UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA TRIENNALE IN INGEGNERIA BIOMEDICA

Il Watermarking Digitale di immagini: garantire integrità e paternità in sanità

Relatore:

PROF. GIOVANNI SPARACINO

Laureando:

ALBERTO PRESTI

1217359

Anno Accademico 2021/22

Indice

Capitolo 1: Sicurezza dei dati clinici 9

1.1 Aspetti generali di integrità e paternità 9

1.2 La Firma Digitale e le Funzioni di Hash 11

1.3 Problemi ulteriori nella gestione e condivisione delle immagini 12

1.4 Scopo dell'elaborato e Presentazione 14

Capitolo 2: Il Digital Watermarking di immagini 15

2.1 Cenni Storici 15

2.2 Requisiti di un sistema di Image Digital Watermarking 15

2.2.1 Impercettibilità 16

2.2.2 Robustezza 16

2.2.3 Sicurezza 18

2.2.4 Capacità 18

2.2.5 Costo Computazionale 18

2.2.6 Falsi Positivi 19

2.2.7 Chiave di Watermarking 19

2.2.8 Resistenza alle Collisioni 19

2.2.9 Reversibilità 20

5.2.10 Necessità di trade-off 20

2.3 I concetti alla base degli algoritmi di watermarking 20

2.3.1 Definizione di Entropia 21

2.3.2 Inserimento del Watermark 21

2.3.3 Estrazione del Watermark 22

Capitolo 3: Alcune tecniche di Digital Image Watermarking 25

3.1 Classificazione delle tecniche 25

3.2 Metodi di Watermarking nel Dominio Spaziale 26

3.2.1 Least Significant Bit (LSB) 26

3.2.2 Intermediate Significant Bit (ISB) 27

3.3 Metodi di Watermarking nel Dominio delle Frequenze 28

3.3.1 Watermarking tramite Discrete Cosine Transform (DCT) 29

3.3.2 Watermarking tramite Discrete Wavelet Transform (DWT) 31

3.4 Metodi di Watermarking Ibridi 32

3.5 Considerazioni riassuntive 33

Capitolo 4: La valutazione dei sistemi di Image Watermarking 35

4.1 Tipologie di attacco al Watermark 35

4.1.1 Attacchi Attivi 35

4.1.2 Attacchi Passivi 36

4.1.3 Attacchi di Rimozione 36

4.1.4 Attacchi Geometrici 36

4.1.5 Attacchi Crittografici 37

4.1.6 Rapporto costo-efficacia delle diverse tipologie di attacco 37

4.2 Metriche di valutazione delle performance 37

4.2.1 Errore Quadratico Medio (MSE) 38

4.2.2 Distanza Euclidea (DE) 38

4.2.3 Structural Similarity Index (SSIM) 39

4.3 Considerazioni riassuntive 40

Capitolo 5: Uso del Digital Image Watermarking in Sanità 41

5.1 Sicurezza nei Sistemi Informativi Sanitari 41

5.2 Requisiti del watermark in applicazioni sanitarie 41

5.2.1 Impercettibilità e Reversibilità 41

5.2.2 Controllo dell'Integrità 42

5.2.3 Autenticazione 42

5.3 Diverse applicazioni del watermarking in sanità 43

5.3.1 Controllo degli accessi 43

5.3.2 Verifica del mittente 43

5.3.3 Verifica dell'integrità 43

5.3.4 Annotazione di informazioni 44

5.3.5 Indicizzazione 44

5.3.6 Pseudonimizzazione 44

Capitolo 6: Approfondimento: metodo di watermarking basato su DFT per bioimmagini 45

6.1 Specifiche del contesto 45

6.2 Analisi dell'algoritmo 45

6.2.1 Inserimento del Watermark 46

6.2.2 Estrazione del Watermark 47

6.3 Risultati 47

6.3.1 Impercettibilità del Watermark 49

6.3.2 Robustezza del Watermark 49

Capitolo 7: Conclusione 51

Bibliografia 53

Alla mia famiglia,

Per un mondo di possibilità

Capitolo 1: Sicurezza dei dati clinici

1.1 Aspetti generali di integrità e paternità

Il rapido avanzare dell'ingegneria dell'informazione nel settore sanitario ha permesso la progettazione e l'implementazione di soluzioni digitali sempre più avanzate. Queste hanno permesso l'introduzione di nuove tecnologie utili a migliorare la salute e la degenza del paziente. Oggi, infatti, è possibile usufruire di applicativi digitali in grado di assistere il medico nel processo di cura oppure permettere di far monitorare al paziente facilmente il proprio stato di salute.

Tra le tante novità, il progresso nel campo della sanità digitale ha permesso la sostituzione della vecchia cartella sanitaria cartacea con un suo equivalente informatico: il fascicolo sanitario digitale.

Come la versione cartacea il fascicolo sanitario digitale, individuato anche come Electronic Health Record (EHR) [1], conserva al suo interno tutte le informazioni riguardanti il percorso clinico di un paziente. Anamnesi, referti, risultati di esami, bioimmagini (come ad esempio radiografie o risonanze magnetiche), certificati, ricette e lettere di dimissioni sono tutte informazioni archiviabili all'interno della cartella digitale.

Oltre ad essere una mera raccolta di tutti i dati sanitari di un paziente, la cartella clinica elettronica ha numerosi vantaggi. In primo luogo, viene garantita una visione integrata dei dati del paziente che possono riferirsi a diversi ricoveri e possono provenire dunque da una collezione di molteplici sistemi informativi. Inoltre, il fascicolo sanitario digitale permette una condivisione rapida ed eventualmente contemporanea delle informazioni, non solo con il personale medico autorizzato ma anche con il paziente stesso, ovunque esso si trovi. Infine, ma non meno importante, la cartella clinica digitale permette di effettuare indagini statistiche senza che i dati sensibili del paziente vengano compromessi.

Tuttavia, il progresso dei software di elaborazione di immagini, così come internet stesso, ha reso sempre più semplice duplicare, riprodurre e distribuire informazioni a basso costo e senza una significativa perdita di qualità [2]. Questo è un problema per la sicurezza e la confidenzialità dei dati, soprattutto nel caso questi si riferiscano a informazioni sensibili di un paziente.

A testimonianza di questo, un rapporto stilato dal dipartimento di ricerca di "Statista" evidenza come il numero di violazioni di dati nella sanità americana sia passato da 18 nel 2009 a ben 712 nel 2021 [3]

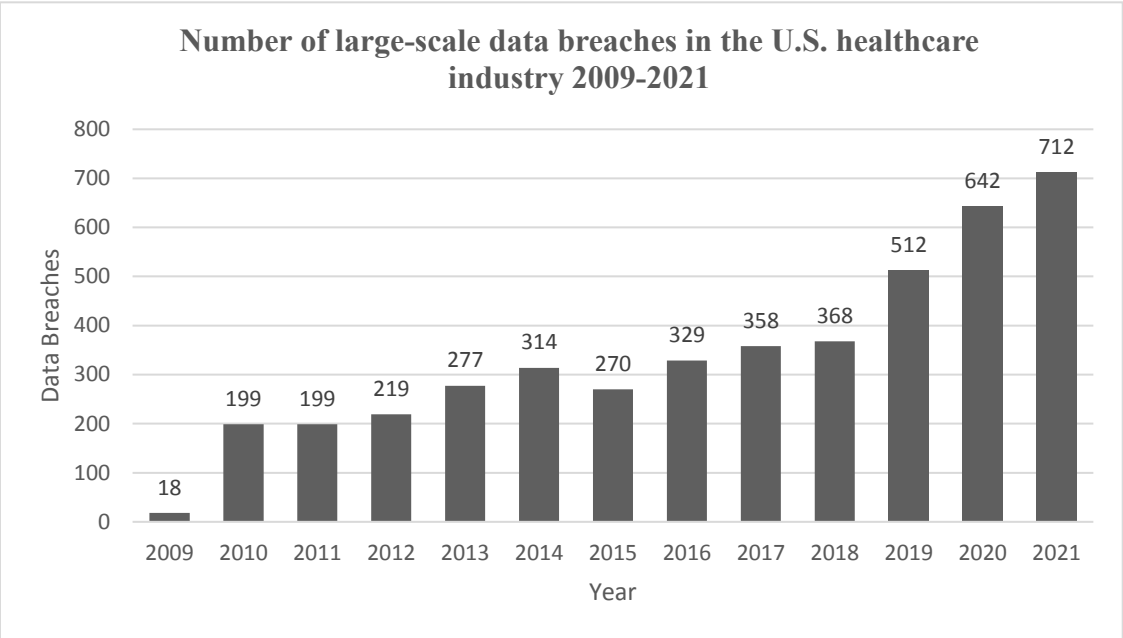


Figura 1: Numero di attacchi hacker nell'industria sanitaria americana nel periodo 2009-2021. Dati ottenuti da [3]

Dovendo gestire l'archiviazione e la condivisione di una moltitudine indefinita e variabile di prestazioni e informazioni mediche ed essendo queste considerate sensibili dal GDPR (General Data Protection Regulation) [4], la cartella clinica sanitaria, intesa come fascicolo digitale, deve quindi poter garantire la sicurezza, l'integrità e la paternità delle informazioni. In particolare, si definiscono le seguenti caratteristiche:

1. **Confidenzialità**: Assicurare che l'informazione in questione sia accessibile solamente dalle persone autorizzate e non da altre che vorrebbero ottenerne l'accesso in modo illecito.
2. **Integrità**: Assicurare che l'informazione venga trasmessa (o archiviata) senza perdita di dettaglio e senza modifiche da parte di agenti esterni
3. **Paternità**: Assicurare che il mittente e proprietario dell'informazione sia riconoscibile e certificabile.

1.2 La Firma Digitale e le Funzioni di Hash

Garantire la sicurezza delle informazioni significa assicurarsi che nessuna persona o servizio informatico possa ottenere l'accesso ai dati in questione senza autorizzazione. Con integrità dei dati, invece, si richiede che le informazioni archiviate o trasmesse vengano ricevute immutate rispetto alla loro versione originale in quanto a contenuto e aspetto. Infine, con paternità delle informazioni ci si riferisce alla possibilità di certificare e riconoscere come tale il creatore del messaggio e delle informazioni in esso contenute.

Lo strumento più utilizzato e adatto a soddisfare queste specifiche è la firma digitale: una particolare firma basata su una coppia di chiavi asimmetriche che consente, come fosse una firma cartacea, di garantire a livello legale l'autenticità di un documento in termini di sicurezza, integrità e paternità.

Il funzionamento della firma digitale si fonda su quelle che sono definite funzioni di hash, ovvero algoritmi in grado di convertire un qualsiasi messaggio in un digest (sequenza binaria) di lunghezza fissata. Algoritmi di hashing comunemente utilizzati possono essere ad esempio: MD2, MD4, MD5 e Secure Hash Algorithm SHA.

Il fatto che il digest generato sia considerabile unico (e quindi rappresentativo di un solo specifico input) e che sia molto difficile da invertire nel messaggio originale rende possibile l'utilizzo di questi metodi per garantire l'integrità e la paternità delle informazioni. Infatti, sia nel caso in cui il messaggio venisse compromesso, che nel caso in cui il mandante non sia chi dice di essere, il digest del file ricevuto non coinciderebbe con quello del file originale [5].

Più in particolare, per la creazione e implementazione di una firma digitale a partire da un messaggio di partenza si procede come segue:

1. Innanzitutto, si crea, a partire dal messaggio originale m_i il digest d_i di lunghezza n-bit. Questo può essere generato con uno degli algoritmi di hashing citati prima anche se in letteratura vi sono molteplici funzioni di hash specifiche per ogni determinato task.

2. Successivamente, con un metodo di crittografia asimmetrica, il digest d_i viene criptato nel digest d_s con la chiave privata $k_{private}$ del mittente e spedito, in allegato al documento in questione, sul canale insicuro.

3. Alla ricezione del documento, il destinatario decripta il digest d_s con la chiave pubblica del mittente k_{public} riottenendo d_i. Questo viene confrontato con il digest d_f generato a partire dal documento m_f appena ricevuto.

4. Nel caso in cui i due digest d_i e d_f coincidano allora il documento inviato può considerarsi integro e inviato dal corretto mittente. Questa procedura permette dunque di garantire l'integrità e la paternità dell'informazione.

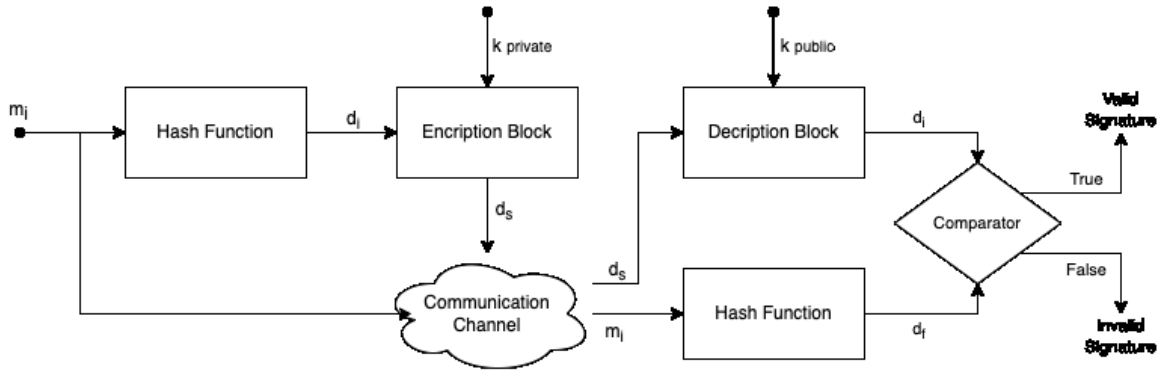


Figura 2: Schema di implementazione e validazione di una firma digitale. Ripreso da [5]

1.3 Problemi ulteriori nella gestione e condivisione delle immagini

Tra le molteplici tipologie di documenti e supporti digitali raccolti all'interno della cartella clinica elettronica le immagini sono quelle che richiedono la maggior attenzione. Lo sviluppo di software di elaborazione delle immagini, i progressi nel campo dell'Intelligenza Artificiale e il diffondersi dello stesso internet, hanno drasticamente facilitato la copia, modifica, riproduzione e distribuzione di immagini senza una sostanziale perdita di qualità. Secondo una ricerca di mercato stilata da VMR [6] nel 2022 il mercato dei software per l'editing di immagini è valutato 293 milioni di dollari e destinato a crescere con un tasso annuale di crescita composito del 3,57% da qui al 2030. È dunque necessario agire per impedire ogni possibile violazione e prevenire quelle future nel migliore dei modi.

Come anticipato nel capitolo precedente, l'utilizzo di una firma digitale basata sul confronto di digest binari, sembra essere la soluzione ottimale per assicurare l'integrità dell'immagine trasmessa e al contempo la sua paternità. Questa è certamente la modalità più utilizzata, ma esistono tuttavia delle problematiche legate all'utilizzo di una firma digitale su dei supporti multimediali come le immagini.

In primo luogo, l'immagine digitale, per poter essere trasmessa tra due o più client via cloud, viene inizialmente sottoposta a delle procedure di compressione. Questo perché nella maggior parte dei casi l'ingombro spaziale dell'immagine originale è incompatibile con una rapida velocità di trasmissione. Tuttavia, queste procedure di compressione con perdita di informazione (lossy) non sono sempre prevedibili e gestibili da parte dell'utente. Di

conseguenza i due digest d_i e d_f potrebbero non coincidere a causa di manipolazioni fuori dal nostro controllo, ma necessarie. Inoltre, il fatto che nemmeno la non compatibilità dei digest sia assicurata, ma solamente possibile, rende il problema ancora più delicato.

In secondo luogo, utilizzando semplicemente una firma digitale, informazioni ulteriori e metadata relativi all'immagine in questione sono solitamente "allegati" all'immagine ma non parte di essa. Il fatto di avere immagine e metadata separati può portare ad una più facile perdita di informazioni importanti e addirittura ad un danneggiamento di questi ultimi durante la fase di condivisione.

Infine, come ultima ma non meno importante problematica, la creazione di una firma digitale basata su digest obbliga il mittente del messaggio alla trasmissione di due documenti: il documento in sé (nel nostro caso un'immagine) e appunto il suo digest, criptato con la chiave privata del destinatario. Si potrebbe sostenere che il digest, in quanto tale, abbia un ingombro spaziale tanto esiguo da non essere un problema per una trasmissione veloce. Tuttavia, risulta essere un file ulteriore che deve essere condiviso con tutti i rischi del caso.

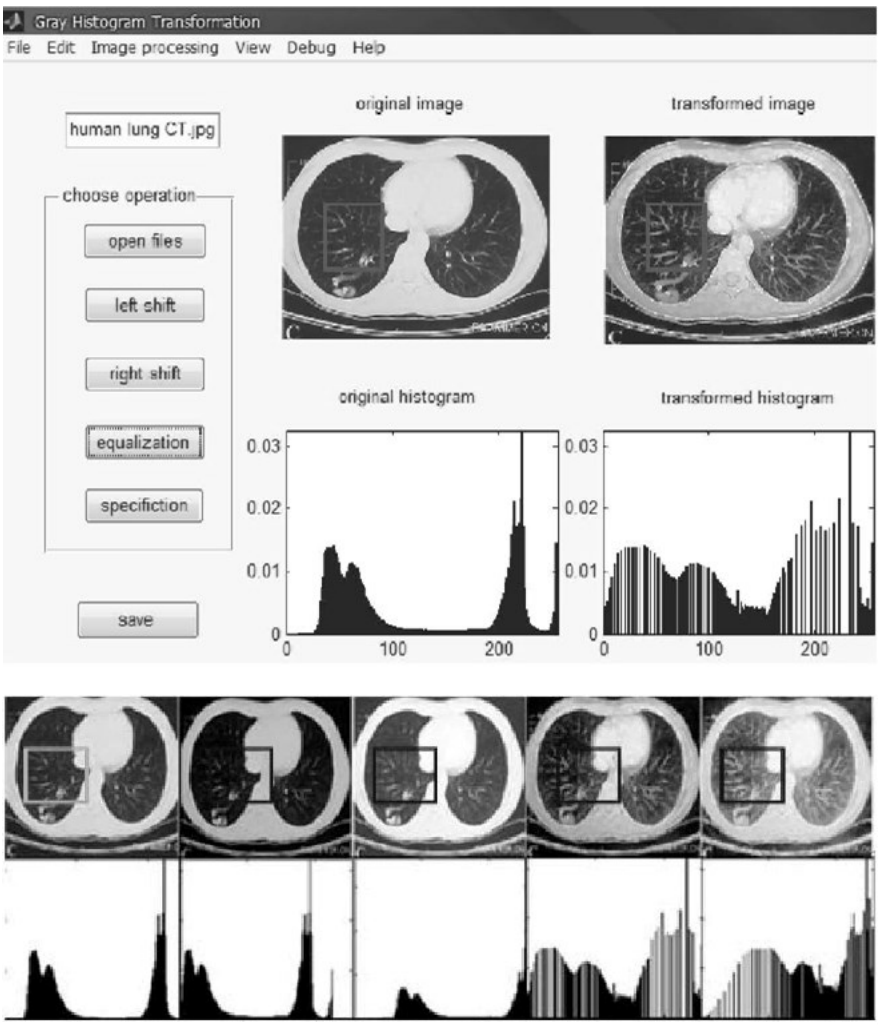


Figura 3: Esempi di image processing in sanità. Ripreso da [30]

1.4 Scopo dell'elaborato e Presentazione

Dopo l'introduzione generale fatta sull'organizzazione e sulla condivisione di dati sanitari tramite una cartella sanitaria elettronica, si è analizzata la problematica inerente alle immagini mediche e alle tecniche, con vantaggi e svantaggi, che possono assicurarne l'integrità e la paternità durante l'archiviazione o trasmissione. Nel prossimo capitolo verrà introdotto il concetto di Watermarking Digitale applicato alle immagini come metodo alternativo alla firma digitale per assicurare l'integrità e la paternità dei file multimediali. In particolare, dopo una breve introduzione storica verranno approfonditi i requisiti per l'implementazione di un watermark digitale. Successivamente, viene spiegato il processo di applicazione ed estrazione del watermark nelle sue varianti spaziali, in frequenza o ibride. Verrà inoltre effettuata, nel capitolo 4, un'analisi dettagliata dei possibili attacchi che possono compromettere il watermark e una valutazione delle performance delle tecniche di applicazione. Infine, nel capitolo 6, dopo un approfondimento sulle applicazioni del watermarking digitale di immagini in sanità, viene analizzato nel dettaglio il processo di inserimento ed estrazione di un watermark per immagini mediche basato sulla trasformata DFT.

Capitolo 2: Il Digital Watermarking di immagini

2.1 Cenni Storici

Con il termine “watermarking” ci si riferisce essenzialmente ad una tecnica di riconoscimento che prevede l’apposizione di un marchio distintivo all’oggetto o al documento che si vuole certificare [7]. Esempi di queste tecniche non sono certamente nuovi; esempi arcaici di watermarking possono essere ricondotti addirittura al tredicesimo secolo quando le filigrane erano utilizzate come marchio per l’identificazione del produttore di una specifica carta [8].

Il nome venne tuttavia coniato per la prima volta solamente nel dicembre 1992 da Andrew Tirkel e Charles Osborne che, nell’anno seguente, dimostrarono inoltre la prima implementazione di questo metodo applicato a supporti digitali [9].

In quanto contenuti digitali, infatti, le immagini possono facilmente “nascondere” dati aggiuntivi al loro interno senza che questi vadano a modificare visivamente l’immagine stessa. Il Watermarking digitale, dunque, è una tecnica per inserire delle informazioni, come ad esempio una firma, all’interno di immagini in modo che queste informazioni possano poi essere estratte e validate.

Il concetto chiave alla base di queste tecniche è la steganografia: (dal greco ‘steganos’: nascosto) una tecnica per occultare un canale di comunicazione e cambiare l’immagine in modo tale che solo il mandante e il ricevente possano identificare il messaggio. Invece di criptare il messaggio, la steganografia tramite Watermarking cela, all’interno delle immagini, degli “oggetti” impercettibili alla vista (marker), che non possono dunque essere scoperti.

2.2 Requisiti di un sistema di Image Digital Watermarking

Prima di analizzare nel dettaglio il processo di implementazione di un watermark digitale all’interno di un supporto multimediale quale le immagini, bisogna descrivere nel dettaglio i requisiti che questo sistema di autenticazione deve soddisfare e le caratteristiche che ne descrivono il funzionamento.

2.2.1 Impercettibilità

L'impercettibilità è un fattore chiave sia per il funzionamento di un algoritmo di watermarking che per la valutazione delle sue performance. L'obiettivo è quello di ottenere un'immagine, contenente il watermark, indistinguibile, all'occhio umano, dall'immagine originale se non per una lieve e trascurabile degradazione in termini di luminosità e contrasto [2]. L'impercettibilità può essere a sua volta descritta da due indicatori:

1. **Invisibilità**: Quanto il watermark risulti invisibile all'occhio umano e alle tecniche di editing.
2. **Fedeltà**: Quanto l'immagine con il watermark risulti essere simile all'originale.

Per valutare il grado di impercettibilità di un sistema di watermarking è possibile utilizzare il **rapporto segnale-rumore [PSNR]** come indicatore. In particolare, un alto valore di PSNR corrisponderà ad un alto grado di impercettibilità. Un metodo ulteriore per la stima del grado di impercettibilità è quello proposto da Yang et al [10]. Questo metodo utilizza come indicatore un rapporto segnale-rumore basato sulle capacità di mascheramento dell'occhio umano (Masking-based Peak Signal to Noise Ratio, MPSNR).

$$\mathrm{PSNR} = 20 \cdot \log_{10} \frac{\mathrm{Max(I)}}{\sqrt{\mathrm{MSE}}} \tag{1}$$

dove $Max(I)$ è il massimo valore (in livelli di grigio) dei pixel dell'immagine e MSE è l'errore quadratico medio tra l'immagine di partenza H e l'immagine elaborata K entrambe di dimensione NxM

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \|H(i,j) - K(i,j)\|^2 \tag{2}$$

2.2.2 Robustezza

La robustezza è un prerequisito fondamentale; consiste nella capacità di riconoscimento di un watermark, inserito in un'immagine, dopo che sul sistema immagine-watermark sono state

effettuate delle operazioni come ad esempio: filtraggio spaziale, color mapping, compressione lossy, traslazione, rotazione, ritaglio e miglioramento dell'immagine stessa [2].
Esistono essenzialmente due modi per garantire un alto livello di robustezza del watermark:

1. **Inserimento ridondante del watermark**: Posizionare il watermark più volte all'interno della stessa immagine ma in posizioni diverse in modo tale da incrementare la probabilità che almeno uno di questi venga riconosciuto [2].
2. **Trasmissione in banda larga**: Utilizzo di una banda di frequenze più ampia del necessario in modo tale da incrementare il rapporto segnale-rumore e di conseguenza la qualità del sistema di watermarking. Questa tecnica funziona in quanto all'aumentare dello spettro disponibile aumenta in maniera proporzionale anche l'energia associata al segnale [2] [11].

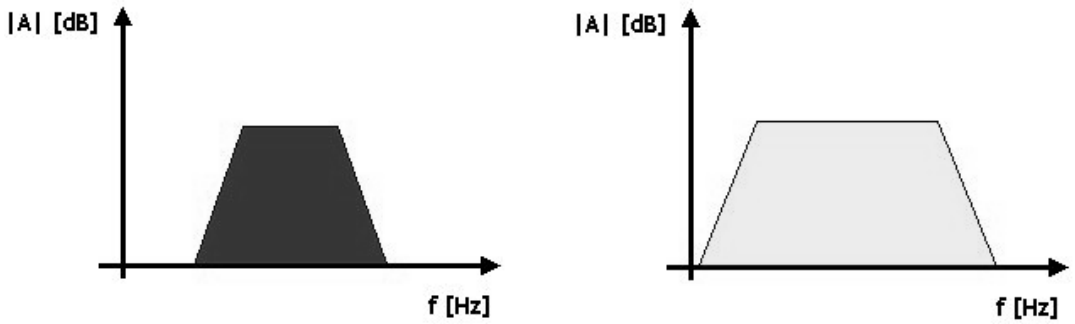


Figura 4: L'energia aumenta se, a parità di modulo, si incrementa l'occupazione in banda del segnale

Un buon sistema di watermarking di immagini dovrebbe essere robusto contro un gran numero di tipologie di attacco, tuttavia, a seconda delle applicazioni, non tutti gli algoritmi di watermarking necessitano di essere robusti allo stesso livello. Si definiscono quindi tre livelli di robustezza [2]:

1. **Forte**: In grado di resistere a diversi attacchi, geometrici e non geometrici, senza che il watermark venga alterato. Il Watermark rimane lo stesso anche dopo numerosi attacchi e mantiene la proprietà di essere utilizzabile come metodo di autenticazione. Viene spesso utilizzato per la protezione del diritto d'autore e il controllo delle copie.
2. **Fragile**: Sono utilizzati principalmente per la verifica dell'integrità di un documento. Il fatto che sia molto sensibile alle trasformazioni e agli attacchi permette infatti di controllare se il documento è stato modificato durante la trasmissione.

3. **Semi-fragile:** Questo tipo di watermark è in grado di resistere bene ad alcune tipologie di attacchi mentre fallisce contro altri. Viene spesso utilizzato per l'autenticazione di immagini.

2.2.3 Sicurezza

Un ulteriore prerequisito è la sicurezza del sistema di watermarking, definita come la l'impossibilità di ricostruire il watermark senza essere in possesso della chiave di criptazione [2].

Un sistema non sicuro non può essere utilizzato per la protezione del diritto d'autore, per l'autenticazione dei documenti e nemmeno per il loro tracciamento. Si prenda come esempio di supporto multimediale le immagini ottenute da una risonanza magnetica funzionale (fMRI). Questa contiene dati altamente sensibili, come quelli relativi all'attività celebrale, che necessitano di essere archiviati e condivisi in sicurezza.

La sicurezza può essere garantita da diversi metodi di criptazione dei quali la tipologia di chiave (o di chiavi) determina il grado di sicurezza dell'algoritmo. Studi hanno evidenziato come i tradizionali metodi di criptazione (ad esempio DES, AES) non si comportano bene nella criptazione di immagini a causa dei loro problemi di correlazione e ridondanza. Si tende dunque a utilizzare sistemi crittografici basati sul caos [12].

2.2.4 Capacità

La capacità di watermarking (watermarking payload) indica la "quantità di informazione" che può essere inserita all'interno dell'immagine ed è basata appunto sulle dimensioni di quest'ultima.

La capacità viene espressa dal numero di bit di informazione aggiuntiva che l'immagine porta con sé dopo l'inserimento del watermark. In altre parole, la capacità di watermarking, determina un limite superiore di informazione che può essere inserita senza andare a sacrificare robustezza e impercettibilità [2].

2.2.5 Costo Computazionale

Il costo computazionale per l'inserimento e la successiva estrazione del watermark all'interno dell'immagine deve essere minimo. Questo costo è condizionato da due fattori principali: il

tempo richiesto per eseguire le operazioni e il numero totale di operazioni di inserimento e rilevamento.

Ad un alto costo computazionale corrisponde anche un alto valore di robustezza e sicurezza ma bisogna, per questioni pratiche, cercare un buon trade off tra complessità computazionale e gli altri parametri [2].

2.2.6 Falsi Positivi

Il tasso di falsi positivi viene qui utilizzato per identificare e contare il numero delle volte in cui un watermark viene riconosciuto all'interno di un'immagine quando in realtà non è stato inserito nessun watermark [2]. Questo problema accade specialmente quando il watermark estratto è sostanzialmente diverso da quello inserito nell'immagine di host.

Considerando il watermark originale W di lunghezza l e il watermark estratto W' allora si può definire il tasso di falsi positivi (FPR) come:

$$\mathrm{FPR} = \frac{\mathrm{l}'}{\mathrm{l}} \tag{3}$$

dove l' è la distanza di Hamming tra W e W', definita come numero di posizioni, tra due stringhe di ugual lunghezza, in cui i simboli corrispondenti sono diversi [13].

2.2.7 Chiave di Watermarking

È una chiave segreta che determina alcuni degli iperparametri degli algoritmi di inserimento. Questa chiave include solitamente informazioni riguardanti la direzione e il dominio di applicazione del watermark [2].

2.2.8 Resistenza alle Collisioni

La resistenza più o meno marcata alle manipolazioni permette di utilizzare un sistema di watermarking per controllare l'autenticità di documento [2]. Qualsiasi cambiamento del watermark risulta infatti in un deterioramento, anche impercettibile, dell'immagine. Testandone l'integrità del sistema si può quindi stabilire se il watermark è stato manomesso oppure no durante la condivisione o archiviazione delle immagini.

2.2.9 Reversibilità

Questo prerequisito assicura che sia possibile estrarre il watermark e ricostruire in maniera esatta l'immagine originale [2].

5.2.10 Necessità di trade-off

In conclusione, è facile intendere che soddisfare contemporaneamente impercettibilità, robustezza e capacità, è impossibile a causa dei conflitti che esistono tra le loro caratteristiche.

Per un sistema di Watermarking si potrebbe diminuire l'impercettibilità aumentando la robustezza e il payload e viceversa. È necessario dunque trovare un buon trade off tra tutte le variabili in gioco [2]. Come mostrato in Figura 5, all'aumentare del grado di impercettibilità diminuiscono robustezza e payload; al crescere della capacità diminuiscono robustezza e impercettibilità; aumentando la robustezza, invece, diminuiscono capacità e impercettibilità.

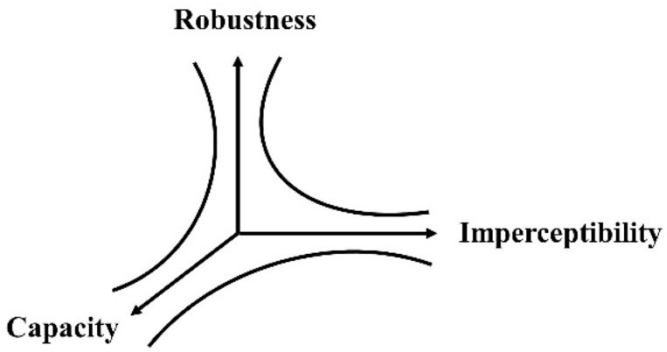


Figura 5: Andamento relativo di robustezza, impercettibilità e capacità (payload). Ripresa da [2]

2.3 I concetti alla base degli algoritmi di watermarking

Nelle tecniche di watermarking, un simbolo (watermark) rappresentante l'autenticità e la paternità di un documento, nel nostro caso le immagini, viene incorporato nel file originale e poi estratto e validato in fase di verifica.

Il watermark, che a seconda delle applicazioni può essere visibile oppure no, può essere formato da un singolo bit, da un set binario di dati oppure da una seconda immagine. Il watermark deve rappresentare informazioni in grado di verificare l'autenticità di un documento e la sua paternità [14] [15].

In ambito biomedico si richiede che il watermark non sia visibile all'occhio umano e al contempo che sia assicurato un buon compromesso tra robustezza e capacità [16]. Per questo

motivo l'entropia, definita in termini di informazione, gioca un ruolo essenziale nell'implementazione di un algoritmo di watermarking in quanto determina le posizioni in cui il watermark può essere inserito senza distorcere o compromettere l'immagine [2].

2.3.1 Definizione di Entropia

L'entropia di un sistema caratterizzato da n stati (o configurazioni) può essere definita dalla seguente relazione [2]:

$$ETP = -\sum_{i=1}^{n} P_i log P_i \quad (4)$$

dove $0 \leq P_i \leq 1$ e P_i è la probabilità che il sistema rappresenti la i-esima configurazione, con

$$\sum_{i=1}^{n} P_i = 1 \quad (5)$$

2.3.2 Inserimento del Watermark

Il processo di inserimento del watermark inizia con la scelta dell'immagine di interesse. Questa immagine viene definita "cover" oppure "host image" in quanto andrà ad ospitare il watermark.

La cover, dal punto di vista del watermark, può essere considerata puramente rumore [2].

1. In primo luogo, si effettua un pre-processing dell'immagine per prepararla ad un migliore inserimento e ad una migliore condivisione. La tipologia di operazioni dipende dallo specifico algoritmo di watermarking. (Le differenti tipologie di watermarking verranno trattate in seguito).
2. Successivamente, si valuta l'entropia dell'immagine in modo tale da determinare il payload massimo consentito.
3. Utilizzando un metodo di criptazione ottica il watermark viene inserito nelle componenti a media/alta entropia dell'immagine host utilizzando una chiave segreta.
4. Infine, il sistema genera l'immagine contenente il watermark.

Dopo avere generato l'immagine contenente il watermark questa è pronta per essere condivisa e trasmessa attraverso un canale di comunicazione. L'informazione contenuta all'interno del watermark potrebbe andare incontro a diversi attacchi come compressione irreversibile, distorsione geometrica e altre operazioni che vanno a generare rumore. Questo rumore va a massimizzare l'entropia e dunque anche l'incertezza (o ambiguità) sull'informazione media contenuta nell'immagine [2]. Le tecniche di watermarking, dunque, possono essere applicate solamente a immagini ad alta risoluzione che hanno un più alto valore di entropia.

Il processo di inserimento (schematizzato in Figura 5) genera dunque un'immagine, D_W, che può essere descritta dalla seguente funzione [2]:

$$\text{Watermarked Image, } \mathrm{D_W} = \mathrm{E(I, ETP, W, K)} \tag{6}$$

Dove E è lo specifico algoritmo di watermarking, I è l'immagine host, ETP è l'entropia, W il watermark e K la chiave segreta.

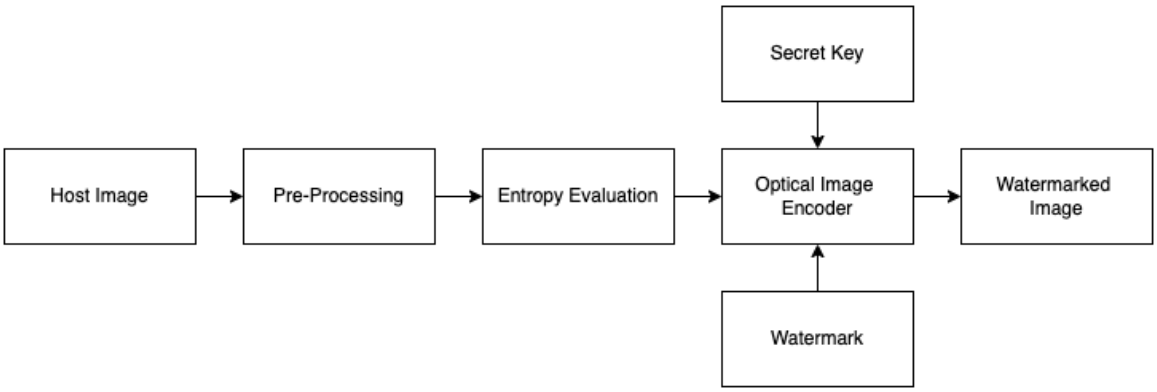


Figura 6: Schema di inserimento del watermark. Ripreso da [2]

2.3.3 Estrazione del Watermark

Nel processo di estrazione del watermark si prende in considerazione l'immagine contenente il watermark ricevuta dopo la sua trasmissione tramite un canale di comunicazione.

1. L'immagine, dopo una fase di pre-processing, viene analizzata nelle sue componenti e vengono estratte le informazioni riguardanti ampiezza e fase

2. Viene valutata l'entropia delle componenti analizzate e viene scelto un alto valore di entropia per estrarre il watermark garantendo al contempo una migliore robustezza e impercettibilità
3. Utilizzando la stessa chiave segreta della fase di inserimento e l'immagine di host, il watermark viene estratto dall'immagine.
4. Infine, l'immagine host originale viene ricostruita e il watermark viene analizzato per valutare l'autenticità e la paternità del documento.

Il processo di estrazione del watermark (illustrato in Figura 6) ricava il watermark, W', che può essere descritto dalla seguente funzione [2].

$$W' = e(D_W, K, ETP, I) \tag{7}$$

Dove $e(.)$ è uno specifico algoritmo di estrazione.

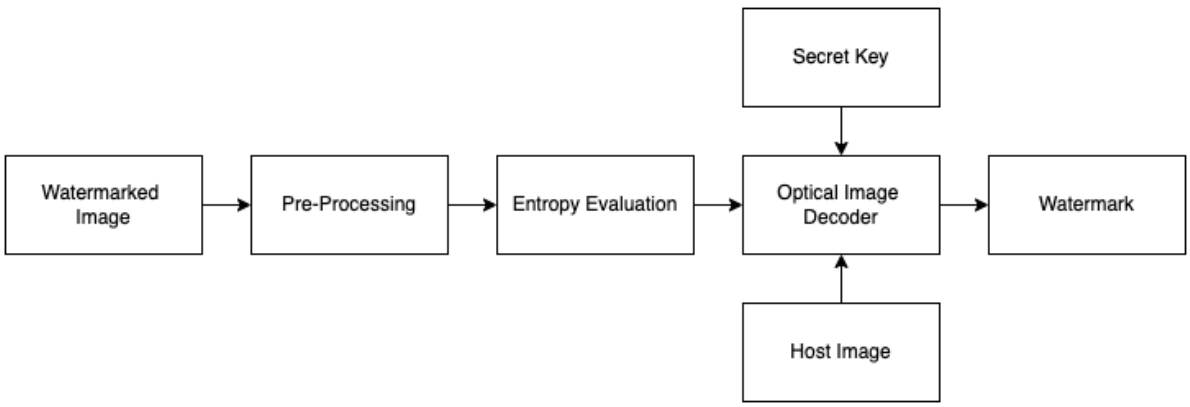


Figura 7: Schema di estrazione del watermark. Ripreso da [2]

Capitolo 3: Alcune tecniche di Digital Image Watermarking

3.1 Classificazione delle tecniche

Dopo aver descritto, nella sezione 2.3, l'algoritmo di inserimento ed estrazione nei suoi principi base è possibile addentrarsi più in dettaglio nelle tecniche che vengono comunemente utilizzate per il digital watermarking di immagini.

Un algoritmo di watermarking per immagini (esistono algoritmi di watermarking per altri tipi di documenti) può essere classificato e distinto da un altro in base a [2]:

1. **Natura dell'algoritmo**: L'algoritmo di watermarking può essere di tipo:
    a. **Sequenziale**: Eseguito una sola volta senza altre elaborazioni in esecuzione
    b. **Parallelo**: Esegue alcune delle sue operazioni in parallelo.
2. **Percezione Umana**: L'algoritmo è definito **visibile** nel caso in cui il watermark applicato risulti visibile all'occhio umano oppure **invisibile** nel caso contrario.
3. **Dominio di Lavoro**: L'algoritmo può operare nel:
    a. Dominio dello **Spazio**
    b. Dominio della **Frequenza**: ottenuto tramite trasformate [DCT, DFT, DWT, SVD]
    c. Dominio **Ibrido**

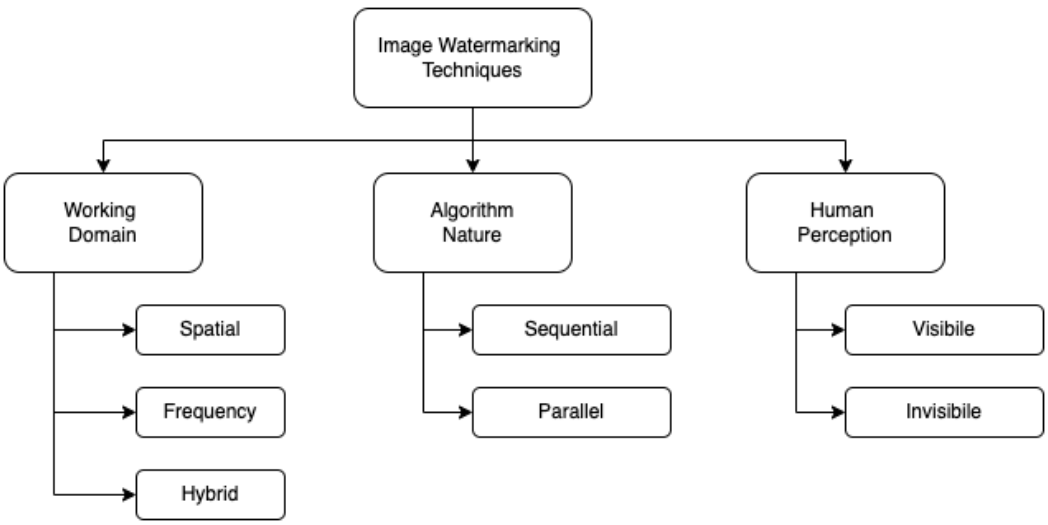


Figura 8: Tipologie di Digital Image Watermarking. Ripreso da [2]

3.2 Metodi di Watermarking nel Dominio Spaziale

Questo tipo di algoritmi inserisce il watermark fornito dall'utente all'interno dell'immagine host sfruttando le informazioni nel dominio dello spazio di quest'ultima. Sono dunque tecniche che lavorano direttamente sui pixel dell'immagine originale [2].

Il watermark può essere inserito manipolando il valore di intensità di grigio (o dei canali RGB per immagini a colori) e a seconda dell'intensità il watermark sarà visibile oppure no all'occhio umano.

Sono tecniche poco complesse ma efficienti e veloci in termini computazionali. Inoltre, queste tecniche permettono un certo controllo sulla qualità dell'immagine risultante [2].

Tuttavia, tecniche basate sul dominio spaziale funzionano bene solo nel caso in cui l'immagine, passando attraverso un canale di comunicazione digitale, non venga esposta ad un eccessivo rumore o ad una eccessiva manipolazione (ad es. compressione). Sono inoltre poco resistenti ad attacchi geometrici: un ritaglio, ad esempio, potrebbe completamente eliminare il watermark dall'immagine [2].

3.2.1 Least Significant Bit (LSB)

La tecnica basata sul "Least Significant Bit" è la tecnica più utilizzata per effettuare il watermarking nel dominio spaziale.

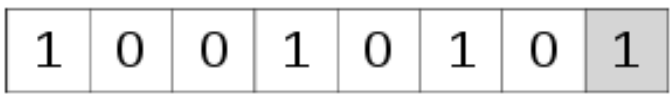


Figura 9: Least Significant Bit. Ripresa da [17]

Il "bit meno significativo" o LSB è la posizione occupata dal bit nel sistema binario che fornisce il valore dell'unità (e determina la parità o la disparità del numero). Nella rappresentazione convenzionale occupa l'ultimo posto a destra (vedi Figura 9) [17].

Nella steganografia si suppone che cambiando l'LSB del colore di ogni pixel di un'immagine, il singolo colore non risulti variato all'occhio umano. [17]

In questa trattazione [14] consideriamo **immagini a 8-bit** di dimensioni $\mathbf{n \times m}$ **.**

Il processo per l'introduzione del watermark, illustrato in Figura 10, prevede i seguenti passi:

1. I valori associati ai vari pixel dell'immagine host vengono convertiti in una rappresentazione binaria equivalente.
2. Anche il watermark, per semplicità di calcolo di dimensione $(\mathbf{n} \times \mathbf{m})/\mathbf{8}$ viene convertito in codice binario.
3. Il bit meno significativo di ogni pixel dell'immagine host (in questo caso l'ottavo bit) viene sostituito con il rispettivo bit del watermark.

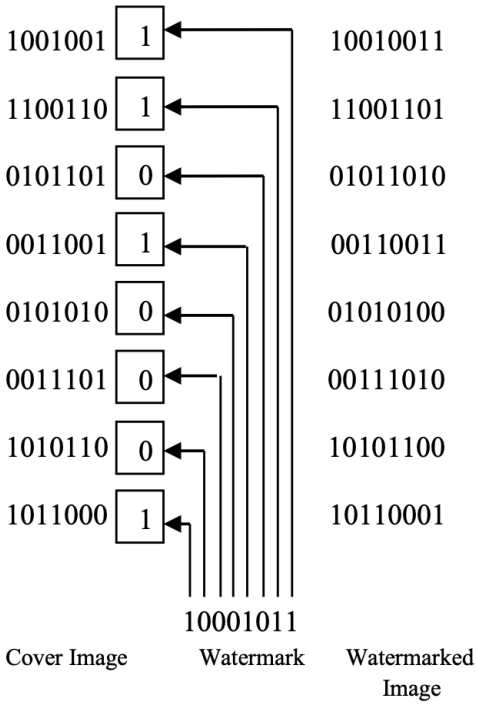


Figura 10: Inserimento del watermark tramite tecnica LSB. Ripresa da [14]

Per l'estrazione del watermark è sufficiente effettuare la correlazione tra quello che è il watermark atteso e l'immagine ricevuta.

Come ulteriore esempio consideriamo un pixel di intensità di grigio 130. La sua rappresentazione binaria è (10,000,010). Consideriamo inoltre il primo carattere binario del watermark essere 1. Dopo l'inserimento del watermark il binario diventa (10,000,011) che corrisponde al livello di grigio 131.

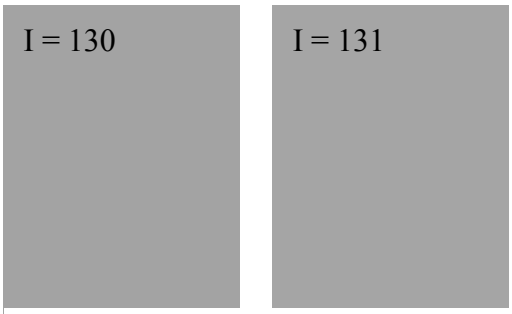


Figura 11: Differenza percettiva tra livelli di grigio simili. (es L1 = 130/255, L2 = 131/255)

Il sistema visivo umano non è in grado di percepire la differenza, tuttavia un hacker, data la semplicità dell'operazione, potrebbe.

3.2.2 Intermediate Significant Bit (ISB)

Le tecniche basate sull'utilizzo dell'LSB sono le più semplici ma non assicurano un buon livello di resistenza agli attacchi. Per questo motivo molti studi hanno sviluppato tecniche che sfruttano i bit intermedi di una sequenza invece che quello all'estremo destro [2].

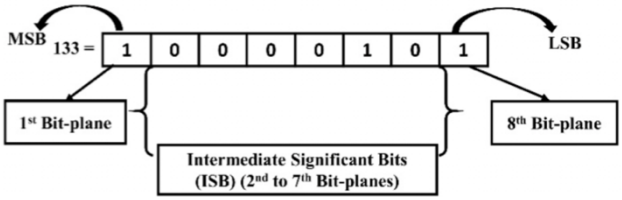


Figura 12: Inserimento del watermark tramite tecnica ISB. Ripresa da [2]

Questi algoritmi si sono dimostrati più robusti rispetto a diverse tecniche di image processing come filtraggio, compressione e rumore nonché rispetto ad attacchi geometrici come ritaglio e deformazione [2].

3.3 Metodi di Watermarking nel Dominio delle Frequenze

Per il fatto che possono essere facilmente manipolate, le tecniche di watermarking operanti nel dominio dello spazio sono troppo fragili. Per questo motivo, negli anni, ci si è focalizzati nell'implementare tecniche di watermarking che nascondano le informazioni all'interno di uno spazio trasformato invece che in quello originale [2].

Queste tecniche sfruttano un algoritmo in più passi leggermente più avanzato:

1. Utilizzando una specifica trasformata [ad es. DCT, DFT, DWT] l'immagine di host viene rappresentata dalle sue componenti nel dominio delle frequenze.
2. Il watermark viene successivamente inserito, con l'utilizzo di una chiave segreta, in specifiche componenti di frequenza modificando il valore assunto da queste.
3. Utilizzando una trasformata inversa si ottiene l'immagine contenente il watermark. Questa può ora essere condivisa attraverso un canale di comunicazione.
4. In fase di estrazione il watermark viene individuato tramite l'utilizzo di un processo inverso a quello di inserimento ma facendo uso della stessa chiave segreta.

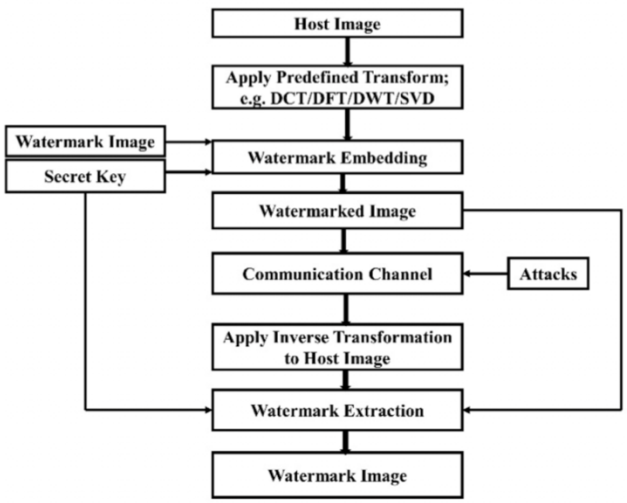


Figura 13: Schema di introduzione/estrazione del watermark nello spazio delle frequenze. Ripresa da [2]

Molti studi hanno dimostrato che algoritmi di watermarking operanti nel dominio delle frequenze sono in grado di garantire migliore robustezza, impercettibilità e sicurezza contro diverse tipologie di attacco come compressione, rumore, filtraggio, ritaglio, rotazione e deformazione.

3.3.1 Watermarking tramite Discrete Cosine Transform (DCT)

In queste tecniche si fa uso della Trasformata Discreta Coseno (DCT): una funzione che, presa in ingresso una sequenza finita di dati (nel nostro caso i valori associati ai pixel dell'immagine), restituisce una rappresentazione di questi sotto la forma di una serie finita di sinusoidi a diversa frequenza [18]. Può essere considerata come una semplificazione della Trasformata Discreta di Fourier in quanto considera solo la componente reale $Re(.)$ tralasciando quella immaginaria $Im(.)$. In quanto reale ed invertibile è utile sia per la conversione in frequenza dell'immagine host che per la trasformazione, nelle coordinate spaziali, successiva all'inserimento del watermark.

La trasformata uni-dimensionale discreta coseno (1D) DCT è definita dalla seguente equazione [2]:

$$y(k) = \alpha(k) \sum_{n=0}^{N-1} x(n) \cos\left(\frac{\pi(2n+1)k}{2N}\right), \qquad k = 0,1,\dots,N-1$$

(8)

Dove N è il numero di campioni, $x(n)$ sono i dati in ingresso, $y(k)$ i coefficienti DCT e $\alpha(k)$ un fattore di scala.

La trasformata inversa è invece definita come:

$$x(n) = \sum_{k=0}^{N-1} \alpha(k) y(n) \cos\left(\frac{\pi(2n+1)k}{2N}\right), \qquad n = 0,1,\dots,N-1$$

(9)

con:

$$\alpha(0) = \sqrt{\frac{1}{N}}, k = 0 \quad \text{e} \quad \alpha(k) = \sqrt{\frac{2}{N}}, 1 \le k \le N-1$$

(10)

Si prenda come esempio il metodo di watermarking DCT proposto da Mohamed Ali Hajjaji, Sondes Laajili, Abdellatif Mtibaa, El-Bey Bourennane [19].

Il loro studio prevede l'integrazione di dati relativi ad uno specifico paziente ed ospedale all'interno di un'immagine presente nella cartella clinica. Come watermark viene considerato un digest (ottenuto tramite hash function) rappresentativo dell'ospedale e dei dati anagrafici del paziente.

L'algoritmo si sviluppa nel seguente modo:

1. Il watermark, rappresentato dal digest identificativo del paziente e dell'ospedale viene convertito in una sua rappresentazione binaria.
2. L'immagine di host viene divisa in blocchi 8x8 sui quali si calcola poi la trasformata DCT (come avviene nella compressione JPEG).
3. Viene selezionata una banda di frequenze medie in cui inserire il watermark. Questo per garantire un buon compromesso tra degradazione dell'immagine e resistenza agli attacchi.
4. Per ogni blocco DCT si inserisce nella frequenza selezionata un bit del watermark binario.
5. Infine, si sfrutta la IDCT per generare l'immagine contenente il watermark.

Per la fase di estrazione è sufficiente seguire al contrario l'algoritmo sopra citato.

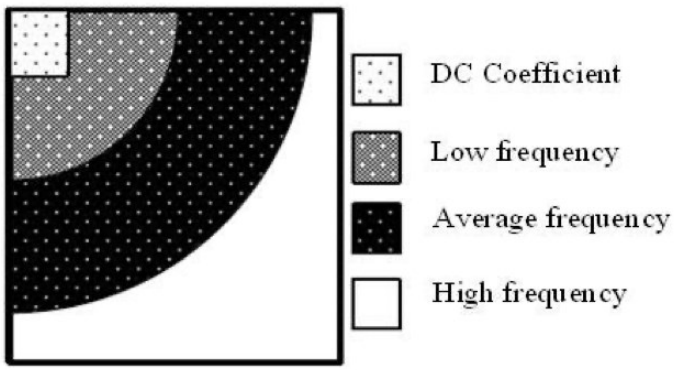


Figura 14: Scomposizione dello spettro di frequenze in: componente continua, basse, medie e alte frequenze Ripresa da [19]

Questa tipologia di watermarking permette di garantire un buon livello di qualità dell'immagine dopo l'inserimento del watermark. Inoltre, viene garantito un buon livello di sicurezza contro attacchi quali compressione e rumore. Lo stesso livello di sicurezza non è tuttavia garantito per alcune trasformazioni geometriche come, ad esempio, il ritaglio e la deformazione [2].

3.3.2 Watermarking tramite Discrete Wavelet Transform (DWT)

Un secondo metodo, sempre basato sull'analisi nel dominio delle frequenze, è quello che prevede l'utilizzo di una trasformata wavelet discreta [2].

La Trasformata Wavelet Discreta (DWT) [20] è uno strumento matematico in grado di decomporre gerarchicamente un'immagine in una serie di "piccole onde" di frequenza variabile e durata limitata. Il segnale originale può essere ricostruito utilizzando una trasformata inversa (IDWT).

La Trasformata DWT, nella sua versione bidimensionale, decompone l'immagine in un insieme di quattro sotto immagini (o sotto bande). Una di queste compone l'approssimazione dell'immagine originale mentre le altre tre ne identificano i dettagli [15].

In particolare, vengono definite le seguenti quattro bande:

1. Banda LL: Contiene le componenti a bassa frequenza sia lungo la direzione orizzontale che quella verticale
2. Banda LH: Contiene le componenti a bassa frequenza nella direzione orizzontale e quelle ad alta frequenza nella direzione verticale
3. Banda HL: Contiene le componenti ad alta frequenza nella direzione orizzontale e quelle a bassa frequenza nella direzione verticale
4. Banda HH: Contiene le componenti ad alta frequenza lungo entrambe le direzioni spaziali

La banda LL, raggruppando le componenti che hanno il maggior contenuto informativo, è una rappresentazione approssimata dell'immagine originale. Le altre tre bande invece sono identificative dei dettagli dell'immagine e in particolare delle porzioni a basso contenuto informativo.

Sfruttando questa suddivisone dell'energia dell'immagine è possibile inserire il watermark all'interno delle componenti delle bande di dettaglio (LH, HL, HH) essendo queste meno sensibili alla vista umana. Questo metodo permette di aumentare la robustezza del watermark senza compromettere sensibilmente la qualità dell'immagine.

Un algoritmo proposto da Mina Lala (MDS University, Ajmer, India) [15] applica i concetti sopra illustrati. In particolare, per il passo di inserimento del watermark, si procede nel seguente modo:

1. L'immagine host viene suddivisa nelle quattro bande rappresentative tramite 2D DWT
2. La stessa trasformata wavelet viene utilizzata sul watermark da inserire

3. Il watermark viene dunque inserito nelle bande rappresentative delle componenti ad alta frequenza tramite una tecnica dette "Alpha Blending" secondo la quale, l'immagine risultante, è ottenuta dalla seguente formula:

$$\mathrm{WMI} = k \cdot (HH) + q \cdot (\mathrm{WM}) \quad (11)$$

Dove $WMI = Immagine\ Risultante$, $HH = Banda\ di\ dettaglio$, WM = Watermark e con k, q fattori di scala.

4. L'immagine risultate è ottenuta tramite l'applicazione della trasformata inversa IDWT.

L'estrazione del watermark è possibile tramite "Alpha Blending" delle componenti ottenute riutilizzando la trasformata DWT [15]. La formula in questo caso è:

$$\mathrm{RW} = (\mathrm{WMI} - k \cdot \mathrm{HH}) \quad (12)$$

Dove RW = Watermark estratto, HH = Banda di dettaglio.

L'immagine originale è riottenuta sempre tramite trasformata inversa IDWT.

È interessante notare come, sostituendo la banda di dettaglio con la banda rappresentativa LL è possibile inserire nell'immagine un watermark visibile all'occhio umano [15].

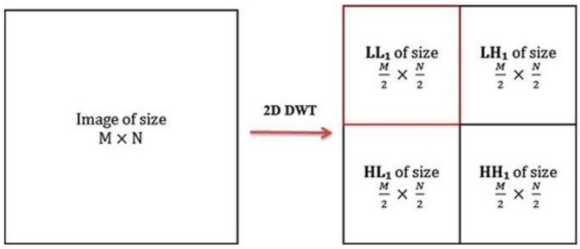


Figura 15: Decomposizione dell'immagine host nelle quattro bande: LL, LH, HL, HH. Ripresa da [15]

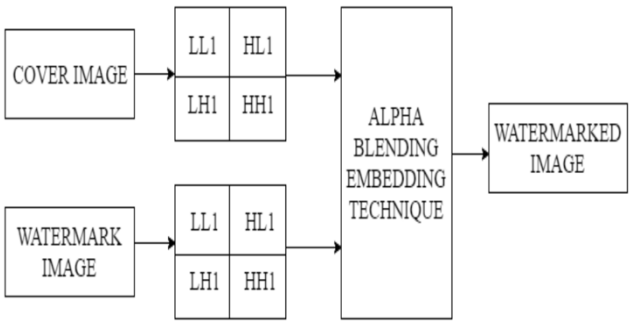


Figura 16: Schema di inserimento del watermark tramite DWT. Ripresa da [15]

3.4 Metodi di Watermarking Ibridi

Tra le varie tecniche di watermarking esistono anche quelle ibride. Queste, infatti, sfruttano una combinazione di algoritmi basati sia sullo spazio originale sia su quello trasformato. È dimostrato che questi algoritmi possono garantire una maggior robustezza e una migliore capacità di inserimento del watermark [2].

Ad esempio, nello studio effettuato da [21], il watermark viene duplicato e successivamente inserito sia nel dominio spaziale (modificando i valori dei bit meno significativi) che nel dominio trasformato (modificando i valori delle componenti in frequenza).

Lo schema ibrido si dimostra ottimo nel contrastare attacchi come la compressione JPEG, il filtraggio, il rumore e altri attacchi geometrici [2].

3.5 Considerazioni riassuntive

Da quanto appena descritto nei paragrafi precedenti, si può concludere che alcuni algoritmi di watermarking sono di facile implementazione ma hanno lo svantaggio di degradare la qualità dell'immagine e distorcerla. Altri algoritmi, invece, sono molto più complessi e di conseguenza più robusti e sicuri contro diverse tipologie di attacco. A seconda dei fini è preferibile scegliere un tipo di algoritmo rispetto ad un altro.

Capitolo 4: La valutazione dei sistemi di Image Watermarking

Un sistema di watermarking, oltre a confidenzialità, integrità e paternità, deve poter assicurare un buon compromesso tra robustezza, impercettibilità, e capacità (payload) [2]. Tuttavia, questo non è sempre facile. Per assicurare, ad esempio, un buon livello di impercettibilità, si potrebbe introdurre il watermark nelle componenti ad alta frequenza di una rappresentazione trasformata dell'immagine host. Questo però non garantisce un buon livello di robustezza, che è invece garantita dall'utilizzo delle componenti a bassa frequenza.

Risulta dunque utile, al fine di valutare la scelta di un metodo di watermarking rispetto ad un altro, una trattazione delle diverse tipologie di attacco e delle metodologie di valutazione delle performance dell'algoritmo di watermarking stesso.

4.1 Tipologie di attacco al Watermark

In un sistema di watermarking, qualsiasi processo che possa risultare in un danneggiamento del watermark o dell'informazione da esso protetta viene definito come un attacco [2]. Di conseguenza, i dati compromessi dall'attacco vengono definiti come "dati attaccati" o "dati esposti". Gli attacchi, che possono essere per la loro natura volontari o meno, causano distorsioni e modifiche dell'immagine contenente il watermark.

Di seguito vengono elencate e descritte diverse tipologie di attacco.

4.1.1 Attacchi Attivi

Un attacco è definito attivo quando un'entità, solitamente un hacker, individua e sfrutta una falla del sistema di individuazione del watermark per danneggiare o rimuovere il watermark stesso. Questo tipo di attacco prevede dunque l'accesso e la modifica dell'algoritmo di implementazione e la conseguente generazione di watemark distorti [2].

In alcuni casi il watermark può essere completamente rimosso dall'immagine di output che risulta comunque identica a quella di host (Elimination Attacks). In altri casi il watermark può essere mascherato in modo tale che, anche se presente, non possa essere riconosciuto dagli

algoritmi di estrazione (Masking Attacks). Infine, come terzo scenario, il sistema stesso può essere modificato in maniera tale da riconoscere watermark non validi (Forgery Attacks) [2].

4.1.2 Attacchi Passivi

Un attacco passivo al sistema di watermarking occorre nel caso in cui si cerchi di valutare la presenza di uno specifico watermark senza preoccuparsi della sua rimozione o del suo parziale danneggiamento. Si cerca dunque di estrarne le informazioni senza compromissione [2].

4.1.3 Attacchi di Rimozione

In un attacco di rimozione si cerca di cancellare il watermark dall'immagine senza utilizzare la chiave segreta utilizzata nella fase di inserimento [2].

Tra le varie modalità di un attacco di rimozione si possono considerare la compressione lossy, l'introduzione di rumore (gaussiano, sale e pepe), la quantizzazione e la collusione (eliminazione selettiva del watermark dall'immagine) [2].

Questi attacchi non sempre riescono ad eliminare completamente il watermark dall'immagine ma ottengono tuttavia un considerabile danneggiamento dell'informazione. Per questo motivo è necessario progettare un sistema di watermarking che renda il più difficile possibile l'attuazione di questo tipo di attacchi.

4.1.4 Attacchi Geometrici

Sono considerati geometrici gli attacchi che, invece di tentare la rimozione del watermark, cercano di distorcere il watermark per evitarne (o garantirne) il riconoscimento. Dopo un attacco geometrico, il watermark è ancora presente nell'immagine ma traslato, ruotato o deformato rispetto la sua posizione originale [2].

Sono considerati geometrici tutti quei processi di trasformazione (rotazione, ritaglio), miglioramento (correzione esposizione, contrasto, gamma) e degradazione dell'immagine che modificano l'immagine nelle sue caratteristiche geometriche [2].

Risulta importante la progettazione di un sistema di watermarking invariante ad attacchi geometrici come, ad esempio, operazioni RST (Rotation, Scaling, Traslation).

4.1.5 Attacchi Crittografici

Un attacco crittografico consiste nella compromissione del sistema di sicurezza dell'algoritmo. Prevede la ricerca, anche per forza bruta, delle chiavi di sicurezza utilizzate per l'introduzione e la successiva estrazione del watermark. Ottenute le chiavi è possibile modificare il procedimento di inserimento o eventualmente estrarre le informazioni senza essere autorizzati [2].

4.1.6 Rapporto costo-efficacia delle diverse tipologie di attacco

Il rapporto costo-efficacia di una tipologia di attacco ad un sistema di watermarking è solitamente basato sulla sua complessità computazionale e indica il costo (in termini di tempo di esecuzione e spazio di memoria) che è richiesto per portare a termine l'attacco [2].

Vengono definiti i seguenti parametri:

- K: Costo di individuazione delle chiavi di sicurezza
- E: Costo di inserimento del watermark. Valuta la robustezza e impercettibilità del sistema
- R: Costo di rimozione del watermark da parte di agenti esterni, senza l'uso delle chiavi di sicurezza
- G: Costo della distorsione geometrica

Di seguito vengono elencati i costi relativi a ciascuna tipologia di attacco precedentemente elencata:

Tabella 1: Formulazione costi di differenti tipologie di attacco. Ripresa da [2]

Tipologia di Attacco	Costo
Attivo	K + E + R
Passivo	K + E
Rimozione	R
Geometrico	K + E + G
Crittografico	K

4.2 Metriche di valutazione delle performance

La qualità dell'immagine risultante, in relazione a quella dell'immagine di host, è un criterio fondamentale per il riconoscimento di oggetti digitali come le immagini. Infatti, ad un alto

livello di degrado della qualità dell'immagine corrisponde una maggior probabilità che il watermark inserito non venga riconosciuto e dunque validato [2].

Come visto in precedenza, per la valutazione della qualità e delle performance di un sistema di watermarking, un buon indicatore risulta essere il rapporto segnale-rumore (PSNR) definito come il rapporto tra la massima potenza possibile del segnale e la potenza del rumore [2]. Esistono tuttavia altre tipologie di indicatori.

4.2.1 Errore Quadratico Medio (MSE)

In statistica, si definisce l'errore quadratico medio come la media delle discrepanze al quadrato tra i valori dei dati osservati e i valori dei dati attesi.

$$\text{MSE } = \frac{1}{N}\sum(y - \hat{y})^2$$

(13)

Applicato ad un sistema di watermarking l'errore quadratico medio calcola la media del quadrato degli scarti tra il watermark di riferimento (quello introdotto nell'immagine host) e il watermark estratto [2].

Come è facilmente verificabile, un più basso valore dell'MSE corrisponde ad una migliore correlazione tra il watermark originale e quello estratto e di conseguenza anche una migliore performance dell'algoritmo.

Spesso è utilizzato anche nella sua forma normalizzata (NSME).

4.2.2 Distanza Euclidea (DE)

Ogni immagine è memorizzata nei computer come un vettore di numeri che la possono descrivere completamente.

La distanza euclidea, definita come distanza di Minkowski di ordine $p = 2$, rappresenta la distanza tra due punti qualsiasi in uno spazio n-dimensionale [22]. È dunque possibile utilizzarla per valutare le differenze tra il watermark originale e quello estratto.

$$dist(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{\frac{1}{p}}$$

(14)

$$DE = \sqrt{\sum_{i=1}^{n} (x_i - y_1)^2}$$

(15)

4.2.3 Structural Similarity Index (SSIM)

L'indice di similarità strutturale di un'immagine è una metrica percettiva che quantifica la degradazione della qualità di un'immagine sottoposta a compressione e trasmissione.

In particolare, SSIM valuta la differenza percettiva tra due immagini senza indicare esplicitamente quale delle due immagini sia migliore (questa classificazione è lasciata all'operatore che ha conoscenza di quale sia l'immagine originale e quale invece quella modificata) [23].

Questa metrica richiede di avere a disposizione sia l'immagine originale che l'immagine risultante. [24]

Il valore di SSIM è calcolato nel seguente modo:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

(16)

Dove:

- μ_x è un pixel di intensità media dell'immagine x
- μ_y è un pixel di intensità media dell'immagine y
- σ_x è la varianza dell'immagine x
- σ_y è la varianza dell'immagine y
- σ_{xy} è la covarianza di x e y
- $c_1 = (0.01 \cdot L)^2$, $c_2 = (0.03 \cdot L)^2$ dove L è il range dinamico

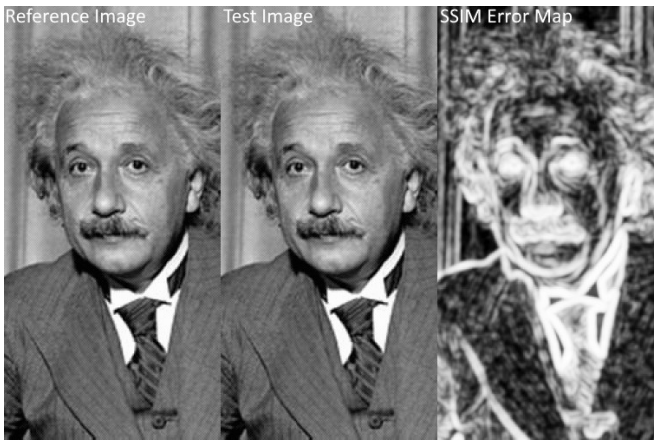


Figura 17: Valutazione visiva dello Structural Similarity Index nella differenza tra immagine host e immagine elaborata. Ripreso da [29]

Uno studio [25] ha dimostrato che, mentre PSNR e MSE restituiscono un errore assoluto, l'indice di similarità strutturale fornisce un errore percettivo basato sul sistema visivo umano. Per questo motivo SSIM risulta più facilmente interpretabile per la valutazione delle performance dell'algoritmo.

4.3 Considerazioni riassuntive

In questo capitolo sono state evidenziate caratteristiche e problematiche di diversi algoritmi di digital image watermarking. Queste tecniche vengono utilizzate come metodo alternativo per assicurare integrità e paternità di un'immagine condivisa lungo un canale di comunicazione oppure archiviata in un server.

Per le sue molteplici caratteristiche e per il contemporaneo alto livello di qualità e robustezza, le tecniche di watermarking basate sulla trasformata DWT sembrano essere le migliori. Tuttavia, è quasi impossibile poter assicurare contemporaneamente un alto livello di robustezza, impercettibilità e capacità. Bisogna dunque individuare un buon compromesso tra questi requisiti fondamentali e scegliere il miglior algoritmo a seconda delle nostre necessità.

Capitolo 5: Uso del Digital Image Watermarking in Sanità

5.1 Sicurezza nei Sistemi Informativi Sanitari

I servizi di teleconsulto e telediagnosi sviluppati negli ultimi anni hanno instaurato nuovi metodi per l'archiviazione, accesso e condivisione di dati sanitari e introdotto nuove modalità, per i pazienti e per i dottori, per accedere alla propria cartella clinica. Tuttavia, questi benefici comportano anche nuove criticità dovute all'archiviazione e condivisione di documenti sensibili tramite Internet e network accessibili da una moltitudine di persone [16].

Tutte le informazioni relative al paziente, che siano raccolte in una cartella digitale o meno, devono sottostare al segreto professionale e dunque essere confidenziali.

La sicurezza delle informazioni mediche del paziente, dettata da forti regole etiche e da leggi di carattere nazionale ed europeo [4] [16], impone tre caratteristiche principali:

1. **Confidenzialità**: Solo le persone autorizzate, come il paziente e il personale medico, hanno modo di accedere alle informazioni.
2. **Autenticazione**: Deve essere garantita una prova che effettivamente l'informazione appartiene al paziente corretto e che non è stata modificata senza autorizzazione.
3. **Disponibilità**: L'informazione deve essere sempre accessibile da chi è autorizzato.

5.2 Requisiti del watermark in applicazioni sanitarie

Con l'obbiettivo di soddisfare i requisiti sopra citati, un algoritmo di watermarking utilizzato per garantire la sicurezza di informazioni cliniche deve sottostare a diversi vincoli di progettazione che ne complicano la realizzazione.

5.2.1 Impercettibilità e Reversibilità

La qualità delle immagini biomediche è di estrema importanza per la loro interpretazione e per il loro studio da parte del personale medico. Una perdita di dettaglio e qualità potrebbe infatti comportare ad una diagnosi diversa ma soprattutto sbagliata; questo a spese della salute del paziente.

I metodi di watermarking implementati in sanità devono dunque essere reversibili e garantire che l'immagine originale, utilizzata come host per il watermark, possa essere ricostruita in maniera esatta dopo l'estrazione del marker.

Questo limita di molto la capacità (payload) informativa dell'immagine biomedicale di host e di conseguenza rende inutilizzabili molti metodi di watermarking.

Un modo per ovviare a questo problema è quello di definire delle regioni di interesse (ROI), all'interno delle immagini biomedicali, che devono essere lasciate intatte, e delle zone sicure dove invece è possibile inserire il watermark senza danneggiare i dettagli importanti alla diagnosi [26].

Un secondo metodo potrebbe essere quello di utilizzare algoritmi che, pur operando su tutta l'immagine, non determinano variazioni di qualità e dettaglio apprezzabili dal sistema visivo umano [2].

5.2.2 Controllo dell'Integrità

Sempre con lo scopo di garantire un valore legale e medico alle immagini, il sistema di watermarking in sanità deve tenere conto delle deformazioni, volontarie o no, che l'immagine subisce durante il processo di archiviazione e condivisione.

Per garantire un livello di integrità accettabile è possibile definire un valore di partenza e valutare, in fase di estrazione, lo scostamento di questo dal valore iniziale. Nel caso in cui la variazione di integrità (spesso calcolata in base al contenuto e non in modo assoluto) sia compresa all'interno di una soglia predeterminata, l'immagine può essere considerata intatta e valida per essere utilizzata [2].

5.2.3 Autenticazione

Un requisito critico in un sistema di watermarking per la sanità è quello di garantire l'autenticazione dei documenti. In particolare, se l'immagine in questione appartiene al corretto paziente e se è stata generata e condivisa da un ente autorizzato.

Solitamente nei sistemi di cartella sanitaria digitale si allega all'immagine un documento esterno contenente tutti i metadata relativi al paziente e all'immagine stessa. Il fatto di avere però due documenti separati può dare luogo a problematiche e facilitare la riuscita di un attacco esterno.

Il watermark permette di introdurre le stesse informazioni all'interno dell'immagine stessa e di tenerle contemporaneamente celate alle persone non autorizzate [27].

Risulta quindi essenziale garantire una buona capacità di payload. Se per un'immagine di qualità televisiva il payload medio varia tra 1 e 100 bits, per le bioimmagini, essendo solitamente file ad alta risoluzione, ci si può aspettare un payload di una decina di bit per ogni Megabit di dati.

5.3 Diverse applicazioni del watermarking in sanità

Come già accennato in precedenza, il digital watermarking di immagini ha il potenziale di risolvere diversi problemi legati alla gestione e alla condivisione di dati sanitari raccolti all'interno di una cartella clinica elettronica.

Tramite l'introduzione, all'interno di un'immagine, di uno o molteplici watermark è infatti possibile assicurare integrità e paternità delle informazioni nonché inserire ulteriori metadata, utili in ambito medico, all'interno dell'immagine stessa.

5.3.1 Controllo degli accessi

Tramite l'inserimento di un watermark altamente robusto e resistente agli attacchi è possibile assicurare l'accesso alle informazioni e garantire la loro autenticità solamente alle persone autorizzate (come il personale sanitario e il paziente).

Inserendo invece un watermark molto fragile e sensibile alle trasformazioni è possibile avvisare gli utenti nel caso il file sia stato condiviso un numero eccessivo di volte (ad esempio da un hacker) o nel caso questo sia uscito dal regolare canale di comunicazione [16].

5.3.2 Verifica del mittente

Inserendo tramite image digital watermarking una sequenza identificativa dell'istituto sanitario e del personale medico è possibile effettuare una verifica sull'identità (paternità) dei documenti condivisi e ricevuti [16].

5.3.3 Verifica dell'integrità

Sempre tramite l'utilizzo di un watermark fragile è possibile verificare se il documento, nel nostro caso l'immagine, sia stata manomessa o eccessivamente degradata. Di conseguenza è

quindi possibile valutare se l'immagine, dopo la condivisione, sia ancora rappresentativa dal punto di vista medico e valida dal punto di vista legale [16].

5.3.4 Annotazione di informazioni

Oltre che assicurare l'integrità e la paternità di un'immagine, il watermark può essere utilizzato anche come metodo per allegare, all'interno dell'immagine stessa, dati relativi ad una possibile diagnosi oppure informazioni sensibili riguardanti il paziente stesso. Anagrafica, patologie pregresse, prescrizioni sono solamente alcune delle informazioni allegabili che possono essere estremamente utili (in termini pratici) se contenute all'interno dell'immagine [16].

5.3.5 Indicizzazione

Il watermark può inoltre essere utilizzato per inserire, all'interno dell'immagine, parole chiave e indici utili all'archiviazione e organizzazione dei documenti all'interno dei server di una struttura sanitaria. Questo risulterebbe in una maggior facilità e rapidità nella ricerca delle informazioni di un paziente nel momento in cui ve ne fosse la necessità [16].

5.3.6 Pseudonimizzazione

Il watermark permette di introdurre informazioni invisibili all'osservatore all'interno delle immagini. Per questo motivo il digital image watermarking può essere visto come un modo per slegare informazioni sensibili e riservate riguardanti il paziente da quelle oggettive e pubbliche utilizzabili in ricerca e in analisi statistiche [16].

Capitolo 6: Approfondimento: metodo di watermarking basato su DFT per bioimmagini

6.1 Specifiche del contesto

Le ultime versioni di radiografi, tomografi e macchine per la risonanza magnetica generano immagini nel formato DICOM®. Questo formato prevede di allegare un "file header", contenente tutti i metadati necessari, all'immagine stessa [28]. Tuttavia, il fatto di avere le informazioni slegate dal supporto multimediale aumenta le probabilità di attacco e la possibilità che queste informazioni vengano danneggiate o addirittura perse.

L'inserimento di un watermark in grado di identificare le informazioni e di essere contemporaneamente parte dell'immagine risolverebbe il problema. D'altro canto, l'inserimento di un watermark comporta una degradazione dell'immagine che potrebbe perdere il suo valore medico e legale.

Uno studio, di Manuel Cedillo-Hernandez, Francisco J. Garcia-Ugalde, Mariko Nakano-Miyatake, Hector M. Perez-Meana [27], ha proposto un robusto algoritmo di watermarking basato sulla trasformata discreta di Fourier e specificamente progettato per essere utilizzato su immagini mediche come radiografie, risonanze magnetiche o tomografie.

6.2 Analisi dell'algoritmo

Nell'implementazione di questo algoritmo [27] si considera come watermark un pattern binario 1-dimensionale generato a partire da una chiave segreta e indicante, ad esempio, l'identità del paziente soggetto all'esame medico.

Questo pattern, dopo essere stato permutato per mezzo di una seconda chiave segreta, viene inserito nelle componenti a media frequenza della trasformata DFT dell'immagine. Questo per garantire al contempo un buon livello di robustezza e impercettibilità. L'immagine risultante è poi ottenuta tramite trasformata inversa IDFT.

Per estrarre l'informazione si calcolano le componenti in frequenza dell'immagine ricevuta e si effettua un'analisi del bit-error-rate (BER) per ricostruire il watermark.

6.2.1 Inserimento del Watermark

L'inserimento del watermark prevede un processo in più fasi:

1. Il watermark W viene generato come una serie unidimensionale binaria tramite l'utilizzo di una chiave privata k_1.

$$W = (w_i | \, j = 1 \dots L) \tag{17}$$

   dove L è la lunghezza del watermark

2. Si ottiene una permutazione non casuale W_1 delle componenti del watermark. Questa è generata tramite una seconda chiave segreta k_2. Questo passaggio aumenta la sicurezza dell'algoritmo.
3. Viene letta l'immagine DICOM in scala di grigi e scalata ad una dimensione di 512x512.
4. Viene applicata la trasformata 2D DFT all'immagine host

$$I(u,v) = \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} i(x,y) e^{-j2\pi(f_1 x/N_1 + f_2 y/N_2)} \tag{18}$$

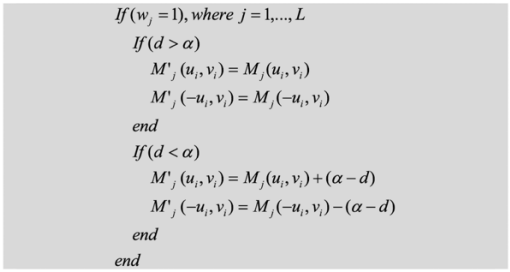
   Ottenendo il modulo $M(u,v)$ e la fase $P(u,v)$

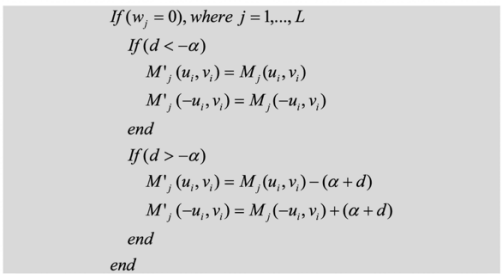
5. Vengono scelti una coppia di raggi $r_1 e \, r_2$ e l'area del relativo anello circolare

$$A = \pi(r_2^2 - r_1^2) \tag{19}$$

   I valori delle distanze radiali devono essere scelti in modo tale che l'area A, centrata nel valore di frequenza nulla, copra le componenti a media frequenza.
   Vengono scelte le componenti di media frequenza per garantire un buon livello di impercettibilità e al contempo evitare che il watermark venga eliminato dalle alte frequenze durante la compressione JPEG.
   Per assicurare la corretta implementazione del watermark si deve garantire $(A/4) \geq L$

6. Viene definito un parametro α e il watermark viene inserito seguendo il seguente metodo [27]:





7. L'immagine contenente il watermark viene ottenuta tramite la trasformata inversa discreta di Fourier (IDFT) come segue:

$$i' = \mathrm{IDFT}(I') \tag{20}$$

8. L'immagine viene riscalata alle sue dimensioni originali MxN.

6.2.2 Estrazione del Watermark

L'algoritmo di estrazione e riconoscimento del watermark è descritto dai seguenti passaggi:

1. L'immagine viene scalata ad una dimensione standard di 512x512.
2. Viene calcolata la trasformata 2D DFT e il relativo modulo e fase.
3. Utilizzando la stessa area circolare A si individuano le componenti a media frequenza
4. Il watermark W' viene calcolato nel seguente modo:

$$if\ d \geq 0 \rightarrow w'_j = 1$$
$$else\ w'_j = 0$$

5. Il watermark originale W viene riordinato con una permutazione inversa basandosi sulla chiave segreta k_2. Si calcola infine il bit-error-rate (BER).

6.3 Risultati

Questo algoritmo [27] di watermarking basato sul dominio delle frequenze è stato testato su diverse tipologie di immagini mediche in formato DICOM.

In particolare, ne sono state valutate le performance su tre tipologie diverse di bioimmagini:

- Radiografia Digitale (CR) in scala di grigi (4280x3520x10 bits) [a]
- Tomografia Digitale (CT) in scala di grigi (1024x1024x16 bits) [b]
- Risonanza Magnetica (MR) in scala di grigi (512x512x16 bits) [c]

Il watermark utilizzato nei test è una sequenza binaria 1-D di dimensione $L = 64$.

Gli iperparametri dell'algoritmo sono invece:

- $r_1 = 80$
- $r_2 = 81$
- $\alpha = 55$

Le performance sono state valutate dal punto di vista dell'impercettibilità e della robustezza valutando gli indici di PSNR e SSIM.

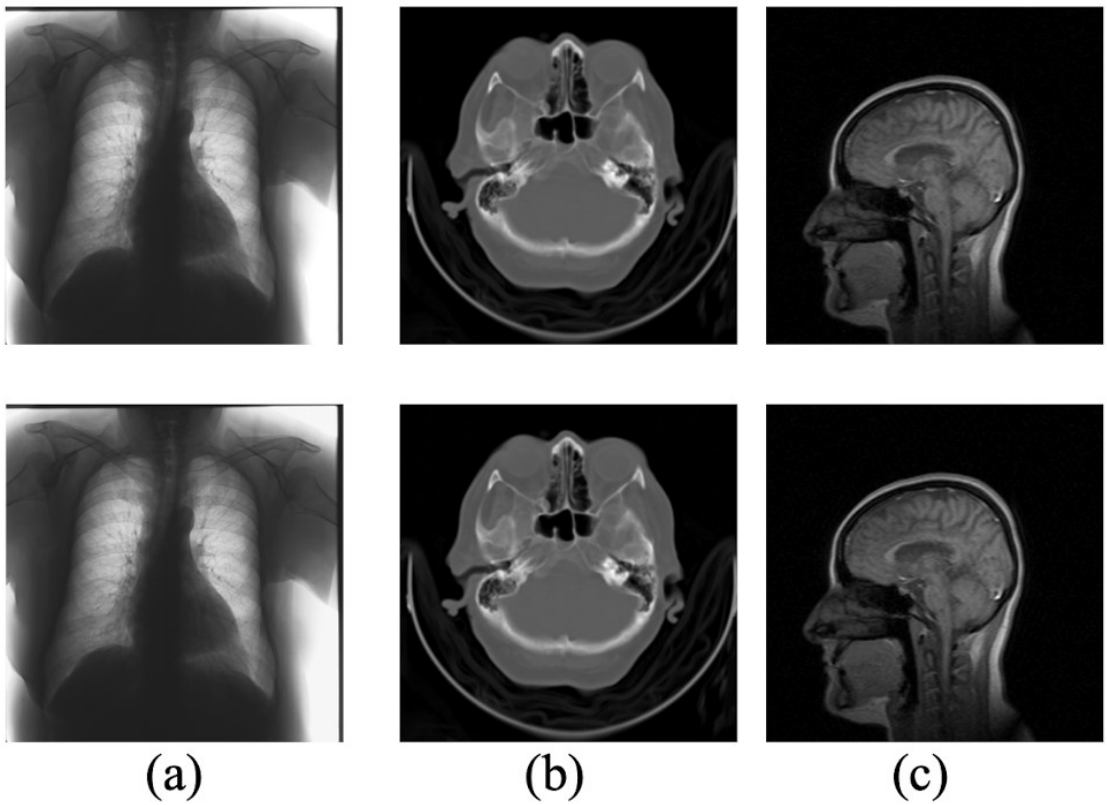


Figura 18: Differenza tra immagine host (sopra) e immagine contenente il watermark (sotto) in una radiografia digitale (a), tomografia digitale (b), risonanza magnetica (c). Ripreso da [27]

6.3.1 Impercettibilità del Watermark

L'impercettibilità del watermark è stata valutata usando le seguenti metriche:

$$PSNR(dB) = 10\,log_{10}\frac{M \cdot N \cdot \text{Max Pixel Value}^2}{\sum_i \sum_j \left(I_o(i,j) - I_w(i,j)\right)^2} \quad (21)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (22)$$

Dai dati sperimentali si osserva che l'algoritmo proposto garantisce una discreta fedeltà dell'immagine risultante rispetto a quella di host con valori di PSNR e SSIM maggiori rispettivamente di 50 dB e 0.98.

Tabella 2: Impercettibilità valutata tramite PSNR e SSIM

Image	PSNR (dB)	SSIM
Lungs (CR)	55.12	0.9954
Brain (CT)	53.82	0.9949
Head (MR)	50.33	0.9892

6.3.2 Robustezza del Watermark

Per la valutazione della robustezza, le immagini sono state sottoposte ad una serie di diversi attacchi geometrici.

Dalla tabella si può verificare che il watermark risulta essere robusto a tutti gli angoli di rotazione nonché alla traslazione e vari fattori di ritaglio.

L'algoritmo risulta inoltre essere robusto rispetto a comuni deformazioni come la compressione JPEG e quella DICOM ma anche rispetto al rumore gaussiano e a variazioni di luminosità e contrasto.

Distortion	CR	CT	MR
Without distortion	0	0	0
DICOM JPEG LOSSLESS	0	0	0
DICOM JPEG LOSSY (QF=50)	0	0.03	0.01
DICOM JPEG RLE	0	0	0
Sharpening 3x3	0	0.03	0
Gaussian Noise M=0, σ^2=0.001	0	0.09	0.07
Median filter 3x3	0	0.03	0
Brightened	0	0.07	0.07
Contrasted	0.01	0.01	0.03
Impulsive noise density=0.001	0.01	0.07	0.03
Gaussian filter 3x3	0	0.03	0
Translation x=25, y=25	0	0	0.01
Rotation 35°	0.03	0	0.03
Scaling 0.4	0	0	0.03

Tabella 3: Valutazione delle performance di resistenza a differenti attacchi. Ripresa da [27]

Capitolo 7: Conclusione

Con l'avvento di nuove tecnologie digitali e con l'utilizzo di queste in sostituzione ai vecchi sistemi informativi cartacei, il mondo ospedaliero e quello della sanità in generale hanno avuto a disposizione mezzi estremamente più efficienti nell'archiviazione e condivisione sicura di dati considerati sensibili da regolamenti come il GDPR. Tuttavia, in parallelo, sono aumentati in maniera esponenziale il numero di attacchi e di furti di dati delle strutture sanitarie. I numeri lo dimostrano; solo nel 2021, negli Stati Uniti, sono stati registrati più di 700 attacchi di larga scala a sistemi informativi sanitari (contro i 18 nel 2009) [3].

I nuovi sistemi di digital watermarking sembrano poter essere di enorme aiuto, in bioingegneria, nell'assicurare l'integrità e la paternità di bioimmagini (come CT, CR e MR) [27].

Nonostante i rigidi vincoli, imposti in ambito medico, nel garantire la massima qualità e massima sicurezza di un'immagine medica, la progettazione di un algoritmo di watermarking digitale per bioimmagini non è di impossibile realizzazione. Selezionando le giuste trasformazioni, nel dominio dello spazio o in quello delle frequenze, è possibile progettare sistemi di digital watermarking robusti contro molte tipologie di attacco e al contempo in grado di non degradare l'immagine (o quantomeno di non rendere visibile la degradazione all'occhio umano).

Oltre a ciò, l'utilizzo di un watermark consente ulteriori vantaggi come la possibilità di introdurre metadati del paziente all'interno del supporto multimediale stesso e la possibilità di creare database di ricerca in cui i dati sensibili sono nascosti.

Tuttavia, ad oggi, il watermarking digitale di immagini non è utilizzato in larga scala nel campo della sanità digitale a causa della sua recente affinazione ma anche a causa di approvazioni medico-legali che devono essere concesse.

A mio personale parere, il digital watermarking di immagini si prospetta essere, dal punto di vista ingegneristico, un'interessante alternativa ad altri metodi di verifica (come la firma digitale) per la sua capacità di sfruttare il supporto multimediale stesso per celare informazioni confidenziali e allo stesso tempo ridurre la probabilità di successo di un attacco hacker.

Bibliografia

[1] N. Anju Latha, B. Rama Murthy, and U. Sunitha, "Electronic Health Record", *International Journal of Engineering Research & Technology*, vol.1, no.10, 2012.

[2] M. Begum and M. S. Uddin, “Digital Image Watermarking Techniques: A Review,” *Information*, vol. 11, no. 2, p. 110, Feb. 2020.

[3] HIPAA Journal, "Number of healthcare data breaches involving the loss of 500 or more records in the United States from 2009 to 2021", HIPAA Journal, 2022.

[4] Commissione Europea, "Regolamento UE n. 2016/679 (GDPR) ", [Online]. Avaliable: "https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32016R0679", [Accessed: Nov. 17, 2022]

[5] R. Kaur , A. Kaur, "Digital Signature", *2012 International Conference on Computing Sciences, 2012,* pp. 295-301, 2012.

[6] Verified Market Research, "Global Photo Editing App Market Size By Product Type (Android/iOS, Windows), By End User (Personal User, Enterprise User), By Geographic Scope And Forecast", VMR®, 2022.

[7] H. Tao, L. Chongmin, J. Zain e A. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review", *JART,* vol. 12, n. 1, 2014.

[8] "Watermark", [Online]. Available: https://en.wikipedia.org/wiki/Watermark, [Accessed: Nov. 17, 2022].

[9] R.G. Schyndel, A.Z. Tirkel and C.F.Osbome, “A Digital Watermark”, in Proceedings of IEEE International Conference on Image Processing (ICIP’94), V01.2, 1994, pp. 86 -90.

[10] H. Yang, Y. Liang, X. Wang e S. Ji, "A DWT-Based Evaluation Method of Imperceptibility of Watermark in Watermarked Color Image", *Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition,* 2007.

[11] "Spread Spectrum", [Online]. Available: https://it.wikipedia.org/wiki/Spread_spectrum, [Accessed: Nov. 17, 2022].

[12] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in *IEEE Access*, vol. 6, pp. 19876-19897, 2018

[13] "Distanza di Hamming", [Online]. Available: https://it.frwiki.wiki/wiki/Distance_de_Hamming, [Accessed: Nov. 17, 2022]

[14] N. Bansal, V. K. Deolia, A. Bansal and P. Pathak, "Digital Image Watermarking Using Least Significant Bit Technique in Different Bit Positions," *2014 International Conference on Computational Intelligence and Communication Networks*, 2014, pp. 813-818.

[15] H. Lala, "Digital Image Watermarking using Discrete Wavelet Transform", *International Research Journal of Engineering and Technology (IRJET),* vol. 4, n. 1, 2017.

[16] A. Giakoumaki, S. Pavlopoulos and D. Koutsouris, "A Multiple Watermarking Scheme Applied to Medical Image Management," *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2004, pp. 3241-3244.

[17] "Least Significant Bit", [Online]. Available: https://it.wikipedia.org/wiki/Bit_meno_significativo, [Accessed: Nov. 17, 2022].

[18] "Trasformata Discreta del Coseno", [Online]. Available: https://it.wikipedia.org/wiki/Trasformata_discreta_del_coseno, [Accessed: Nov. 17, 2022].

[19] Mohamed Ali Hajjaji, Sondes Laajili, Abdellatif Mtibaa, El-Bey Bourennane. A Digital Watermarking Algorithm Based on DCT: Application on Medical Image. International Conference on EMBEDDED SYSTEMS in TELECOMMUNICATIONS and INSTRUMENTATION (ICESTI'12), Nov 2012, Algeria.

[20] "Discrete Wavelet Transform", [Online]. Available: https://en.wikipedia.org/wiki/Discrete_wavelet_transform, [Accessed: Nov. 17, 2022].

[21] F. Shih e S. Wu, "Combinational Image Watermarking in the Spatial and Frequency Domains", *J.Pattern Recognit.,* vol. 36, pp. 969-975, 2003.

[22] "Distanza di Minkowski", [Online]. Available: https://it.wikipedia.org/wiki/Distanza_di_Minkowski, [Accessed: Nov. 17, 2022].

[23] "SSIM", [Online]. Available: https://www.imatest.com/docs/ssim/, [Accessed: Nov. 17, 2022].

[24] "Structural Similarity", [Online]. Available: https://en.wikipedia.org/wiki/Structural_similarity, [Accessed: Nov. 17, 2022]

[25] U. Sara, M. Akter e M. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE, and PSNR-A Comparative Study", *J. Comput. Commun.,* vol. 7, 2019.

[26] D. Ravichandran, P. Praveenkumar, S. Rajagopalan, J.B.B Rayappan,R. Amirtharajan, "ROI-based medical image watermarking for accurate tamper detection, localisation and recovery", *Med Biol Eng Comput, vol 6,* 2021.

[27] M. Cedillo-Hernandez, F. J. Garcia-Ugalde, M. Nakano-Miyatake and H. M. Perez-Meana, "DFT-Based Watermarking Method for Medical Images," *2012 IEEE Ninth Electronics, Robotics and Automotive Mechanics Conference*, 2012, pp. 21-24

[28] W.D. Jr Bidgood, S.C. Horii, F.W. Prior, D.E. Van Syckle, "Understanding and using DICOM, the data interchange standard for biomedical imaging", *J Am Med Inform Assoc,* 1997.

[29] "Structural Similarity in Neural Style Transfer", [Online]. Available: https://matthewmcateer.me/posts/ssim-aware-style-transfer/, [Accessed: Nov. 17, 2022]

[30] Yang, Baohui et al. “Matlab-based GUI for medical image processing.” *BioTechnology: An Indian Journal* 8 (2013), [Online]. Available: https://www.semanticscholar.org/paper/Matlab-based-GUI-for-medical-image-processing-Yang-Wang/a217fd274962e020286817379e1beb75be0f8561, [Accessed: Nov. 17, 2022].