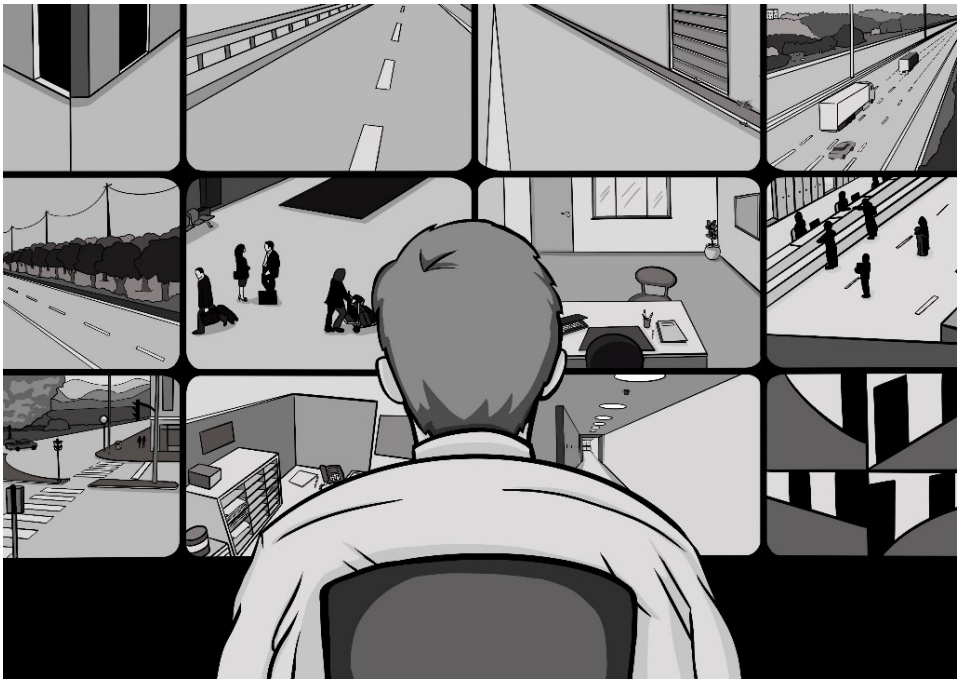
Concetti e Princìpi Fondamentali per l'Utilizzo delle Prove Video nell'Ambito della Pubblica Sicurezza e della Giustizia Penale

A cura di Martino Jerian, CEO e fondatore di Amped Software



Un insieme di concetti e princìpi in supporto all'operato delle istituzioni, delle Forze dell'Ordine e del sistema giudiziario, per un corretto utilizzo di immagini e video nell'ambito della pubblica sicurezza e della giustizia penale.

Prefazione

Video e foto fanno ormai parte di molti aspetti della nostra società. Diversi studi hanno dimostrato che le prove video sono fra le più significative fonti di informazione per investigatori, analisti e giudici. Nonostante la loro importanza, spesso questo tipo di prove non viene trattato con lo stesso rigore riservato ad altre prove scientifiche, come il DNA e le impronte digitali. Il video è uno dei principali strumenti per comprendere le dinamiche di un evento e identificarne gli autori, ma analizzarlo nel modo giusto - e interpretarlo correttamente – è meno semplice di quanto sembri.

Lo scopo di questo documento è quello di delineare alcuni princìpi molto importanti di cui dovrebbe essere a conoscenza chiunque faccia parte di un'organizzazione operante nella pubblica sicurezza o lavori all'interno del sistema giudiziario; ciò consentirebbe di ottenere migliori risultati durante le indagini, garantire un processo più equo e trasparente, e ridurre al minimo il rischio di errori in sede giudiziaria causati dall'uso improprio di immagini e prove video.
I princìpi che stiamo delineando in questo documento dovrebbero essere già ben noti ad analisti forensi e tecnici del settore. Tuttavia, una grande quantità di prove video viene gestita localmente da operatori e investigatori, che potrebbero non avere le competenze e le conoscenze tecniche di base per lavorare con questo tipo di prove per poi consegnarle correttamente al sistema giudiziario.
Un uso improprio di video ed immagini può comportare importanti ripercussioni sulla nostra sicurezza, dalla mancanza di dettagli rilevanti durante le attività operative fino alla scelta di seguire una pista errata durante le indagini; ci sono errori che potrebbero causare l'invalidazione di prove chiave in tribunale o addirittura la condanna della persona sbagliata.

Conoscere e seguire questi princìpi fondamentali porterà ad un Paese più sicuro, a processi equi e corretti dal punto di vista procedurale e ad un sistema giudiziario più veloce, efficiente e meno costoso.

PREFAZIONE **3**

DICHIARAZIONE UNIVERSALE DEI DIRITTI UMANI **7**

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA **8**

INTRODUZIONE **9**

SEZIONE ISTITUZIONALE **11**

Principali Problematiche e Rischi Relativi alle Prove Video **12**

1. Gestire prove video sembra semplice, ma è facile sbagliare 12
2. I formati video proprietari causano complicazioni nelle indagini e rischi per la sicurezza informatica 13
3. Spesso la qualità dell'immagine risulta scarsa: è importante migliorarla in modo corretto 14
4. Non sempre possiamo fidarci delle prove video: deepfake, manipolazioni e attribuzioni errate 15
5. Giudici e giurie: la facilità di essere fuorviati in ambito tecnico 16
6. L'impatto dell'Intelligenza Artificiale 17
7. Privacy e Sicurezza Informatica 18

Lavorare con le Prove Video nel Modo Corretto: 4 Concetti Fondamentali **19**

1. Consapevolezza e Formazione 19
2. Originalità e Acquisizione 19
3. Autenticazione e Verifica 19
4. Elaborazione Corretta e Trasparente 19

I vantaggi di lavorare correttamente con le prove video **20**

1. Miglioramento della sicurezza 20
2. Un miglior sistema giudiziario 20
3. Maggiore efficienza 20

SEZIONE TECNICA **21**

Parte A: Preparazione Tecnica **22**

1. Porsi domande e avere obiettivi specifici 22
2. Avere le competenze, la formazione e gli strumenti adeguati 22

Parte B: Acquisizione, Autenticazione e Verifica **23**

3. Acquisizione dei file originali 23
4. Convertire e visualizzare i file in modo preciso 24

5. Verificare l'integrità e l'autenticità dei file 25

Parte C: Elaborazione Corretta e Trasparente **26**

6. Concentrarsi sulle parti interessate dall'analisi 26
7. Identificare le problematiche dell'immagine e relative cause 27
8. Elaborare i file seguendo un workflow scientificamente valido 28
9. Utilizzare algoritmi appropriati per l'ambito forense 29
10. Applicare gli algoritmi seguendo il giusto ordine 30
11. Scegliere i parametri corretti 31
12. Seguire le linee guida 32

Parte D: Analisi e Presentazione **33**

13. Quantificare, quando possibile 33
14. Adottare tecniche di limitazione dei bias 34
15. Scrivere una relazione tecnica oggettiva e riproducibile 35
16. Presentare e spiegare il proprio lavoro in modo semplice, corretto ed efficace 36

CONCLUSIONI **37**

RIFERIMENTI **39**

L'Autore **39**

Amped Software **39**

Contatti **39**

Dichiarazione Universale dei Diritti Umani

Articolo 3
Ogni individuo ha diritto alla vita, alla libertà ed alla sicurezza della propria persona.

Articolo 6
Ogni individuo ha diritto, in ogni luogo, al riconoscimento della sua personalità giuridica.

Articolo 7
Tutti sono eguali dinanzi alla legge e hanno diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge. Tutti hanno diritto ad una eguale tutela contro ogni discriminazione che violi la presente Dichiarazione come contro qualsiasi incitamento a tale discriminazione.

Articolo 9
Nessun individuo potrà essere arbitrariamente arrestato, detenuto o esiliato.

Articolo 10
Ogni individuo ha diritto, in posizione di piena uguaglianza, ad una equa e pubblica udienza davanti ad un tribunale indipendente e imparziale, al fine della determinazione dei suoi diritti e dei suoi doveri, nonché della fondatezza di ogni accusa penale che gli venga rivolta.

Articolo 11
1. Ogni individuo accusato di un reato è presunto innocente sino a che la sua colpevolezza non sia stata provata legalmente in un pubblico processo nel quale egli abbia avuto tutte le garanzie necessarie per la sua difesa.
2. Nessun individuo sarà condannato per un comportamento commissivo od omissivo che, al momento in cui sia stato perpetuato, non costituisse reato secondo il diritto interno o secondo il diritto internazionale. Non potrà del pari essere inflitta alcuna pena superiore a quella applicabile al momento in cui il reato sia stato commesso.

Articolo 12
Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.

Articolo 28
Ogni individuo ha diritto ad un ordine sociale e internazionale nel quale i diritti e le libertà enunciati in questa Dichiarazione possano essere pienamente realizzati.

Carta dei Diritti Fondamentali dell'Unione Europea

Articolo 6
Diritto alla libertà e alla sicurezza
"*Ogni persona ha diritto alla libertà e alla sicurezza*."

Articolo 8
Protezione dei dati di carattere personale
1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 13
Libertà delle arti e delle scienze
"Le arti e la ricerca scientifica sono libere. La libertà accademica è rispettata."

Articolo 20
Uguaglianza davanti alla legge
"Tutte le persone sono uguali davanti alla legge."

Articolo 21
Non discriminazione
1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.

Articolo 47
Diritto a un ricorso effettivo e a un giudice imparziale
Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato, qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.

Introduzione

Data la presenza ormai universale dei sistemi di videosorveglianza, la popolarità degli smartphone e l'uso diffuso dei social network, oggi le immagini e i video sono una delle principali fonti di prova durante le indagini in ambito penale[1] [2]. È molto raro indagare su un crimine in cui non siano coinvolti in qualche modo foto o video digitali. Nessun altro tipo di prova può rispondere così frequentemente a tutte le domande del cosiddetto "metodo investigativo 5WH"[3]: *who*, *where*, *what*, *when*, *why*, and *how,* ovvero *chi*, *dove*, *cosa*, *quando*, *perché* e *come*.

La questione principale, dal punto di vista della sicurezza pubblica e della giustizia, è che questo tipo di prove spesso non viene gestito con la stessa cura e lo stesso rigore riservati a prove di diversa natura. Le prove video sembrano facili da interpretare, ma in realtà sono molto suscettibili di errori. Senza una corretta procedura, le competenze e gli strumenti adeguati, c'è il rischio di condurre le indagini nella direzione sbagliata o di avere delle prove che non reggono il minuzioso esame di un'aula di tribunale.

Dal momento che non sappiamo cosa non conosciamo, il primo passo per affrontare un problema è quello di rendere le persone consapevoli di averne uno. A tal fine, questo documento è stato suddiviso in due sezioni: la prima sezione è specificamente rivolta alle istituzioni e a tutti coloro che operano in ambito di pubblica sicurezza e giustizia, per renderli consapevoli di alcuni importanti concetti che dovrebbero prendere in considerazione quando si tratta di casi in cui figurano video e immagini come fonti di prova; la seconda sezione si rivolge, invece, ai professionisti in materia di analisi forense di immagini e video e contiene i princìpi veri e propri. Con il termine *professionista* si intende qualsiasi individuo con ruoli, responsabilità e competenze diverse, che lavora con prove video e immagini. Esperti e analisti dovrebbero già conoscere bene la maggior parte dei princìpi (sia che si tratti di membri delle Forze dell'Ordine, di altre agenzie governative o di operatori del settore privato), mentre tali concetti possono suonare più nuovi al personale operativo, investigatori e agenti delle unità territoriali. Questi princìpi sono infatti particolarmente importanti per i ruoli meno specializzati: solitamente essi hanno infatti molti altri compiti, tecnici e non, ma sono a tutti gli effetti coloro che hanno a che fare con le prove video mentre operano in prima linea.

Un'ultima parola per quanto riguarda la terminologia: il campo di cui scriviamo viene chiamato in una varietà di modi, con sfumature simili ma leggermente diverse: analisi forense di immagini/video, analisi forense multimediale, prove digitali multimediali (DME) o semplicemente prove video. In letteratura, la definizione più usata è la seguente: "L'analisi forense di video è l'esame scientifico, il confronto e/o la valutazione del video in materia legale."[4] Di seguito, useremo i termini *immagine* o *video* indifferentemente, poiché normalmente un video è considerato una sequenza di immagini, eventualmente con una componente audio aggiuntiva, o metadati come marche temporali (*timestamp*) o localizzazioni GPS.

[1] **Ashby, M.P.J. The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. Eur J Crim Policy Res 23, 441–459 (2017). https://doi.org/10.1007/s10610-017-9341-6**

[2] **https://pure.southwales.ac.uk/ws/portalfiles/portal/3994343/HIFS_Project_Research_Insight_3._The_Use_of_CCTV_during_Homicide_Investigations_Contributions_Challenges_and_Risks_April_2020_.pdf**

[3] **Stelfox, Peter. (2013). Criminal Investigation: An Introduction to Principles and Practice. 10.4324/9781315880730.**

[4] **https://www.swgde.org/glossary**

I concetti e i princìpi che seguono saranno descritti da una frase riassuntiva e da una spiegazione più dettagliata a introduzione del tema e delle relative problematiche.

SEZIONE ISTITUZIONALE

PER AUTORITÀ, ORGANIZZAZIONI DI PUBBLICA SICUREZZA E SISTEMA GIUDIZIARIO

Principali Problematiche e Rischi Relativi alle Prove Video

1. Gestire prove video sembra semplice, ma è facile sbagliare

Chiunque può premere "Play" o scaricare una foto sul proprio PC e cercare di interpretarla. Proprio a causa di queste "barriere all'ingresso" molto basse, coloro che hanno a che fare con le prove video potrebbero non avere la giusta preparazione tecnica o gli strumenti adeguati, senza però esserne consapevoli.

Il processo di generazione delle immagini digitali è costituito da molteplici passaggi, molti dei quali sconosciuti ai più. La maggior parte di questi passaggi influenza il modo in cui la realtà viene rappresentata nel video. Di seguito vedremo alcuni esempi; si prega di notare che si tratta di problematiche molto comuni, non di eccezioni:

- La tipica "immagine in bianco e nero" creata dalle telecamere di sorveglianza in modalità "visione notturna" **non contiene alcuna informazione sul reale colore** degli oggetti: **una camicia a scacchi in genere appare perfettamente uniforme** in queste immagini in scala di grigi[5].

- Gli obiettivi delle telecamere di sorveglianza causano una distorsione dell'immagine; un **soggetto immortalato può sembrare quindi molto più alto e magro** di quanto non sia in realtà. Inoltre, ogni misurazione estrapolata da un video risulterà errata se la distorsione non viene presa in considerazione[6].

- La conversione da telecamere analogiche a registratori digitali spesso presenta proporzioni errate (nello specifico, la proporzione tra l'altezza e la larghezza del video). Se questo aspetto non viene correttamente gestito, **un SUV può apparire nel video come una limousine[7]**.

- Un'elevata compressione video può rimuovere i dettagli presenti sulla scena del crimine: questo potrebbe causare la **scomparsa di una cicatrice dal volto di qualcuno**. Allo stesso tempo, la compressione può anche introdurre artefatti digitali che potrebbero essere erroneamente considerati dettagli reali: può, ad esempio, **aggiungere facilmente un neo sul volto di un sospettato[8]**.

Risulta quindi facile comprendere che anche uno solo degli artefatti menzionati, se non correttamente individuato e corretto, può condurre un'indagine nella direzione sbagliata e portare anche all'arresto di un innocente. Naturalmente, questi artefatti si sommano durante il processo di generazione, di conseguenza una prova video risulta spesso molto più lontana dalla realtà degli eventi di quanto possiamo immaginare, specie quando si parla di dettagli molto minuti.

[5] https://blog.ampedsoftware.com/2021/01/19/infrared-dont-trust-the-colors-of-most-cctv-footage-at-night/
[6] https://blog.ampedsoftware.com/2021/02/02/lens-distortion-cameras-may-change-the-shape-of-things/
[7] https://blog.ampedsoftware.com/2021/01/26/aspect-ratio-be-sure-your-image-is-not-stretched-in-either-direction/
[8] https://blog.ampedsoftware.com/2021/04/13/compression-artifacts-hiding-or-adding-details-to-the-scene/

2. I formati video proprietari causano complicazioni nelle indagini e rischi per la sicurezza informatica

La maggior parte dei dispositivi di sorveglianza registra video in formati proprietari non riproducibili da software standard. Anche la mera riproduzione di tali video è un compito impegnativo, spesso frustrante per agenti e professionisti. Se i video vengono "convertiti" nel modo sbagliato, la qualità e l'affidabilità delle prove possono essere gravemente compromesse.

La stragrande maggioranza dei file provenienti da sistemi di videosorveglianza sono in formato proprietario. Ciò significa che, di solito, non si tratta di normali file MP4 o AVI che possono essere facilmente riprodotti con dei software standard come Windows Media Player o VLC, ma deve essere utilizzato un player software creato dal produttore stesso del sistema. Molto spesso, questi player sono di bassa qualità, presentano delle problematiche significative e sono totalmente inadeguati per poter effettuare un'analisi forense del video.

Per poter analizzare dei video, il più delle volte i file proprietari devono essere convertiti. Questa è un'altra fase critica; una conversione eseguita senza la giusta attenzione, infatti, può facilmente comportare i seguenti problemi[9]:

- **Perdita di integrità dei file,** con un inevitabile impatto sulla catena di custodia, che deve essere garantita per ogni tipo di prova. Una conversione errata porterà a lavorare con dati che non rappresentano una prova affidabile.
- **Perdita di qualità:** se, come parte della conversione, il video subisce anche una ri-compressione, questo può causare una notevole perdita di qualità.
- **Perdita di metadati e informazioni** sulla codifica originale, come l'orario preciso dei vari fotogrammi e il tipo di compressione applicata a diverse parti dell'immagine; informazioni che potevano risultare preziose per valutare l'affidabilità del contenuto visivo.

Inoltre, la ricerca e l'utilizzo di player proprietari può causare non pochi problemi dal punto di vista della sicurezza informatica e della gestione dei sistemi informativi.

Una cattiva gestione delle prove video è solitamente più pericolosa della cattiva gestione di altri tipi di prove forensi. Per esempio, quando un campione biologico non è conservato correttamente, l'analisi del DNA può diventare impossibile e ciò implica la perdita di potenziali prove. Se un video non viene gestito correttamente, potrà comunque raggiungere il tribunale, ma è probabile che **mostri una versione alterata degli eventi**. Fortunatamente, è solitamente più facile implementare una adeguata catena di custodia per le prove video che per le prove fisiche.

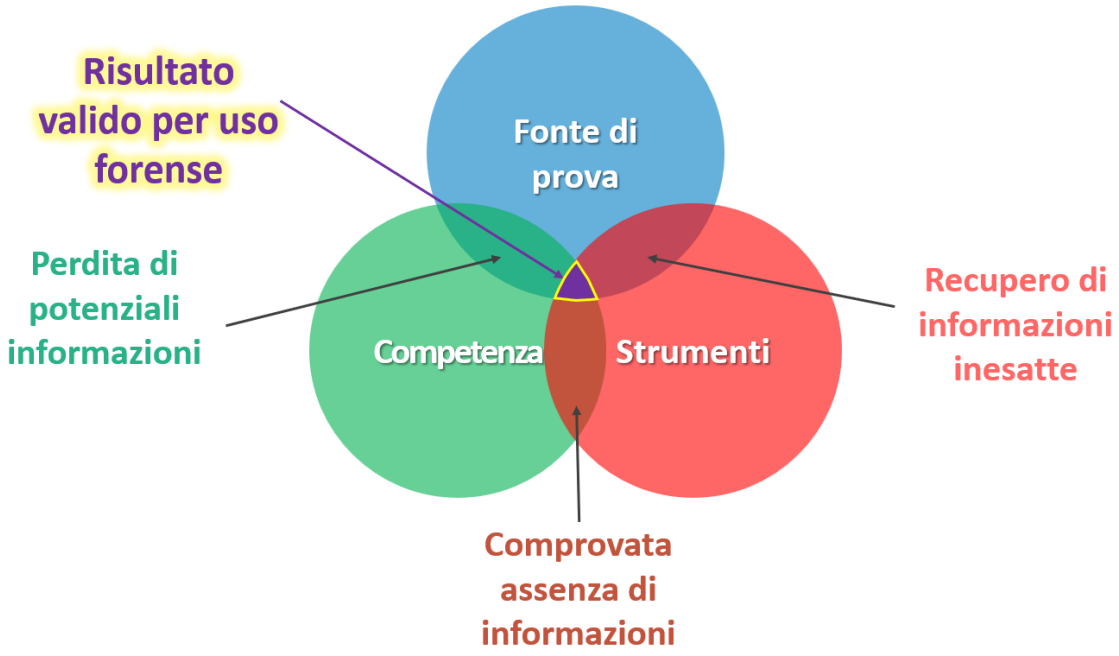
Negli Stati Uniti, c'è stato un caso, ad esempio, in cui un agente è stato accusato di **aver spinto un soggetto arrestato contro un muro**, sulla sola base della registrazione di sorveglianza. È poi emerso che, a causa di una conversione errata, la **velocità di riproduzione è stata cambiata** per quella porzione di video e l'agente si era comportato in realtà nella maniera corretta.

[9] **https://blog.ampedsoftware.com/2021/03/16/proprietary-cctv-dvr-players-often-not-showing-the-original-pixels/**

3. Spesso la qualità dell'immagine risulta scarsa: è importante migliorarla in modo corretto

Le prove video spesso non presentano la qualità sufficiente per poter ottenere le informazioni necessarie, ad esempio per identificare una persona o un veicolo. Tuttavia, utilizzando gli strumenti giusti, le tecniche corrette e potendo disporre delle adeguate condizioni tecniche, il video può essere migliorato con risultati eccellenti.

Anzitutto è fondamentale capire che un buon risultato nell'analisi forense è sempre la combinazione di tre elementi, nessuno dei quali è facoltativo: **fonte di prova, competenza e strumenti**. Questo concetto è chiaramente raffigurato nel seguente diagramma:



L'elaborazione deve essere effettuata in modo attento e **rigoroso**, utilizzando metodologie applicabili in ambito forense e **scientificamente validate**, altrimenti le prove potrebbero essere escluse durante il processo. Il miglioramento video in ambito forense **non dovrebbe mai creare nuove informazioni**, dovrebbe piuttosto rendere disponibili le informazioni già esistenti.

Secondo una ricerca condotta da Amped Software attraverso un sondaggio sottoposto agli utenti nel 2021[10], il miglioramento video può produrre risultati utili in circa il 50% dei casi.

[10] **https://blog.ampedsoftware.com/2022/02/15/a-survey-on-video-evidence-the-highlights-from-the-amped-user-days-2021/**

4. Non sempre possiamo fidarci delle prove video: deepfake, manipolazioni e attribuzioni errate

Siamo cresciuti in un mondo in cui vedere era credere, ma negli ultimi due decenni si sono diffuse tecniche di manipolazione che creano falsi visivamente verosimili. Quando si valuta l'ammissibilità di un'immagine come fonte di prova, è importante chiedersi: "È autentica?". Autenticità significa che l'immagine è una rappresentazione accurata di ciò che raffigura.

L'autenticazione di immagini e video sta ormai diventando una questione della massima importanza. Ultimamente, i notiziari ci mostrano ovunque la presenza di **deepfakes**, ovvero immagini manipolate o create ex-novo utilizzando tecniche di intelligenza artificiale. I deepfakes possono essere usati come mezzo per **rovinare la reputazione di un politico**, ad esempio creando un video in cui dice cose che non ha mai detto, oppure per creare **falsi contenuti a sfondo sessuale**, tipicamente sostituendo il volto di un attore di film per adulti con quello di un altro soggetto. I deepfake sono stati utilizzati anche nella guerra russo-ucraina nel 2022 per ordinare ai soldati ucraini di arrendersi utilizzando le fattezze del loro capo di Stato[11].

Nella realtà, tuttavia, è ancora più comune incontrare delle **contraffazioni "standard",** create usando dei software di fotoritocco. Possono essere utilizzati per **creare un falso alibi**, per mettere in atto **frodi assicurative**, ecc.
Non è nemmeno necessario modificare un'immagine per utilizzarla in modo fraudolento: può essere sufficiente riutilizzare una foto fatta in un momento completamente diverso, o inscenare un dato evento e affermare che sia accaduto. Tutto questo è molto più facile da realizzare di un deepfake o anche di una manipolazione con software come Photoshop.

Per tutti questi motivi, è importante **valutare l'attendibilità di un'immagine** prima di ammetterla come fonte di prova.

[11] **https://www.youtube.com/watch?v=X17yrEV5sl4**

5. Giudici e giurie: la facilità di essere fuorviati in ambito tecnico

Le problematiche poste dalle prove video non devono essere sottovalutate: se del caso, si dovrebbero chiamare periti o consulenti esperti nel settore. Tuttavia, è spesso difficile per giudici, giurie e, in generale, soggetti non tecnici, valutare le competenze tecniche e l'affidabilità di tali figure. Pertanto, è importante valutare il loro contributo nel modo più obiettivo possibile.

Come spiegato in precedenza, l'analisi forense di immagini e video è una **disciplina complessa, piena di insidie.** Non si può ragionevolmente supporre che giudici e giurie abbiano le competenze tecniche per comprendere nel dettaglio tutto ciò che si cela dietro un'analisi di questo tipo. Dovrebbero tuttavia comprendere che l'analisi video deve essere trattata con la stessa cautela con cui viene trattata ogni altra disciplina in ambito forense.
Il "buon senso" da solo, senza un'adeguata preparazione tecnica, non dovrebbe essere ammesso come criterio valido, così come non verrebbe preso in considerazione se si trattasse di DNA, impronte digitali o analisi tossicologiche.

La presentazione di prove video è una questione importante. Per questo, quando devono essere presentate, dovrebbero essere rese disponibili delle attrezzature adeguate e dovrebbe essere evitato qualsiasi aggiustamento "al volo" per presentare le prove, poiché spesso ciò influisce negativamente sulla ripetibilità del risultato presentato. Ad esempio, anche un semplice "zoom" sul filmato presentato dovrebbe essere fatto solo da un professionista qualificato.

6. L'impatto dell'Intelligenza Artificiale

L'elaborazione delle prove video tramite IA deve essere gestita con estrema cautela. L'uso dell'IA per migliorare le immagini spesso crea nuove immagini, il cui processo di generazione non può essere spiegato nemmeno da un esperto.

L'intelligenza artificiale sta influenzando molti aspetti della nostra vita e rappresenta certamente un importante impulso per lo sviluppo tecnologico. Le recenti tecnologie IA, come le reti neurali profonde (*deep neural networks)*, offrono prestazioni eccezionali quando vengono utilizzate per migliorare o analizzare immagini e video. Tuttavia, nonostante i notevoli sforzi prodotti dalla comunità scientifica, **si ritiene che i risultati ottenuti con queste tecniche siano ancora difficili da spiegare.** Queste reti neurali tendono ad agire come delle efficienti ed efficaci **scatole nere**, il che significa che anche gli esperti in materia (e gli stessi sviluppatori di software) non possono spiegare la logica che sta dietro il risultato finale.

Se si vuole rimanere fedeli al principio, finora indiscusso, per cui **qualsiasi risultato prodotto come parte di un'analisi forense dovrebbe essere spiegabile e ripetibile**, allora l'IA non dovrebbe essere utilizzata per attività di miglioramento video forense ai fini di un utilizzo probatorio (ad esempio, super-risoluzione del viso, miglioramento dell'immagine di una targa, rimozione del rumore, ecc.)[12]. Si potrebbe valutare di utilizzare queste tecniche al solo fine investigativo, avendo cura di prevenirne l'utilizzo a fini probatori e minimizzando i rischi connessi alla potenziale inaffidabilità e all'introduzione di precondizionamenti (bias).

L'intelligenza artificiale potrebbe essere presa in considerazione, invece, per l'analisi video (ad esempio, per rilevare contenuti relativi ad abusi su minori, ricercare il volto di un sospettato in un database di volti, ecc.). Tuttavia, è necessario mettere in atto alcune misure di sicurezza: bisogna conoscere le prestazioni del sistema utilizzato; la decisione finale dovrebbe essere sempre presa da un esperto; si dovrebbero adottare delle tecniche di attenuazione del condizionamento (*bias*) per evitare che l'esperto sia eccessivamente influenzato dal sistema di IA.

Le considerazioni di cui sopra sono motivate da requisiti riconosciuti storicamente per quanto riguarda i metodi di analisi forense e dal fatto che la maggior parte delle tecniche di miglioramento tramite IA non sono ad oggi spiegabili. In futuro, nuove politiche potrebbero portare anche una diversa sensibilità per quanto riguarda tali requisiti, così come tecniche di IA più esplicabili.

[12] **https://blog.ampedsoftware.com/2021/10/05/can-ai-be-used-for-forensics-and-investigations/**

7. Privacy e Sicurezza Informatica

Lavorare entro i limiti posti dalle normative sulla privacy è un aspetto molto importante che deve essere preso in considerazione anche dalle Forze dell'Ordine. Poiché vengono trattate delle informazioni sensibili, software e sistemi utilizzati dovrebbero essere sicuri, per quanto possibile.

Esiste un conflitto naturale tra la necessità di acquisire il maggior numero possibile di dati durante le indagini, il loro **uso dal punto di vista forense e le considerazioni da fare sulla privacy**. In buona parte del mondo, si sta assistendo sempre di più all'adozione di inquadramenti sulla privacy sempre più severi, che in genere seguono le orme del GDPR europeo. Fatte salve alcune eccezioni, lavorare all'interno del sistema giudiziario non esenta dal rispetto di tali regolamentazioni.

Inoltre, la sicurezza informatica è un aspetto molto importante. Le indagini e le analisi forensi sono, per loro stessa natura, contesti delicati, dove i dati e la sicurezza devono essere presi estremamente sul serio. Il software e i sistemi operativi dovrebbero sempre essere protetti, in modo da **evitare perdite di informazioni sensibili** e non consentire ad hacker e aggressori esterni di alterarle.

Lavorare con le Prove Video nel Modo Corretto: 4 Concetti Fondamentali

Le problematiche sopra menzionate possono essere risolte. È necessario creare consapevolezza e cultura sull'argomento a 360 gradi, quindi attraverso l'intera catena di gestione e fruizione della fonte di prova.

Una volta assodato che le prove video non dovrebbero essere date per scontate, ma gestite con metodo scientifico e molta attenzione, nasce il bisogno di creare programmi di sensibilizzazione per tutti i livelli del sistema giudiziario. Non è necessario, né raccomandato, che tutti gli agenti di polizia, gli avvocati e i giudici diventino tecnici forensi, ma è essenziale creare una base culturale che permetta di comprendere l'importanza e la delicatezza del video come fonte di prova.

Quali sono i concetti principali?

1. Consapevolezza e Formazione

È necessario educare gli utenti e il pubblico alla complessità e alle insidie che si nascondono dietro le prove video. Offrire alle persone che operano in questo campo un breve programma di formazione di poche ore, per aprire gli occhi di fronte a concetti attualmente sconosciuti alla maggior parte delle persone.

2. Originalità e Acquisizione

Tutti gli operatori del settore dovrebbero comprendere l'importanza di una corretta acquisizione del materiale digitale. Troppo spesso vediamo filmati di videosorveglianza acquisiti erroneamente filmando lo schermo con uno smartphone. Una corretta acquisizione dovrebbe essere seguita da una rigorosa catena di custodia, al fine di garantire l'accesso alle prove originali e la condivisione di ogni azione intrapresa in merito. Questo garantirebbe la migliore qualità possibile e ridurrebbe il rischio di rigetto delle prove in tribunale.

3. Autenticazione e Verifica

Verificare l'integrità del file (è originale e inalterato?) e stabilire se i suoi contenuti sono attendibili. Inoltre, questo processo dovrebbe essere in grado di verificare l'effettiva correttezza dell'acquisizione.

4. Elaborazione Corretta e Trasparente

Adozione di linee guida chiare per l'elaborazione, che prevedano l'uso di algoritmi validati dalla comunità scientifica e l'adozione di un flusso di lavoro corretto, ripetibile e riproducibile. Ci sono diverse linee guida

di ottima qualità disponibili, come quelle pubblicate da **ENFSI**[13], **SWGDE**[14], **OSAC**[15] e **FSR**[16]. Dovrebbero essere seguite e adottate da un numero sempre crescente di professionisti e addetti ai lavori.

I vantaggi di lavorare correttamente con le prove video

Lavorare correttamente su immagini e video, tenendo in considerazione i concetti menzionati nella sezione precedente e seguendo nello specifico i princìpi ulteriormente enunciati in questo documento, comporta diversi vantaggi che possono migliorare molti aspetti della nostra società.

1. Miglioramento della sicurezza

Seguire procedure corrette e ben definite permette di semplificare il flusso di lavoro, invece di reinventare la ruota ogni volta. Anche se è vero che ogni caso è diverso, le problematiche e gli obiettivi di un'indagine sono spesso molto simili: la maggior parte delle volte, lo scopo dell'analisi è identificare una persona, un veicolo, o capire le dinamiche di un dato evento. Lavorare nel modo corretto permette altresì di risolvere più crimini e quindi **migliorare il livello di sicurezza delle nostre città e dei nostri Paesi**.

2. Un miglior sistema giudiziario

Utilizzando i dati originali, valutandone l'autenticità e l'integrità e gestendoli nel modo corretto, i tribunali possono migliorare la loro capacità di valutazione e quindi ammettere le prove video in quanto attendibili per l'accertamento dei fatti. In questo modo possiamo **garantire processi più equi e ridurre la percentuale di errori giudiziari.**

3. Maggiore efficienza

Fare le cose nel modo giusto non richiede più tempo, anzi comporta un flusso di lavoro più efficiente. Questo significa **meno tempo** speso dal personale e **meno problemi** causati da prove mal gestite.

[13] **https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/**
[14] **https://www.swgde.org/documents/published-complete-listing**
[15] **https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-standards-and-guidelines**
[16] **https://www.gov.uk/government/publications/video-analysis-codes-of-practice-for-forensic-service-providers**

SEZIONE TECNICA

PER OPERATORI

E PROFESSIONISTI

CHE LAVORANO

CON LE PROVE VIDEO

Parte A: Preparazione Tecnica

1. Porsi domande e avere obiettivi specifici

Cosa fare: *assicurarsi che obiettivi e quesiti siano chiaramente definiti prima di iniziare qualsiasi lavoro.*
Cosa non fare: *non iniziare ad analizzare un video senza avere già uno scopo chiaro, e non accettare richieste generiche come "cercare informazioni interessanti" o "migliorare la qualità".*
Rischi: *perdita di tempo ed eventuale introduzione di bias e preconcetti nell'analisi video.*

Analizzare un'immagine o un video costituisce solo un mezzo per arrivare ad un fine. È necessario, perciò, sapere cosa stiamo cercando. Non ha senso "migliorare" un'immagine senza uno scopo chiaro in mente. La maggior parte delle volte, l'elaborazione di un'immagine fornisce un'altra immagine, meno piacevole da vedere a livello globale, ma più chiara nei punti in cui si trovano le informazioni pertinenti. Ad esempio, se miglioriamo una targa, spesso perdiamo qualità in altre parti dell'immagine.
Generalmente, le due richieste più comuni durante l'analisi video sono legate all'identificazione (tipicamente di una persona o di un veicolo) e alla ricostruzione e comprensione di una sequenza di eventi.
Seguire questo principio permette di condurre l'analisi nella giusta direzione, di perdere meno tempo e di ottenere un risultato migliore. Come possiamo rispondere a una domanda se non sappiamo cosa stiamo cercando?

2. Avere le competenze, la formazione e gli strumenti adeguati

Cosa fare: *l'analisi video dovrebbe essere presa sul serio, come qualsiasi altra indagine tecnica. Si dovrebbero avere le competenze e gli strumenti adeguati per adempiere ai compiti richiesti.*
Cosa non fare: *non eseguire un compito a cui non si è preparati e, se non è possibile rifiutare, evidenziare chiaramente i rischi che ne derivano.*
Rischi: *perdere troppo tempo, condurre l'indagine nella direzione sbagliata e potenzialmente presentare delle prove che verranno invalidate in tribunale.*

Una prova video sembra facile da capire perché si tratta di qualcosa che tutti possono vedere, ma sotto la superficie si nascondono molti concetti complessi, di tipo tecnico e matematico. Infatti, l'elaborazione delle immagini è, in definitiva, la visualizzazione di operazioni matematiche.
Le persone che hanno a che fare con questo tipo di prove dovrebbero avere le giuste competenze tecniche e ricevere la formazione necessaria per i loro ruoli (come investigatori, tecnici e analisti). Inoltre, molti strumenti di uso comune, come player standard o editor di immagini preposti a funzioni creative, mancano del rigore e della trasparenza necessaria per le applicazioni forensi, mancano di alcune funzioni fondamentali o rendono le cose più complicate di quanto dovrebbero essere. Spesso espongono inutilmente l'operatore e le prove stesse a dei rischi, utilizzando metodologie e strumenti totalmente inappropriati per l'ambito forense.

Parte B: Acquisizione, Autenticazione e Verifica

3. Acquisizione dei file originali

Cosa fare: *assicurarsi di ottenere la miglior prova possibile, che idealmente è la versione originale di un filmato.*
Cosa non fare: *non analizzare immagini e video inviati via e-mail, scaricati da social media, app di messaggistica, acquisiti tramite screenshot o schermate di un monitor, a meno che non ci sia davvero nessun altro modo per ottenere file migliori o originali.*
Rischi:
- non essere in grado di recuperare dettagli fondamentali che si sarebbero potuti ottenere analizzando un file originale;
- perdita di metadati importanti (come la misurazione del tempo e i dati del GPS);
- introduzione nella catena di custodia di prove inaffidabili (che possono comportare il rigetto delle prove stesse in sede di giudizio).

Il lavoro di analisi dovrebbe iniziare dai file video originali, il che è più facile a dirsi che a farsi. La maggior parte dei filmati di videosorveglianza utilizzati durante le indagini, infatti, proviene da telecamere a circuito chiuso (in inglese "CCTV – Close-Circuit-TeleVision") collegate a piccoli dispositivi a basso costo chiamati DVR (da "Digital Video Recorder" - videoregistratore digitale)[17]. Questi sistemi offrono diverse opzioni di esportazione per recuperare i filmati. La maggior parte dei DVR supporta una combinazione di formati proprietari e formati standard. L'errore più comune, durante l'acquisizione di filmati CCTV, è quello di esportarli in un formato conosciuto, ma pur sempre convertito, come AVI, MOV o MP4[18]. È essenziale invece recuperare il filmato originale, in qualsiasi formato esso sia stato generato. Inoltre, immagini e video provenienti da dispositivi mobili vengono spesso convertiti già nel momento in cui vengono condivisi con varie applicazioni o trasferiti su un PC.
Se i file non vengono acquisiti con la procedura corretta, ci troviamo di fronte a due problemi significativi:

a) dal punto di vista forense e giudiziario**, rompiamo la catena di custodia**, che è fondamentale perché qualsiasi tipo di prova sia accettabile e accettata;
b) potremmo **causare una perdita di informazioni e/o di qualità**, oltre che una **perdita di metadati originali** che possono contenere informazioni fondamentali per il caso, come ad esempio nomi di videocamere, misurazioni del tempo, dati GPS, impostazioni, tipo di compressione e così via.

Va detto che non è sempre possibile ottenere il file originale: a volte potrebbe essere stato cancellato, danneggiato o semplicemente non disponibile, soprattutto quando si ha a che fare con dati provenienti dal cloud o dai social media. Tuttavia, anche in questo caso, si dovrebbe fare attenzione a ottenere il file più vicino possibile all'originale o perlomeno con la migliore qualità e, quando necessario, saper fornire una giustificazione del perché non sia stato possibile utilizzare l'originale.
Nel peggiore dei casi, che purtroppo accade più spesso di quanto dovrebbe, si riceve un video proveniente da telecamere a circuito chiuso che è stato acquisito filmando il monitor del sistema di sorveglianza con un telefono cellulare. In questo caso non si tratta più di una "prova", bensì di un *video della prova*. È come fare un'analisi balistica sulla foto di un proiettile anziché sul proiettile stesso. Il file

[17] **https://blog.ampedsoftware.com/category/cctv-acquisition**
[18] **https://blog.ampedsoftware.com/2023/03/28/cctv-recovery**

digitale originale costituisce la prova, non solo il suo contenuto visivo. Ci sono moltissime informazioni utili che non sono visibili a occhio nudo.

4. Convertire e visualizzare i file in modo preciso

Cosa fare: *convertire e visualizzare i file conservando i dati originali, per quanto possibile, e prevenire ulteriori perdite di qualità.*
Cosa non fare: *non fidarsi ciecamente dei player proprietari CCTV/DVR e dei file esportati dagli stessi. Non acquisire un video dal sistema, o peggio ancora, filmare il monitor di un sistema di videosorveglianza con un telefono cellulare, a meno che non sia assolutamente l'ultima risorsa.*
Rischi:
- non essere in grado di recuperare dettagli fondamentali che si sarebbero potuti ottenere analizzando un file originale;
- perdita di metadati importanti (come la misurazione del tempo e i dati del GPS);
- introduzione nella catena di custodia di prove inaffidabili (che possono comportare il rigetto delle prove stesse in sede di giudizio).

Come illustrato in precedenza, quando si parla di video provenienti da sistemi CCTV, la maggior parte delle volte i file originali sono in un formato proprietario (non sono dunque semplici file AVI, MOV o MP4). Questi file devono essere riprodotti utilizzando un software specifico, fornito dal produttore del sistema stesso, oppure devono essere convertiti per renderli compatibili con altri player o software di elaborazione.
Ci sono centinaia, se non migliaia, di formati e player diversi sul mercato. Spesso questi sistemi non sono adeguati ad un'analisi forense del video e, anche quando vengono forniti strumenti di esportazione, la conversione può causare una perdita di qualità e altri problemi[19].
Una conversione e visualizzazione dei file accurata e rigorosa può essere realizzata da coloro che hanno una buona conoscenza in ambito video forense oppure utilizzando degli specifici software di applicazione forense, che possano elaborare i file con precisione. Purtroppo, ci sono casi in cui il video non può essere esportato, o viene esportato in maniera non corretta; quindi, l'unica possibilità è quella di utilizzare un altro software per acquisire ciò che viene visualizzato sullo schermo durante la riproduzione. Questa dovrebbe tuttavia essere considerata l'ultima risorsa, poiché la probabilità di introdurre errori è molto alta: il risultato dipende dalla precisione di riproduzione del player, dalla capacità del sistema di cattura di evitare fotogrammi duplicati o mancanti e dalle impostazioni di compressione. In ogni caso, il risultato sarà un file significativamente diverso dall'originale, anche se il contenuto visivo potrebbe risultare abbastanza simile, se acquisito correttamente.

[19] **https://blog.ampedsoftware.com/2021/03/16/proprietary-cctv-dvr-players-often-not-showing-the-original-pixels**

5. Verificare l'integrità e l'autenticità dei file

Cosa fare: *copiare i file seguendo una procedura forense (come confrontare i codici hash), valutare possibili indizi che suggeriscano la non-originalità del file (ad esempio, un video proveniente da un sistema CCTV in formato AVI è probabile che non sia originale) e prendere in considerazione possibili tracce di manipolazione.*
Cosa non fare: *non copiare i file senza verificare l'origine e la destinazione della copia e non fidarsi ciecamente del contenuto.*
Rischi:

- *avviare l'analisi su file che non sono stati copiati o acquisiti nel modo corretto, causando quei problemi di qualità e integrità evidenziati in precedenza;*
- *utilizzare prove inaffidabili.*

Una volta ottenuti i file da visualizzare ed analizzare, è importanti chiedersi se essi possano essere ritenuti attendibili. Questo richiede due diversi tipi di analisi: verifica dell'integrità ed autenticazione[20].

La verifica dell'integrità (o originalità) è il processo di conferma che i dati presentati *sono completi e sono rimasti inalterati dal momento dell'acquisizione*. Di solito questa verifica può essere eseguita abbastanza facilmente confrontando un codice hash sicuro (un identificatore univoco) della prova originale con la copia di lavoro.
L'autenticazione, invece, è il processo eseguito per comprovare che *i dati sono una rappresentazione accurata di ciò che viene rappresentato*.
Qual è la differenza tra integrità e autenticità? Lo spiegheremo con un'analogia. Un vero passaporto è un documento originale e autentico. Se ne facciamo una fotocopia, non si tratterà più dell'originale, ma finché i dati che raffigura sono corretti, il contenuto è autentico. D'altra parte, il passaporto contraffatto di una persona che non esiste può essere prodotto "in originale," - fisicamente parlando - ma non è autentico.
Una foto manipolata, in cui un soggetto è stato rimosso dall'immagine, non è un'immagine originale né autentica. D'altra parte, se insceniamo un evento e scattiamo una foto per fingere che sia successo, potremmo avere una foto originale, ma che non è autentica.

In alcuni casi, il focus dell'analisi può essere proprio la determinazione dell'integrità e dell'autenticità di un video o di un'immagine. Tuttavia, questo è un passaggio fondamentale che deve essere fatto, anche a un livello meno approfondito, in qualsiasi caso riguardante immagini e video. Potrebbe essere semplice, come chiedersi se c'è qualche ragione per non credere che il video sia originale e che possiamo fidarci del suo contenuto. Ad esempio, se acquisiamo un video proveniente da un sistema CCTV in formato standard, e non in formato proprietario, molto spesso non è stato acquisito nel modo descritto nel principio numero 3. Dovremmo quindi chiederci: "Come mai?" e "Possiamo ancora ottenere l'originale?". D'altra parte, se un'immagine viene fornita da una persona coinvolta in un'indagine, si dovrebbe valutare attentamente il grado di attendibilità di quella prova.

[20] **https://www.swgde.org/glossary**

Parte C: Elaborazione Corretta e Trasparente

6. Concentrarsi sulle parti interessate dall'analisi

Cosa fare: *acquisire dati a sufficienza nella fase iniziale, quindi identificare le parti rilevanti per l'indagine e concentrarsi su quelle.*
Cosa non fare: *non analizzare ed elaborare l'intero filmato disponibile, se questo non contiene informazioni utili, a meno che non sia stato esplicitamente richiesto.*
Rischi:

- *lavorare sull'intero filmato, anche quando non contiene informazioni utili, può causare un enorme spreco di tempo e risorse;*
- *elaborazione e analisi non ottimali su parti rilevanti per le indagini.*

Il più delle volte, sembra di cercare un ago in un pagliaio. Possiamo raccogliere ore di video da più videocamere, alla ricerca di un soggetto o di un evento che dura solo pochi fotogrammi. Questa procedura può essere facile e veloce, o lunga e difficile, a seconda dei casi.
Per gli operatori è difficile mantenere attenzione e concentrazione su video o immagini per ore intere, alla ricerca di alcuni piccoli dettagli. Esistono software specializzati per vagliare grandi moli di dati: se da un lato questo può essere di grande aiuto, dall'altro si rischia di non rilevare eventi o dettagli importanti (soprattutto se la qualità è bassa), o essere condizionati da troppi falsi allarmi. In definitiva, convalidare un risultato e ritenerlo affidabile è responsabilità di chi opera con questi sistemi semi-automatizzati, che deve accertarsi che tutte le informazioni chiave siano state correttamente identificate.
Una volta identificati i punti di interesse, è importante focalizzare l'attenzione su di essi e individuare il miglior metodo di elaborazione per quei punti specifici. Infatti, un metodo che può essere ottimale per l'intero video potrebbe non essere il più indicato per le specifiche porzioni che ci interessano.

7. Identificare le problematiche dell'immagine e relative cause

Cosa fare: *prima di compiere qualsiasi azione, è necessario analizzare e comprendere le eventuali problematiche tecniche legate alla qualità che interessano le immagini.*
Cosa non fare: *non elaborare immagini senza avere una chiara comprensione dei problemi da risolvere.*
Rischi:

- *un miglioramento che risulta non ottimale o addirittura una qualità peggiore dell'originale, che potrebbe introdurre artefatti indesiderati;*
- *la mancanza di una spiegazione adeguata che giustifichi l'elaborazione potrebbe far sì che le prove vengano respinte in tribunale.*

Spesso il video non sarà in grado di rispondere immediatamente a tutte le nostre domande. Identificare i problemi e capire se e come possiamo affrontarli è una delle parti più complicate e più importanti dell'analisi. Nella maggior parte dei casi, le problematiche riguardano la qualità dell'immagine, ma non solo.

Di seguito un elenco non esaustivo di alcuni problemi tipici riscontrati in immagini e video digitali[21].

- **Bassa risoluzione spaziale** dei dettagli rilevanti: numero di pixel insufficiente nell'area di interesse.
- **Bassa risoluzione temporale**: una bassa frequenza dei fotogrammi (*frame rate*) può far sì che alcuni eventi brevi non siano rappresentati nel video.
- **Compressione di immagini e video**: può causare una perdita di dettagli e generare artefatti.
- **Sfocatura**: il punto o l'area in cui un'immagine appare sfocata o "sporcata" da soggetti in rapido movimento.
- **Rumore**: variazioni casuali o periodiche dei valori dei pixel, spesso visibili come "grana" nelle immagini con scarsa illuminazione.
- **Forte distorsione prospettica:** rende difficile la visualizzazione dei dettagli da una forte angolazione.
- **Distorsione ottica**: fa apparire le linee rette come curve, soprattutto con le lenti utilizzate nelle ottiche grandangolari.
- **Problemi di luminosità**, contrasto e colore: causa colori non attendibili, immagini troppo scure o troppo luminose, oppure scarsa visibilità dei dettagli.
- **Distorsione delle proporzioni**: il rapporto tra la larghezza e l'altezza dell'immagine risulta errato, facendo apparire i soggetti schiacciati e, di conseguenza, con proporzioni sbagliate.
- **Interlacciamento**: un retaggio dei sistemi analogici che provoca un effetto "pettine".
- **Problemi di temporizzazione**: velocità di riproduzione errata o informazioni di temporizzazione non affidabili.
- **Altre problematiche**: fotogrammi mancanti o duplicati, artefatti causati dal tipo di sensore (ad es. *rolling shutter*), errori di decodifica e così via.

Tipicamente, molti di questi problemi sono presenti in una forma o nell'altra, quindi è importante capire quali possono e devono essere corretti. Infatti, ci sono problemi che in determinate condizioni possono essere corretti seguendo la procedura adeguata (come un video scuro o sfocato) e altri che invece non è possibile correggere (come la conversione di un video a infrarossi in colori chiari e visibili).

[21] **https://blog.ampedsoftware.com/2022/09/13/the-image-generation-model-cheat-sheet-included**

8. Elaborare i file seguendo un workflow scientificamente valido

Cosa fare: *per tutti i casi a cui si lavora, definire, documentare e utilizzare un flusso di lavoro corretto, ripetibile e riproducibile.*
Cosa non fare: *non elaborare i file senza un approccio sistematico.*
Rischi: *non poter spiegare cosa è stato fatto e perché o, peggio ancora, non essere in grado di replicare nuovamente la stessa analisi con i medesimi passaggi.*

Una volta compresi i problemi che riguardano l'immagine e lo scopo dell'analisi, possiamo procedere a lavorare sui file. Il miglioramento dell'immagine è una parte importante dell'elaborazione, anche se non è l'unica, ed è importante ricordare che si tratta solo di un mezzo per raggiungere un fine. Ci si deve quindi preoccupare maggiormente di ottenere informazioni utili e fruibili da un video, piuttosto che di avere un'immagine visivamente gradevole.
Quando elaboriamo i file, è necessario tenere a mente che stiamo maneggiando delle prove; quindi, il flusso di lavoro deve seguire una metodologia scientificamente valida che rispecchi questi princìpi[22]:

a) **Accuratezza**: i procedimenti dovrebbero essere il più possibile accurati e privi di errori e, se possibile, l'errore dovrebbe essere quantificabile. I metodi dovrebbero essere basati sulla ricerca scientifica, per quanto possibile, in modo che gli strumenti e le tecniche siano il più possibile privi di *bias* e contribuiscano a limitare il precondizionamento dell'operatore.
b) **Ripetibilità**: si dovrebbe essere in grado di ripetere l'analisi in qualsiasi momento ottenendo gli stessi risultati. Se ogni volta si ottiene un risultato diverso, c'è evidentemente un serio problema.
c) **Riproducibilità**: il metodo scientifico esige che, seguendo la procedura documentata, una terza persona adeguatamente qualificata sia in grado di riprodurre i risultati ottenuti dall'analisi in qualsiasi momento.

Una delle domande più comuni è: "*Come posso giustificare alla Corte il fatto di aver elaborato un'immagine usata come prova?*" La risposta è in realtà molto semplice: comprendendo come vengono introdotti i difetti e correggendoli, possiamo ottenere una *rappresentazione più fedele della scena* (o di soggetti e oggetti di interesse) rispetto alle immagini originali.

Un esempio molto semplice è la distorsione dell'immagine introdotta dagli obiettivi grandangolari: le pareti diritte nell'immagine appaiono curve, a causa delle caratteristiche ottiche della fotocamera. Poiché le pareti reali sono diritte e non curve, la correzione della distorsione consente di produrre un'immagine che è una rappresentazione più affidabile della realtà**.**

[22] **https://blog.ampedsoftware.com/2021/10/05/can-ai-be-used-for-forensics-and-investigations/**

9. Utilizzare algoritmi appropriati per l'ambito forense

Cosa fare: *utilizzare solo metodologie e strumenti che risultino accettabili in un contesto giudiziario: dovrebbero essere spiegabili da un professionista competente, validati, deterministici e non introdurre dati esterni al caso che potrebbero influenzare i risultati.*
Cosa non fare: *non utilizzare algoritmi, strumenti o metodologie che non soddisfino i requisiti di cui sopra, non importa quanto promettenti siano i potenziali risultati. Ad esempio, gli algoritmi di miglioramento dell'immagine basati sull'intelligenza artificiale (IA) di solito non sono appropriati per fini probatori.*
Rischi:

- *condurre le indagini nella direzione sbagliata;*
- *confidare troppo in risultati che sembrano chiari ma non sono affidabili;*
- *errori e distorsioni dei risultati;*
- *invalidazione delle prove in tribunale a causa dell'uso di una metodologia inaffidabile.*

Le metodologie e gli algoritmi che usiamo in ambito forense dovrebbero seguire i princìpi di accuratezza, ripetibilità e riproducibilità presentati in precedenza. Altrimenti, come può qualsiasi procedimento forense essere rispettato nella pratica? I professionisti dovrebbero fare affidamento su algoritmi con le seguenti caratteristiche:

a) **Esplicabili**: gli algoritmi devono poter essere comprensibili e spiegabili da un professionista competente. Dato il contesto critico in cui si svolge il lavoro, è necessario comprendere il funzionamento generale degli algoritmi per superare le potenziali limitazioni proprie delle tecniche di "*black-box testing*" utilizzate per valutare l'accuratezza di tali algoritmi.

b) **Validati**: se possibile, gli algoritmi dovrebbero essere stati accettati dalla comunità scientifica. Ad esempio, molte tecniche sono state pubblicate in una rivista scientifica o in una pubblicazione accademica dopo *peer review*. Se tale riferimento non è disponibile, può essere accettabile una spiegazione dettagliata del funzionamento, che consenta una validazione indipendente.

c) **Deterministici**: per garantire la loro ripetibilità e riproducibilità, gli algoritmi utilizzati non dovrebbero avere componenti casuali. Nel caso di algoritmi che necessitano di un numero casuale all'interno del loro processo computazionale, una possibile soluzione è quella di fissare o documentare il seme del generatore di numeri casuali, al fine di ottenere lo stesso risultato ogni volta che un operatore esegue l'analisi.

d) **Assenza di dati esterni:** l'output dovrebbe basarsi solo su una combinazione tra i dati di input e l'algoritmo, senza dati esterni al caso in esame che potrebbero influenzare l'elaborazione. Si noti che questo è molto importante sia a livello algoritmico che a livello umano nella successiva analisi.

In generale, attenersi a questi punti dovrebbe consentire di lavorare in modo valido dal punto di vista forense. Se alcuni dei requisiti non venissero rispettati, l'ammissibilità dell'elaborazione potrebbe essere messa in dubbio. Ad esempio, è attualmente in corso una discussione sull'applicabilità di algoritmi basati sull'intelligenza artificiale (IA) per alcune applicazioni forensi. Infatti, le tecniche di IA presentano diverse criticità per quanto riguarda la comprensibilità e i *bias* introdotti dai dati utilizzati per l'addestramento della rete.

10. Applicare gli algoritmi seguendo il giusto ordine

Cosa fare: *identificare le anomalie che devono essere corrette, capire l'ordine in cui tali difetti vengono introdotti e correggerli seguendo l'ordine inverso.*
Cosa non fare: *non applicare le correzioni nell'ordine sbagliato e non esagerare, non correggere cioè i difetti quando non influiscono sull'analisi richiesta.*
Rischi: *a seconda delle problematiche e degli algoritmi utilizzati, il procedimento potrebbe essere formalmente errato o causare più danni che benefici all'immagine. Situazioni che potrebbero essere facilmente risolte applicando le correzioni nel giusto ordine, potrebbero rivelarsi impossibili se tale ordine non viene seguito.*

Durante l'elaborazione dei file, ci sono solitamente più problemi da correggere, ognuno nel giusto ordine. Per farlo, dobbiamo capire il **modello di generazione dell'immagine**[23].

Il modello di generazione dell'immagine rappresenta una comprensione concettuale di come la luce, proveniente da una scena nel mondo reale, viene catturata dalla fotocamera, convertita in un'immagine e, nel caso di un'immagine (o video) digitale, salvata come una sequenza di zeri e uni.

In ogni fase del processo, ci sono delle limitazioni tecniche che introducono alcune differenze tra quella che sarebbe una visione ideale della realtà e la rappresentazione che otteniamo dal processo di imaging.

[23] https://blog.ampedsoftware.com/2022/09/13/the-image-generation-model-cheat-sheet-included/

Il filmato con cui stiamo lavorando è quindi il prodotto di una lunga catena di acquisizione ed elaborazione, che di solito introduce diversi difetti nell'immagine. Il modo più logico per compensare questi difetti è agire in **ordine inverso**[24].
Comprendere il modello che sta dietro al caso specifico e capire quale difetto viene introdotto in ogni fase è la chiave per migliorare l'immagine seguendo un metodo scientifico.

11. Scegliere i parametri corretti

Cosa fare: *dopo un adeguato esame, scegliere i parametri più logici e più performanti per la configurazione di un algoritmo di elaborazione.*
Cosa non fare: *non usare impostazioni errate o imprecise.*
Rischi: *usare gli algoritmi giusti con i parametri sbagliati può comunque causare risultati non ottimali o addirittura un risultato visivamente peggiore dell'originale.*

Usare gli algoritmi corretti nel giusto ordine non è tuttavia sufficiente. Il risultato dell'applicazione di un algoritmo cambia drasticamente a seconda dei parametri utilizzati. È necessario definire attentamente le impostazioni dell'algoritmo utilizzato, che possono essere uniche per una data immagine, al fine di avere il giusto risultato. Se si applica una correzione della distorsione dell'obiettivo o una riduzione della sfocatura con un parametro che non riflette le caratteristiche di quello specifico difetto, probabilmente si otterrà un'immagine molto peggiore dell'originale, o addirittura fuorviante.

Di solito si raccomanda di fare pratica e sperimentare algoritmi e strumenti su alcuni dati di riferimento di cui si conosce già la base di partenza e di arrivo, al fine di comprendere come diversi parametri influenzino il risultato finale in un ambiente controllato.

[24] **https://blog.ampedsoftware.com/2019/07/11/amped-five-filter-order-its-better-to-get-it-right**

12. Seguire le linee guida

Cosa fare: *utilizzare delle linee guida riconosciute a livello internazionale o seguire le procedure operative definite nella propria organizzazione.*
Cosa non fare: *non tentare di reinventare la ruota. Anche se ogni caso può essere diverso, la maggior parte si può ricondurre ad alcune situazioni abbastanza standard e quindi dovrebbero essere affrontate in modo coerente.*
Rischi:

- *non seguire quella che è universalmente riconosciuta come la metodologia adeguata;*
- *dedicare troppo tempo alla ricerca e alla sperimentazione della strategia giusta;*
- *lavorare su casi simili in modi completamente diversi (o avere diversi operatori che si affrontano lo stesso caso in maniera diversa), sollevando così dubbi sul modo corretto di lavorare;*
- *rendere più complicato e inaffidabile il lavoro svolto dagli esperti della controparte in tribunale.*

I princìpi enunciati nel presente documento forniscono una panoramica degli argomenti più importanti quando si lavora con le prove video, ma esistono diverse linee guida, disponibili a livello nazionale e internazionale, che dovrebbero essere più ampiamente seguite e adottate. Alcuni esempi, come già accennato in precedenza, sono quelli di **ENFSI**[25], **SWGDE**[26], **OSAC**[27] e **FSR**[28].
Diverse linee guida forniscono una quantità diversa di dettagli, a seconda del loro target di riferimento, ma di solito rappresentano un ottimo punto di partenza per molti campi di applicazione, in quanto promosse dalle comunità di esperti in ambito forense, scientifico o legale.

Sfortunatamente, spesso queste linee guida non sono molto conosciute o adottate, il che può portare i professionisti a rallentare il loro lavoro mentre cercano di "reinventare la ruota". Sulla base di queste linee guida, è spesso opportuno scrivere procedure operative standard specifiche per la propria organizzazione, che consentano a tutti i membri di seguire le stesse metodologie.

[25] https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/
[26] https://www.swgde.org/documents/published-complete-listing
[27] https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-standards-and-guidelines
[28] https://www.gov.uk/government/publications/video-analysis-codes-of-practice-for-forensic-service-providers

Parte D: Analisi e Presentazione

13. Quantificare, quando possibile

Cosa fare: *cercare di misurare e quantificare il risultato dell'analisi con un margine di errore o un intervallo di fiducia, quando è possibile e quando ha senso.*
Cosa non fare: *non limitarsi a "descrivere" qualcosa qualitativamente quando è possibile misurarlo.*
Rischi: *non quantificare qualcosa di oggettivamente misurabile può dare adito a diverse interpretazioni, essere più soggetto ad errori e sollevare dubbi in tribunale.*

Quando si lavora su immagini e video, si è tentati di descrivere ciò che si vede, piuttosto che misurarlo oggettivamente. Ma a causa di diversi fattori tecnici e umani, è spesso difficile quantificare e stimare oggettivamente qualcosa, a meno che non venga misurato. Molte illusioni ottiche mostrano quanto facilmente i nostri sensi possano essere ingannati. Un esempio tipico è la percezione errata di dimensioni e distanze a causa della prospettiva[29].

Quando possibile, è meglio quindi misurare qualcosa e fornire un **margine di errore o un intervallo di fiducia** ad esso correlato. Ad esempio, piuttosto che dire che due immagini sembrano simili, bisognerebbe documentare matematicamente la loro differenza con elementi descrittivi noti (come *SAD*, *SSIM* o *MSE*). È possibile identificare e correggere vari problemi di luminosità, contrasto e colore di un'immagine osservando il suo istogramma e aggiustando correttamente i valori. L'altezza dei soggetti e la velocità dei veicoli possono essere stimate numericamente, piuttosto che qualitativamente.
Anche se questo non è sempre possibile, e a volte possono essere necessarie anche delle stime qualitative, la loro natura soggettiva rende tali valutazioni meno facili da motivare e sostenere, rispetto a degli oggettivi valori numerici.

[29] **https://blog.ampedsoftware.com/2021/02/09/perspective-size-comparison-may-be-tricky**

14. Adottare tecniche di limitazione dei bias

Cosa fare: *assicurarsi di ricevere solo le informazioni strettamente necessarie per l'analisi; evitare che terzi condividano dettagli che potrebbero influenzare il lavoro.*
Cosa non fare: *non chiedere ad altri quali sono i loro risultati prima di aver effettuato la propria analisi.*
Rischi: *lavorare ad un caso su cui si hanno troppe informazioni può facilmente influenzare chi se ne occupa, introducendo un precondizionamento che può condurre l'analisi verso un risultato sbagliato, o meno accurato.*

Il fattore umano rappresenta un aspetto critico dell'analisi di prove video. Uno dei maggiori problemi è limitare i precondizionamenti umani durante l'interpretazione di tali prove. Come già affermato, anche solo essere consapevoli del rischio è un buon inizio.

Per iniziare, è molto importante che chi lavora ad un caso non abbia precondizionamenti e **riceva solo le informazioni tecniche strettamente necessarie per svolgere il proprio lavoro**, eventualmente rifiutando di ricevere qualsiasi altra informazione. È molto facile, infatti, essere "troppo coinvolti" in un caso e cercare istintivamente conferma delle proprie convinzioni. Questo può accadere, e spesso accade, perché siamo esseri umani. Anche senza alcun secondo fine, la nostra mente utilizza abitualmente i preconcetti come scorciatoia in situazioni difficili e complesse.

Un caso tipico è quello di chiedere ad un collega di verificare una targa, fornendo già la sequenza di caratteri che ci aspettiamo di identificare. Specialmente quando l'intelligibilità è bassa, è molto facile essere influenzati e leggere quello che ci aspettiamo di vedere. Questo fenomeno viene chiamato bias di conferma.

Le targhe sono solo la punta dell'iceberg: per esempio, il riconoscimento facciale è un ambito ancora più labile. Quando si migliora il viso di una persona, un'elaborazione diversa da quella adeguata può facilmente portare a un aspetto del volto significativamente diverso. Pertanto, è fondamentale che l'operatore che elabora il video si astenga dal guardare in anticipo il volto della persona sospettata, altrimenti, potrebbe tendere a impostare inconsciamente i valori necessari a renderla compatibile (o viceversa, naturalmente).

Inoltre, i professionisti del settore dovrebbero essere consapevoli dei possibili **precondizionamenti che il sistema può innescare nell'utente umano**, e adottare le misure adeguate a evitarli o quantomeno ridurli. Se si nota una forte corrispondenza proveniente da un sistema automatico (basato su IA o su tecniche "tradizionali") per una possibile identificazione, è probabile che si tenderà verso una corrispondenza positiva. È possibile però che il volto corretto sia stato erroneamente scartato dal sistema, e che quindi l'operatore lo abbia ignorato. A questo proposito, è importante non solo educare il professionista sui limiti della tecnologia e sul modo in cui può condizionare la percezione e opinione umana durante l'analisi, ma anche adottare tecniche per limitare i precondizionamenti, come il protocollo LSU (*Linear Sequential Unmasking*)[30].

[30] **Dror IE, Kukucka J. Linear Sequential Unmasking-*Expanded* (LSU-*E*): A general approach for improving decision making as well as minimizing noise and bias. Forensic Sci Int Synerg. 2021 Aug 13;3:100161. doi: 10.1016/j.fsisyn.2021.100161. PMID: 34466797; PMCID: PMC8385162.**

15. Scrivere una relazione tecnica oggettiva e riproducibile

Cosa fare: *rispondere a tutte le domande poste e solo a quelle, attenersi ai fatti e non uscire dalle proprie aree di competenza. Richiedere l'aiuto di un esperto per questioni che esulano dalle proprie competenze.*
Cosa non fare*: non fornire informazioni non richieste, opinioni personali o commenti.*
Rischi*: risultati errati, una relazione tecnica scientificamente inaffidabile e l'esposizione in tribunale al rischio di domande non inerenti al proprio ambito di competenza, potenzialmente invalidando il lavoro svolto.*

Il prodotto del lavoro su una prova video è solitamente costituito da un'immagine o un file video, una relazione tecnica e talvolta una presentazione da mostrare in sede dibattimentale.
In questo contesto, **è importante rimanere focalizzati su quanto è stato richiesto**; questo significa tre cose:

1) **Rispondere alle domande poste**. Se si notano altre cose interessanti, potrebbe essere necessario informare il richiedente, ma senza un quadro completo del caso, è meglio generalmente attenersi a ciò che è stato richiesto.
2) **Attenersi ai fatti**. Mostrare i dati e ciò che è stato espressamente definito nei quesiti, senza esprimere opinioni personali, a meno che non venga richiesto e, in tal caso, assicurarsi che ciò rientri nel proprio ruolo.
3) **Rimanere nella propria area di competenza**. Essere esperti di immagini o video non significa essere esperti anche del contenuto delle immagini. Non si dovrebbero realizzare confronti su un'automobile o su un volto, a meno di non possedere anche quella competenza specifica. Su questo punto, diverse giurisdizioni hanno regole più o meno rigide ma, in generale, è sempre meglio richiedere l'aiuto di un esperto in materia per questioni che esulano dalle proprie competenze specifiche.

La relazione dovrebbe essere sufficientemente dettagliata per consentire a terzi (con le giuste competenze e gli strumenti adeguati) di esaminarla e di replicare l'analisi in modo autonomo. Infatti, si dovrebbe essere in grado di elaborare i dati originali seguendo il procedimento descritto nella relazione, per poi ottenere in maniera indipendente dei risultati compatibili.

16. Presentare e spiegare il proprio lavoro in modo semplice, corretto ed efficace

Cosa fare: *presentare i fatti in modo oggettivo e cercare di trovare il giusto equilibrio tra la correttezza tecnica ed una spiegazione del lavoro svolto comprensibile in termini comuni.*
Cosa non fare: *non entrare troppo in dettagli tecnici, a meno che non sia richiesto, ma non semplificare eccessivamente la spiegazione al punto di dire qualcosa di non corretto, che può essere usato a proprio svantaggio.*
Rischi: *non presentare in modo efficace il lavoro svolto o in modo pedante e troppo complicato può renderlo incomprensibile limitandone o addirittura ribaltandone l'utilità. Al contrario, semplificare eccessivamente può esporre ad attacchi durante il controinterrogatorio.*

Aver eseguito un lavoro tecnicamente eccellente serve a poco, se non si è in grado di **presentarlo nel modo corretto.** Giudici, avvocati, procuratori, giurie e il pubblico di solito hanno poche conoscenze scientifiche e tecniche. Tuttavia, si dovrebbe essere in grado di spiegare le cose correttamente e in termini semplici e comprensibili.

Spesso è difficile per i soggetti sopra **menzionati valutare la capacità tecnica e l'affidabilità dei vari testimoni, consulenti e periti**. Supponiamo che una delle parti faccia un'analisi corretta e molto prudente. La controparte, che è stata invece meno attenta per quanto riguarda le varie procedure forensi, si produce in un discorso molto più d'impatto, magari fornendo un risultato dell'analisi opposto. Spesso basta questo per gettare dubbi sull'analisi precedentemente presentata, anche se si trattava di quella corretta. Senza un minimo di formazione e competenza scientifica e tecnica, questo è un problema molto difficile cui far fronte.

Spesso, la capacità di comunicare è molto più impattante dell'effettiva correttezza dell'analisi.

Nella fase di presentazione ci possono essere anche altri aspetti da considerare. Un fattore importante è quello della strumentazione disponibile. Questo dipende da tribunale a tribunale, ma è importante essere consapevoli dei mezzi a propria disposizione quando si mostrano immagini e video in aula: c'è un monitor, uno schermo TV, o un proiettore disponibile? È necessario utilizzare il proprio laptop e farlo passare di mano? O è possibile mostrare solo immagini stampate? L'efficacia della presentazione si basa anche su quanto efficacemente si è in grado di adattarsi alle limitazioni di un dato contesto.

Infine, può essere importante, quando richiesto e se fattibile, **omettere parti sensibili di video e immagini**, ad esempio volti o altre informazioni personali di soggetti che appaiono nel filmato.

Conclusioni

Il primo obiettivo di questi concetti e princìpi è quello di aumentare la consapevolezza riguardo l'importanza delle immagini e dei video come fonti di prova, e dare qualche indicazione su come trattarli in modo scientificamente corretto. Questi princìpi dovrebbero essere ulteriormente sviluppati, possibilmente adottando linee guida già esistenti e riconosciute a livello internazionale. Solo in questo modo possiamo garantire ai nostri Paesi una maggiore sicurezza e una giustizia più efficace, riducendo al contempo i costi per le risorse umane e i problemi causati da una cattiva gestione delle fonti di prova. Lavorare alle prove video nel modo giusto comporta solo vantaggi. È necessaria una sola cosa, ma molto importante: un cambiamento di mentalità. **Le prove video non sono "solo un video", sono "fonti di prova" e dovrebbero essere trattate come tali.**

Riferimenti

L’Autore

Martino Jerian è un ingegnere elettronico, CEO e fondatore di Amped Software. Si è laureato in Ingegneria Elettronica presso l'Università di Trieste (Italia) nel 2005 (summa cum laude) con una tesi sull'elaborazione delle immagini in ambito forense. Vanta un’ampia esperienza nello sviluppo di software, avendo progettato e implementato lo sviluppo dei prodotti Amped Software. Durante la sua carriera, ha anche ricoperto il ruolo di professore a contratto presso l'Università di Roma Tor Vergata, nonché presso l'Università Link Campus di Roma, dove ha tenuto lezioni relative a indagini, analisi forense e intelligence. Attualmente si sta concentrando sul miglioramento del rapporto tra scienza e giustizia, in particolare durante le indagini forensi. È fermamente convinto che sia necessaria una formazione adeguata quando si tratta di analisi di immagini e video, poiché queste tecnologie sono spesso date per scontate e non sempre considerate in maniera adeguata in relazione alle problematiche di cybersecurity e intelligenza artificiale.

Amped Software

Amped Software è una software house che sviluppa software per l'analisi e il miglioramento di immagini e video. Gli ambiti di applicazione vanno da quello forense alla sicurezza e alle indagini in oltre 100 Paesi in tutto il mondo. Fondata a Trieste nel 2008, e con una sede di supporto negli USA, a Brooklyn, New York, l'azienda supporta più di 1400 organizzazioni nei settori della pubblica sicurezza e della sicurezza nazionale. Amped Software è formata da un team composto da più di 35 persone provenienti da 10 Paesi diversi con vari background professionali, tra cui ex operatori delle Forze dell’Ordine, fisici, personale militare ed esperti nell'elaborazione delle immagini.

Contatti

Martino Jerian
CEO e fondatore
Amped Software
martino.jerian@ampedsoftware.com

Versione 1.00 - 2023-07-28 © Amped SRL 2023