare "Nuovo livello".
3	Scegliere il tipo di watermark che si desidera utilizzare, come testo o immagine, e creare il watermark in questo livello.
4	Regolare l'opacità del livello del watermark se necessario utilizzando la barra di scorrimento Opacità nella finestra dei livelli.
5	Salvare l'immagine con il watermark utilizzando il comando "File" nella barra dei menu in alto e selezionando "Salva come". Assicurarsi di salvare come formato JPEG o PNG per mantenere la qualità dell'immagine originale e del watermark.



Software per rimuovere il Watermark

- [Remove.bg](#)
- [WatermarkRemover.io](#)

“AI” LA NUOVA FRONTIERA DELLE IMMAGINI FAKE

Negli ultimi anni l’Intelligenza artificiale sta sfornando decine di siti (Ultimo fra tutti ChatGPT -4) che con una serie di logaritmi riesce a riprodurre immagini (di paesaggi, persone, cose, luoghi etc), ma anche audio video e testi falsi.

Questo può diventare un problema per chi fa attività di web investigation, perché può cadere in inganno, trovandosi davanti un’informazione apparentemente veritiera.

La maggioranza di Hacker/Cracker utilizzano dei “sockpuppet” (Profili anonimi), per le loro attività di ricerca e criminali. Di conseguenza, anche gli Analisi OSINT utilizzano questi strumenti, ai fini di non lasciare traccia nel web durante le fasi investigative.

Di seguito vediamo alcune immagini create dall’intelligence artificiale e che sono state poi pubblicate nei post dei social network.



Questo ovviamente, diventa anche un problema di verità delle informazioni che vengono date su social network. La creazione di profili falsi, immagini false, sono un connubio perfetto per poi la diffusione di fakenews.

I principali siti che vedremo che realizzano questo tipo di immagini sono:

- [This person does not exist.com](https://thispersondoesnotexist.com)
- [OpenAI Dall-E 2](https://openai.com/dall-e-2)
- [Generated Photos](https://generated.photos)

Per proteggersi dal deepfake, occorre sviluppare tecniche avanzate di rilevamento delle immagini false (e negli argomenti precedenti ne abbiamo visti molteplici), non chè è importante informare ed educare gli utenti del web (ormai il 62.5% della popolazione mondiale ha accesso ad internet), su come riconoscere questo tipo di informazioni false.

In Italia non esiste un vero articolo legislativo sull’utilizzo dei deepfake¹⁰, ma esistono delle normative su casi specifici come l’art.494 del Codice Penale¹¹ (*Sostituzione di persona*) e l’art. 656 del Codice Penale¹² (*Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l’ordine pubblico*).

Inoltre, il Parlamento Europeo ha adottato una risoluzione (del 6 ottobre 2021 - (2020/2016(INI)))¹³ sulle misure da adottare per combattere l’abuso delle tecnologie di manipolazione audiovisiva e per prevenire l’uso fraudolento dei deepfake.

¹⁰ È una tecnica per la sintesi dell’immagine umana basata sull’intelligenza artificiale, usata per combinare e sovrapporre immagini e video esistenti con video o immagini originali, tramite una tecnica di apprendimento automatico. Wikipedia

¹¹ <https://www.brocaldi.it/codice-penale/libro-secondo/titolo-vii/capo-iv/art494.html>

¹² <https://www.brocaldi.it/codice-penale/libro-terzo/titolo-i/capo-i/sezione-i/art656.html>

¹³ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.pdf

LINEE GUIDA UTILI E TESTI CONSIGLIATI

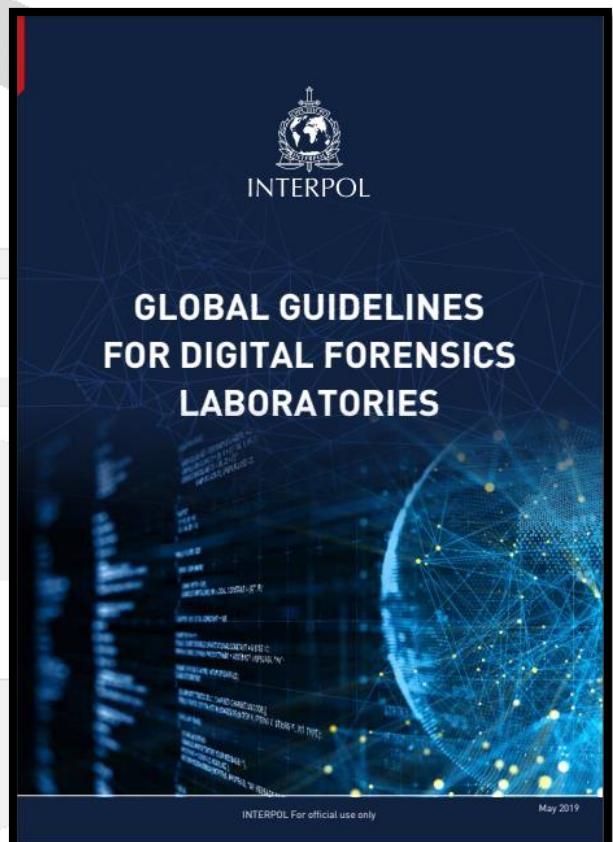
ENFSI

- [**Best Practice Manual for Facial Image Comparison**](#)
- [**Best Practice Manual for Forensic Image and Video Enhancement**](#)
- [**BPM for Digital Image Authentication**](#)



INTERPOL

- [**INTERPOL DFL Global Guidelines Digital Forensics Laboratory**](#)



CAPITOLO VIII

LINEE GUIDA PER L'AUTENTICAZIONE FORENSE DI IMMAGINI

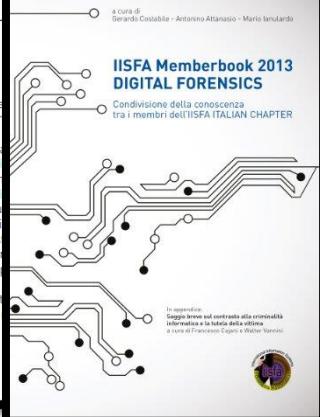
Sebastiano Battiatto - Fausto Galvan - Martino Jerian - Matteo Salcuni

Sommario:

1. Introduzione - 1.1 Un'immagine vale più di mille parole? - 2. La prova visiva - 2.1 Il Principio di Scambio di Locard - 2.2 Prova analogica e prova digitale - 2.3 Autenticità (ed integrità) di un'immagine digitale - 3. L'analisi forense di immagini - 4. Ricostruire la storia di un'immagine - 4.1 Formazione delle immagini digitali - 4.2 Un segno ad ogni passo - 4.3 Caratteristiche intrinseche della scena - 4.4 Tracce lasciate durante la fase di acquisizione - 4.5 Tracce lasciate dal software di elaborazione interno alla fotocamera - 4.6 Tracce lasciate dopo il primo salvataggio - 5. Modifica al contenuto informativo di un'immagine - 6. Linee guida per l'analisi di un'immagine digitale - 6.1 Analisi generale - 6.1.1 Analisi visiva dell'immagine - 6.1.2 Analisi generale del file - 6.2 Analisi dei metadati - 6.2.2 Analisi di thumbnail e preview - 6.2.3 Analisi del formato JPEG - 6.2.4 Analisi binaria - 6.3 Analisi globale dell'immagine - 6.3.1 Analisi dei coefficienti DCT - 6.3.2 Analisi della correlazione dei pixel - 6.3.3 Analisi di intensità e colori - 6.4 Identificazione del dispositivo - 6.4.1 Analisi globale del PRNU - 6.5 Analisi locale dell'immagine - 6.5.1 ELA - 6.5.2 Mappa DCT - 6.5.3 Mappa di probabilità - 6.5.4 Mappa del rumore - 6.5.5 Analisi locale del PRNU - 6.5.6 Analisi dei cloni - 6.6 Analisi dettagliata della scena - 6.6.1 Analisi dell'illuminazione - 6.6.2 Analisi della geometria - 6.7 Analisi conclusive - 7. Un caso di studio - 7.1 Analisi generale - 7.1.1 Analisi visiva dell'immagine - 7.1.2 Analisi generale del file - 7.2 Analisi del file - 7.2.1 Analisi di thumbnail e preview - 7.2.2 Analisi del formato JPEG - 7.2.3 Analisi binaria del file - 7.3 Analisi globale dell'immagine - 7.3.1 Analisi della correlazione dei pixel - 7.3.2 Analisi di intensità e colori - 7.4 Identificazione del dispositivo - 7.5 Analisi Locale - 7.5.1 ELA - 7.5.2 Mappa DCT - 7.5.3 Mappa di probabilità - 7.5.4 Mappa del rumore - 7.5.5 Analisi locale del PRNU - 7.5.6 Analisi dei cloni - 7.6 Analisi dettagliata della scena - 7.6.1 Analisi di un'immagine analogica - 8.1 Presenza del negativo - 8.2

1. INTRODUZIONE

Il numero di immagini create dai nostri dispositivi e sul web è in costante aumento. Nel 2008 il numero stellare nel mondo ammontava a circa 11 milioni, ci si attende che il loro numero sia più che triplicato caricate su YouTube circa 2,5 milioni di ore di accadimenti ripresi dagli utenti in ogni parte del mondo sono state inserite circa 300 milioni di fotografie di cui è evidente l'importanza crescente che la comunità assumerà, sia nel trasmettere sensazioni, ricordi e fissare un accadimento. È naturale quindi che queste modalità di fruizione dell'informazione abbiano delle applicazioni in ambito giudiziario [sia civile che penale]; è sempre vero che un evento delittuoso possa essere consumato del crimine o parte di essa venga ripresa da un solo soggetto prima, durante o dopo la commissione del



ISFAA MEMBERBOOK 2013 Digital Forensics

- Cap. VIII - [**LINEE GUIDA PER L'AUTENTICAZIONE FORENSE DI IMMAGINI**](#)

Bibliografia

- [Forensic Digital Image Processing: Optimization of Impression Evidence 1st Edition](#), scritto da Brian Dalrymple, Jill Smith (2021)
- [Crime Scene Photography.pdf](#), scritto da Edward M. Robinson (2010)
- [Multimedia Forensics \(Advances in Computer Vision and Pattern Recognition\) 1st ed. 2022 Edition](#), by Husrev Taha Sencar (Editor), Luisa Verdoliva (Editor), Nasir Memon (Editor)
- [Image and Video forensics](#) Irene Amerini, Gianmarco Baldini and Francesco Leotta , Eds. Published: January 2022
- [Dattiloscopia forense. Preventiva e giudiziaria a confronto.](#) Dall'identità personale all'evidenziazione e comparazione delle impronte di Nicola Caprioli (Autore), Silvestro Marascio (Autore)
- [Digital forensics](#) di Roberto Murenec Editore: Egaf Collana: Libri. Monografie Data di Pubblicazione: novembre 2021

Casi studio e Pubblicazioni prof. Sebastiano Battiato

- S. Battiato, G. Messina, R. Rizzo - [Image Forensics - Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive](#) - Chapter in IISFA Memberbook 2009 DIGITAL FORENSICS – Eds. G. Costabile, A. Attanasio – Experta, Italy 2009; (pdf)
- S. Battiato, G.M. Farinella, G. Messina, G. Puglisi – [Digital Video Forensics: Status e Prospettive](#) – Chapter in IISFA Memberbook 2010 DIGITAL FORENSICS – Eds. G. Costabile, A. Attanasio – Experta, Italy, 2010. (pdf)
- S. Battiato, G.M. Farinella, G. Puglisi – [Image/Video Forensics: Casi di Studio](#) - Chapter in IISFA Memberbook 2011 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio - Experta, Italy 2012; (pdf)
- S. Battiato, M. Moltisanti – [Tecniche di Steganografia su Immagini Digitali](#) - Chapter in IISFA Memberbook 2012 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio - Experta, Italy 2013; (pdf)
- S. Battiato, F. Galvan, M. Jerian, M. Salcuni– [Linee guida per l'autenticazione forense di immagini](#) - Chapter in IISFA Memberbook 2013 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio – Experta, Italy 2014; (pdf)
- S. Battiato, A. Catania, F. Galvan, M. Jerian, L.P. Fontana – [Acquisizione ed Analisi Forense di Sistemi di Videosorveglianza](#) - Chapter in IISFA Memberbook 2014 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio – Experta, Italy 2015 (pdf)
- S. Battiato, O. Giudice, A.B Paratore - ["Social" Image Forensics: Status e Prospettive](#) - Chapter in IISFA Memberbook 2016 DIGITAL FORENSICS - Eds. G. Costabile, A. Attanasio, M. Ianulardo - Edizioni In Magazine/Menabò Group, Italy 2016 (pdf)
- S. Battiato, G. M. Farinella, E. Messina, G. Puglisi - [Robust Image Alignment for Image Authentication and Tampering Detection](#) – IEEE Transactions on Information Forensics & Security, Vol. 7 – Issue 4, pp. 1105-1117, 2012; (pdf)
- S. Battiato, G. M. Farinella, G. Puglisi, D. Ravì – [Aligning Codebooks for Near Duplicate Image Detection – Multimedia Tools and Applications](#) - Vol.72, Issue 2, pp.1483-1506, 2014; (pdf)
- F. Galvan, G. Puglisi, A.R. Bruna, S. Battiato - [First Quantization Matrix Estimation from Double Compressed JPEG Images – IEEE Transactions on IEEE Transactions on Information Forensics & Security](#), Vol. 9, Issue 8, pp. 1299-1310, 2014. (pdf)
- S. Battiato, G. Messina – [Video Digitali in Ambito Forense – Ciberspazio e Diritto](#) – Mucchi Editore – Vol. 11, No 4, pp. 687-710, 2010. (pdf)
- S. Battiato, F. Galvan - [Introduzione alla Image/Video Forensics - Sicurezza e Giustizia](#) - Numero I/MMXIII - pp. 42-43 – 2013. (pdf)
- S. Battiato, F. Galvan - [La Validità Probatoria Delle Immagini e dei Video](#) - Sicurezza e Giustizia - Numero II/MMXIII - pp. 30-31 – 2013.(pdf)
- S. Battiato, F. Galvan - [Ricostruzione di Informazioni 3D a Partire da Immagini](#) - Sicurezza e Giustizia - Numero IV/MMXIII - pp. 38-40 – 2013.(pdf)
- S. Battiato, F. Galvan - [Verifica dell'Attendibilità di un Alibi Costituito da Immagini o Video](#) - Sicurezza e Giustizia - Numero II/MMXIV - pp. 47-50 – 2014. (pdf) ([pdf2](#))
- F. Rundo, E. Tusa, S.Battiato - [Medical Image Enhancement nei Procedimenti Giudiziari Medico-Legali in ambito Oncologico](#) - Sicurezza e Giustizia - Numero I/MMXVI - pp. 53-56 - 2016 (pdf)
- S. Battiato, G. Tessitore - [La Stima dell'Errore nella Determinazione dell'Altezza di un Sogetto](#) - Sicurezza e Giustizia - Numero 4/MMXVI - pp. 38-41 - 2016 (pdf)
- S. Battiato - [Investigare su Immagini e Video](#) - 2017 ([link](#), pdf)

Casi studio e Pubblicazioni Prof. Stefano Bistarelli

- [Steganografia.pdf](#)

Ringraziamenti

Questa piccolo contributo, non sarebbe stato possibile realizzare senza il supporto di molti.

Ad iniziare dalla mia Famiglia che mi ha sempre supportato nelle varie decisioni ai miei Colleghi per il supporto e la motivazione nel continuare la mia carriera professionale.

Ma anche e soprattutto ad OsintItalia, nella figura del suo presidente Mirko Lapi, che mi ha dato la possibilità di mettere al servizio dei soci dell'associazione la mia conoscenza sull'OSINT e sulla Digital Forensics.

Questa linea guida, come la precedente (Best Practices di Digital Forensics), nascono essenzialmente per divulgare e accrescere la conoscenza del mondo della forensics digitale e dell'intelligence a tutte quelle persone esperte del settore o a quelli che stanno muovendo i primi passi.

Si vede solo ciò che si osserva, e si osserva solo ciò che già esiste nella mente.

- Alphonse Bertillon

Dove c'è una grande volontà non possono esserci grandi difficoltà

- Nicolo Macchiavelli

CScorza

Analista OSINT e Multimedia Digital Forensics, socio di OSINTITALIA, ha aperto un profilo GitHub (“CScorza”), dove raccoglie tools e strumenti di OSINT, Digital Forensics e Cyber Security, e un Canale Telegram pubblico denominato CScorza “Indagini Telematiche”.