DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA,
ELETTRONICA E SISTEMISTICA

Corso di Laurea Magistrale in Ingegneria Informatica

Machine & Deep Learning

Relazione

Re-Engineering AE-XAD with Vision Transformers for Explainable Anomaly Detection

Professore:
Prof. **Fabrizio Angiulli**

Studente:
Presta Vincenzo
matr. 252290

ANNO ACCADEMICO 2024/2025

AE-XAD - ViT

Elaborato finale: Machina & Deep Learning

Vincenzo Presta

Novembre 2025

Indice generale

1 Introduzione

L'anomaly detection su immagini è un compito particolarmente complesso, poiché richiede non solo l'identificazione di osservazioni che deviano dal comportamento normale, ma anche la capacità di spiegare quali componenti dell'immagine giustifichino tale devianza. In numerosi contesti applicativi — come ispezione industriale, manutenzione predittiva o monitoraggio di qualità — non è sufficiente stabilire se un'immagine sia anomala: è necessario produrre una spiegazione interpretabile e coerente che evidenzi le regioni responsabili dell'anomalia.

La letteratura tradizionale sull'Explainable Artificial Intelligence (xAI) si è concentrata principalmente su modelli di classificazione o regressione, mentre una minore attenzione è stata dedicata al problema dell'Explainable Anomaly Detection (xAD). Tuttavia, le peculiarità del rilevamento di anomalie rendono i metodi post-hoc scarsamente efficaci in questo scenario [**?**]. In particolare, tre criticità strutturali ostacolano l'applicazione diretta delle tecniche di spiegabilità classiche:

- **Rarità delle anomalie:** i difetti sono poco rappresentati e non esiste un processo affidabile per generarli artificialmente in modo realistico; ciò limita l'uso di metodi post-hoc basati sull'abbondanza di esempi anomali.
- **Eterogeneità delle anomalie:** forme, estensioni e intensità possono variare significativamente rendendo difficile definire un modello universale.
- **Bassa fedeltà delle spiegazioni post-hoc:** tali metodi operano su modelli già addestrati, non progettati per essere esplicabili, producendo mappe che spesso non riflettono accuratamente le regioni realmente responsabili dell'anomalia.

A fronte di questi limiti, è cresciuto l'interesse verso approcci *explainability-by-design*, ossia modelli che integrano il meccanismo di spiegazione all'interno del processo di addestramento. In questo contesto si colloca **AE–XAD**, un metodo basato su Autoencoder che ha come obiettivo non solo il rilevamento dell'anomalia, ma anche la produzione di una *heatmap* interpretabile in grado di evidenziare le regioni che più contribuiscono al comportamento anomalo.

Il problema affrontato da AE–XAD può essere formulato come segue:

> *Data un'immagine potenzialmente anomala, determinare non solo se essa contenga difetti, ma anche quali regioni dell'immagine siano responsabili della deviazione rispetto al comportamento normale.*

I metodi ricostruttivi convenzionali, come gli Autoencoder standard, non sono sufficienti per questo scopo: tendono infatti a ricostruire anche le regioni anomale e a produrre mappe di errore poco informative e rumorose. AE–XAD supera tali limitazioni introducendo una strategia di addestramento semi-supervisionata progettata per:

- ricostruire accuratamente i pixel normali;

- ricostruire intenzionalmente *in modo errato* i pixel anomali;
- generare una heatmap stabile, coerente e interpretabile basata sull'errore di ricostruzione.

Nelle sezioni successive si analizzeranno i principi operativi del metodo, la formulazione matematica della loss, la struttura dell'architettura e il processo di generazione della heatmap.

2 Formulazione del problema

Sia un insieme di training $X = \{x_1, \ldots, x_n\}$, dove ciascuna osservazione $x_i \in [0,1]^D$ rappresenta un'immagine normalizzata. Per ogni immagine è inoltre disponibile una heatmap binaria $y_i \in \{0,1\}^D$, che specifica per ciascun pixel se esso sia normale ($y_{i,j} = 0$) oppure anomalo ($y_{i,j} = 1$). Come indicato in [**?**], una heatmap assume valore zero ovunque per gli esempi *inlier*, mentre presenta almeno un pixel attivo per gli esempi *outlier*.

La quantità $\|y_i\|_1$ (somma degli elementi della heatmap) permette di distinguere formalmente:

- gli **inlier**, caratterizzati da $\|y_i\|_1 = 0$;
- gli **outlier**, per cui $\|y_i\|_1 > 0$.

Sia inoltre I l'insieme degli indici degli inlier e O quello degli outlier, come definito nel paper.

Il compito del modello, dato un insieme di immagini di test $T = \{t_1, \ldots, t_m\}$, consiste nel generare per ciascuna immagine una heatmap h_i che stimi il contributo di ogni pixel all'anomalia complessiva. La heatmap può essere:

- **binaria**, con $h_{i,j} \in \{0,1\}$;
- **continua**, tipicamente $h_{i,j} \in [0,1]$, indicando il grado di outlierness del pixel.

Come descritto in [**?**], la dimensione del dato D coincide con $H \times W \times C$, ovvero le dimensioni spaziali e il numero di canali dell'immagine. L'obiettivo finale è definire per ogni immagine un valore di *anomaly score* $S(t_i)$, idealmente proporzionale alla presenza e all'estensione delle regioni anomale.

Il problema posto da AE–XAD può quindi essere formalizzato come segue:

> dato un insieme limitato di esempi anomali annotati a livello pixel, addestrare un modello capace di ricostruire fedelmente le regioni normali e di enfatizzare, attraverso la ricostruzione, le regioni anomale, così da ottenere una heatmap interpretabile che evidenzi i pixel maggiormente responsabili della devianza.

Questo scenario rientra nel paradigma della *semi-supervised anomaly detection*, poiché il modello sfrutta informazioni supervisionate limitate (le heatmap anomale sparse) e, al tempo stesso, apprende la distribuzione dei pixel normali da grandi quantità di dati privi di difetti.

3 Architettura del modello

L'architettura di AE–XAD è composta da un encoder convoluzionale pre-addestrato, da un decoder con struttura biforcata e da un modulo finale che combina le due ricostruzioni per ottenere un'immagine finale $\tilde{x}$. Come descritto in [**?**], la rete è progettata per guidare l'Autoencoder verso una ricostruzione accurata dei pixel normali e, al contempo, una ricostruzione intenzionalmente distante dei pixel anomali, secondo quanto imposto dalla loss semi-supervisionata.

3.1 Encoder

L'encoder è costruito selezionando i primi tre blocchi residuali di una rete ResNet pre-addestrata su ImageNet. Tale scelta consente di sfruttare un estrattore di feature robusto ed efficiente, capace di catturare strutture di basso e medio livello utili per la fase di ricostruzione. L'output della ResNet viene poi passato attraverso un ulteriore strato convoluzionale che riduce il numero di canali, producendo una rappresentazione latente di dimensione $28 \times 28 \times 64$. Come specificato nel paper, i pesi del modello ResNet rimangono congelati durante l'addestramento, al fine di ridurre il costo computazionale e preservare le capacità generalizzative dell'encoder pre-addestrato.

3.2 Decoder

Il decoder di AE–XAD è articolato in due rami paralleli, ciascuno con un ruolo distinto nel processo di ricostruzione dell'immagine.

Branch 1 (non-trainable). Questo ramo effettua un semplice upsampling della rappresentazione latente, da $28 \times 28 \times 64$ fino a $224 \times 224 \times 64$. Viene quindi applicata una funzione `tanh`, e successivamente i 64 canali vengono compressi tramite somma in gruppi da 8, producendo un tensore $b_1 \in \mathbb{R}^{224 \times 224 \times 8}$. Tale ramo funge da "maschera morbida" (*soft mask*) che enfatizza o attenua regioni specifiche della ricostruzione finale.

Branch 2 (trainable). Questo ramo comprende tre blocchi convoluzionali, ciascuno costituito da una convoluzione seguita da una trasposed convolution con attivazione SeLU. L'obiettivo è ricostruire progressivamente dettagli strutturali e texture dell'immagine, generando un tensore $b_2 \in \mathbb{R}^{224 \times 224 \times 8}$.

3.3 Combinazione dei due rami

Come riportato in [**?**], i due rami vengono combinati tramite la seguente operazione per-pixel:

$$b = b_1 \cdot b_2 + b_2.$$

Il termine b_1 agisce come una maschera adattiva che amplifica o sopprime particolari regioni di b_2. Questo meccanismo consente al decoder di focalizzare la

ricostruzione nelle aree più informative, favorendo un errore di ricostruzione più marcato nelle regioni anomale durante l'addestramento.

Due ulteriori strati convoluzionali affiancati a valle di questa combinazione rifiniscono l'immagine ricostruita e convertono il tensore risultante in un output finale $\tilde{x} \in \mathbb{R}^{224\times224\times3}$, con la stessa dimensione dell'immagine di input.

3.4 Considerazioni architetturali

L'utilizzo di un encoder pre-addestrato e congelato riduce il costo computazionale e stabilizza l'addestramento, mentre la struttura biforcata del decoder permette di controllare con precisione la ricostruzione delle regioni anomale attraverso la loss specifica. Questa architettura rappresenta un compromesso efficiente tra capacità espressiva, interpretabilità e sostenibilità computazionale, come evidenziato dagli esperimenti presentati nel paper.

4 Loss Function

La componente centrale di AE–XAD è una loss semi-supervisionata progettata per ottenere una ricostruzione accurata delle regioni normali e, al tempo stesso, una ricostruzione deliberatamente distante nelle regioni anomale. Come mostrato in [**?**], dato un campione $x \in [0,1]^D$ e la relativa heatmap binaria $y \in \{0,1\}^D$, la loss per-pixel è definita come:

$$\ell(x,y) = \sum_{j=1}^{D} \left[(1-y_j)\, \frac{(x_j - \tilde{x}_j)^2}{(F(x_j) - x_j)^2} \;+\; \lambda_y\, y_j\, \frac{(F(x_j) - \tilde{x}_j)^2}{(F(x_j) - x_j)^2} \right]. \tag{1}$$

La loss totale sull'intero training set è data da:

$$L(X,Y) = \frac{1}{|X|} \sum_{(x,y)\in X\times Y} \ell(x,y). \tag{2}$$

4.1 Interpretazione dei termini

La formulazione della loss riflette due comportamenti distinti:

- **Pixel normali ($y_j = 0$):**

$$\frac{(x_j - \tilde{x}_j)^2}{(F(x_j) - x_j)^2}.$$

  In questo caso, il modello è incentivato a ricostruire fedelmente il pixel originale x_j. Il denominatore normalizza l'errore affinché i contributi siano comparabili tra diversi valori di intensità.

- **Pixel anomali ($y_j = 1$):**

$$\lambda_y \frac{(F(x_j) - \tilde{x}_j)^2}{(F(x_j) - x_j)^2}.$$

  Qui il modello non deve ricostruire x_j, ma deve avvicinare $\tilde{x}_j$ al valore trasformato $F(x_j)$, forzando un errore di ricostruzione elevato nelle regioni anomale. Questo comportamento è essenziale affinché la differenza $|x_j - \tilde{x}_j|$ diventi un indicatore affidabile di anomalia.

4.2 Ruolo della trasformazione F

La funzione $F : [0, 1] \to \mathbb{R}$ è un iperparametro introdotto per massimizzare la distanza di ricostruzione nelle regioni anomale. Due scelte discusse in [**?**] sono:

- $F_-(x) = 1 - x$, che rappresenta il negativo del pixel;
- $F_v(x) = v$, con $v \notin [0, 1]$ (nel paper viene utilizzato $v = 2$).

In entrambi i casi, $F(x_j)$ è costruita per essere distante dall'originale x_j, aumentando così l'ampiezza dell'errore ricostruttivo nelle zone anomale.

4.3 Peso di bilanciamento λ_y

Il coefficiente λ_y compensa lo sbilanciamento tra pixel normali e anomali:

$$\lambda_y = \begin{cases} D/\|y\|_1 & \text{se } \|y\|_1 > 0, \\ 1 & \text{altrimenti.} \end{cases}$$

Poiché le anomalie sono generalmente molto rare nello spazio dei pixel, λ_y evita che la loss sia dominata dai termini relativi ai pixel normali.

4.4 Effetto complessivo della loss

Complessivamente, la loss in Eq. (1) realizza un comportamento *explainability-by-design*: le regioni normali vengono ricostruite con accuratezza, mentre quelle anomale vengono ricostruite in modo intenzionalmente errato. La differenza tra immagine originale e ricostruita diventa così una stima affidabile dell'outlierness locale, utilizzabile per generare heatmap interpretabili.

5 Training Strategy

L'addestramento di AE–XAD segue una strategia semi-supervisionata che combina data augmentation mirata e oversampling, con l'obiettivo di compensare la scarsità e l'eterogeneità delle anomalie nel dataset. Come proposto in [**?**], la pipeline di training si articola in due componenti principali.

5.1 Data augmentation sulle anomalie

Poiché gli esempi anomali sono poco rappresentati e spesso molto diversi tra loro, AE–XAD applica un potenziamento artificiale dei campioni anomalie prima dell'addestramento. In particolare, per ogni immagine anomala x nel training set:

- essa viene replicata 5 volte senza modifiche;
- ulteriori 10 copie vengono generate tramite una procedura di *copy–paste*: la regione anomala viene ritagliata e incollata su immagini normali, dopo trasformazioni geometriche standard (zoom, rotazioni, traslazioni, ecc.).

Questa strategia migliora la diversità delle anomalie osservate dal modello e rafforza la sua capacità di generalizzare a difetti di forma e dimensione variabili.

5.2 Oversampling all'interno del batch

Dopo l'augmentation, ogni batch B viene bilanciato imponendo la seguente proporzione:

$$\frac{1}{3}|B| \quad \text{anomalie}, \qquad \frac{2}{3}|B| \quad \text{inlier}.$$

Questa scelta contrasta l'effetto predominante dei pixel normali nella loss e garantisce che il modello riceva un segnale supervisionato sufficiente durante l'ottimizzazione, senza sovraccaricare il training con esempi anomali artificiali.

5.3 Ottimizzazione

AE–XAD viene addestrato per 200 epoche utilizzando l'ottimizzatore Adam con learning rate pari a 10^{-3} e weight decay pari a 10^{-4}, come riportato in [**?**]. La ResNet dell'encoder è mantenuta congelata durante tutto l'addestramento, mentre solo i livelli convoluzionali del decoder vengono aggiornati.

6 Inference e generazione delle heatmap

Durante la fase di inference, AE–XAD utilizza l'errore di ricostruzione per individuare le regioni anomale dell'immagine. Il processo, descritto in [**?**], si articola in tre passaggi principali: calcolo dell'errore, normalizzazione e filtraggio tramite una finestra gaussiana adattiva.

6.1 Errore di ricostruzione

Dato un test sample t, si calcola la ricostruzione $\tilde{t}$ ottenuta dall'Autoencoder e si definisce il vettore di errore:

$$e = (t - \tilde{t})^2.$$

L'errore contiene valori elevati nelle regioni in cui il modello non ha tentato di replicare fedelmente l'input, tipicamente corrispondenti alle zone anomale.

6.2 Normalizzazione

Per rendere l'errore confrontabile attraverso pixel e immagini, AE–XAD applica la normalizzazione seguendo la procedura definita in Eq. (3):

$$\tilde{e} = \frac{e - \mu_e}{\sigma_e},$$

dove μ_e e σ_e sono media e deviazione standard dei valori in e. La mappa normalizzata $\tilde{e}$ funge da *raw heatmap*, evidenziando in modo preliminare le regioni devianti.

6.3 Selezione automatica del filtro gaussiano

Per migliorare la coerenza spaziale della heatmap, viene applicato un filtro gaussiano F_k di dimensione $(2k+1) \times (2k+1)$. La dimensione k non è fissata a priori, ma viene stimata automaticamente da AE–XAD sulla base delle proprietà geometriche delle anomalie. In particolare [**?**]:

1. si considera la mappa binarizzata di $\tilde{e}$ utilizzando la soglia $\mu_{\tilde{e}} + \sigma_{\tilde{e}}$;
2. si analizzano in tale mappa le componenti connesse per stimare l'estensione media delle regioni anomale, orizzontalmente e verticalmente;
3. il valore k viene scelto come metà della maggiore tra tali estensioni.

In questo modo, il filtro si adatta alle dimensioni effettive del difetto, evitando sia oversmoothing su anomalie piccole sia dispersione su anomalie estese.

6.4 Heatmap filtrata e binarizzazione

Applicando il filtro gaussiano, si ottiene la heatmap finale:

$$h = F_k(\tilde{e}).$$

Se è richiesta una segmentazione binaria delle anomalie, la heatmap viene ulteriormente sogliata usando:

$$\text{threshold} = \mu_h + \sigma_h,$$

dove μ_h e σ_h sono media e deviazione standard dei valori in h.

6.5 Anomaly score

AE–XAD definisce un anomaly score più robusto rispetto alla norma dell'errore grezzo, sfruttando la coerenza spaziale enfatizzata dal filtro:

$$S(t) = \|e \cdot F_k(e)\|.$$

Questa formulazione privilegia regioni in cui l'errore è consistente e spazialmente continuo, riducendo l'impatto del rumore isolato e migliorando la capacità di rilevare difetti piccoli ma strutturati.