Regular Paper

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

具授權閘控之可逆重建機制的隱私保護監控影像人臉軌跡檢索

江柔萱[1]、龐靚伊[2]、周永振[3*]
[123]逢甲大學人工智慧技術與應用學位學程
[1] {stella.lala1002, kellyxx931028, yungchen}@gmail.com

摘要

監控系統必須在保障公眾隱私與滿足執法機關的證據回復需求之間取得平衡。現有方法不是儲存原始人臉資料(造成隱私侵犯)，就是將殘差嵌入影片(無法跨攝影機進行搜尋)。本論文提出一種新穎的混合式架構，結合向量資料庫以實現即時人臉軌跡檢索，以及具備授權門控的可逆重建功能。系統首先由人臉感興趣區域 (ROI) 提取加入隱私保護的人臉嵌入向量 (ArcFace＋ 對抗性雜訊)，並將其索引於 Milvus (向量資料)，以支援跨 CCTV 網路的快速近似最近鄰 (ANN) 搜尋能力。完成配對的軌跡則透過區塊鏈雜湊值鏈結至存放於 IPFS 的殘差資料，並僅在授權驗證後啟用像素級精確重建。

關鍵詞：人臉去識別化、向量資料庫、可逆匿名化、監控隱私、區塊鏈鑑識

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

Privacy-Preserving Face Trajectory Retrieval in Surveillance Video with an Authorization-Gated Reversible Reconstruction Mechanism

Rou-Syuan Jiang[1], Ching-Yi Pang, Yung-Chen Chou[1*]
[1]Bachelor's Degree Program in Artificial Intelligence Technology and Application, Feng Chia University
[1]{stella.lala1002, kellyxx931028, yungchen}@gmail.com

Abstract

Surveillance systems require balancing public privacy with law enforcement's need for forensic evidence recovery. Existing approaches either store raw face data (a privacy violation) or embed residuals into videos (no cross-camera search capability). VectorChain introduces a novel hybrid architecture that combines vector databases for real-time face-trajectory retrieval with warrant-gated reversible reconstruction. Face ROIs extract privacy-preserving embeddings (ArcFace+adversarial noise) indexed in Milvus for sub-second approximate nearest neighbor (ANN) search across CCTV networks. Matching trajectories link to IPFS-stored residuals via blockchain hashes, enabling pixel-perfect reconstruction only after warrant verification.

Keywords: Face de-identification, vector databases, reversible anonymization, surveillance privacy, blockchain forensics

壹、前言

全球各地的閉路電視 (Closed-Circuit Television, CCTV) 系統每日產生高達 PB 級的影像資料，構成公共安全、刑事調查與都市分析等應用的重要基礎。然而，隨著 GDPR (General Data Protection Regulation，一般資料保護規則)、CCPA (California Consumer Privacy Act，加州消費者隱私法)、PIPEDA (Personal Information Protection and Electronic Documents Act，加拿大個人資訊保護與電子文件法)以及我國《個人資料保護法》(Personal Data Protection Act, PDPA) 等隱私法規持續強化全球資料保護要求，監控系統的營運者正面臨一項長期存在的監管悖論：一方面，系統必須在符合法律程序與正當授權的前提下，保有辨識個體身分的能力；另一方面，卻同時被禁止以原始且可識別的形式儲存生物特徵資訊。此兩難困境導致視覺監控領域長久以來存在三項核心挑戰，即隱私性 (privacy)、可搜尋性 (searchability) 與可回復性 (reversibility)。

首先，隱私保護的法規限制明確禁止儲存可識別個人身分的人臉影像。傳統的去識別化方法，如模糊化 (blurring)、像素化 (pixelation) 或遮罩 (masking)，雖能移除身分識別資訊，卻同時嚴重削弱後續分析與應用所需的資料效用。較為先進的可逆式去識別化技術 (reversible de-identification)，例如 UU-Net，可生成具備寫實外觀的匿名人臉，同時嵌入足夠資訊以支援日後的身分重建。相關研究顯示，UU-Net 證實以生成對抗網路 (GAN) 為基礎的替代影像，能在受控存取條件下保留姿態、光照與背景的一致性，並於後續階段實現身分回復 [1]。然而，此類方法多半僅運作於單一影格 (frame-level) 層級，尚未提供有效的跨攝影機檢索機制。

其次，在執法應用情境中，可搜尋性仍屬於不可或缺的系統需求，因為調查人員必須在大規模攝影機網路中追蹤特定對象的行為軌跡。逐影格的人臉去識別化處理會破壞用於索引與檢索的關鍵判別特徵，而將可逆式身分嵌入資訊分別儲存於各個影片之中，亦缺乏跨攝影機一致性，難以支援可靠的多視角軌跡關聯。另一方面，向量資料庫系統能夠提供高吞吐量的近似最近鄰 (Approximate Nearest Neighbor, ANN) 搜尋能力，但若直接儲存原始人臉嵌入向量，系統將暴露於嵌入重置攻擊 (embedding inversion attacks) 的風險之中，使攻擊者得以由潛在向量重建可識別的人臉影像，進而違反隱私法規並削弱公眾對監控系統的信任。

可回復性 (reversibility) 是指在符合法律授權的情況下重建原始人臉影像的能力，目前有基於流模型 (flow-based) 與可逆式神經網路 (invertible neural networks) 的研究中獲得探討。例如，PRO-Face S 採用具備金鑰控制回復機制的可逆網路架構，僅在提供正確密碼學金鑰時，方能對人臉影像進行安全轉換與後續重建 [2]。此類系統在存取控制層面提供了高度的安全保證，然而現有設計尚未整合高效能的跨攝影機搜尋能力，亦未納入符合現代數位鑑識流程需求的令狀 (warrant) 導向的人臉影像重建機制。

綜合而言，現有研究方法多半在三項核心需求之間進行取捨：強調隱私保護的系統往往缺乏可搜尋性；以嵌入向量為核心的檢索流程則難以滿足隱私要求；而具備可逆特

性的技術又欠缺可擴展的跨攝影機索引能力。因此，目前尚無任何既有解決方案能同時支援以下三項關鍵目標：(1) 符合隱私法規的資料儲存機制，(2) 於大規模攝影機網路中進行快速且準確的人臉軌跡檢索，以及 (3) 具備授權閘控 (authorization-gated) 且可稽核之原始人臉身分重建流程。

本文提出 VectorChain，一種混合式系統架構，整合具隱私保護特性的可逆式表徵、高效能向量資料庫檢索機制，以及受授權控制的人臉身分重建流程。該系統首先擷取人臉感興趣區域 (Region of Interest, ROI)，並將其轉換為經隱私保護處理的嵌入向量，同時注入對抗性雜訊 (adversarial noise)，再以 Milvus 為基礎的向量資料庫架構中實現快速的近似最近鄰 (ANN) 搜尋能力。其後，系統將匹配之人臉軌跡透過密碼學鏈結方式進行關聯，並利用區塊鏈雜湊機制加以錨定，而可逆式身分殘差則儲存於去中心化的儲存環境中。原始人臉身分僅能在經由授權閘控 (authorization-gated) 的程序予以重建，確保隱私保護為系統之預設狀態，而身分回復則成為受到嚴格規範與監管的例外行為。本研究之主要貢獻可歸納如下：

(一) VectorChain 架構：串聯 ANN 軌跡搜尋、授權狀驗證與可逆式重建之監控系統框架

本研究提出點到點 (end-to-end) 的整合式監控系統架構，在同一體系中協同整合下列關鍵技術要素：

- 具隱私保護特性、且適用於高速向量搜尋的人臉嵌入表徵；
- 透過大規模近似最近鄰 (Approximate Nearest Neighbor, ANN) 索引實現的跨攝影機人臉軌跡檢索；
- 基於密碼學令狀 (cryptographic warrants) 之授權控制可逆式身分重建機制。

此一統一化設計使閉路電視 (CCTV) 基礎架構得以在執行日常營運與分析任務的同時，確保任何涉及身分揭露的行為皆受到嚴格規範，並具備完整的可稽核性 [18] [19]。

(二) 兼顧隱私保護與身分相似性之嵌入表徵：對抗 GAN 反推攻擊的設計

本研究基於 ArcFace 架構，提出一套經對抗式訓練 (adversarial training) 之嵌入模組，並引入具隱私保護特性的擾動機制，以提升對身分反推攻擊的防禦能力 [5] [10]。所生成之嵌入表徵具備以下關鍵特性：

- 對生成對抗網路 (GAN) 反推攻擊 (inversion attacks) 展現高度抗性，其重建結果之 Fréchet Inception Distance (FID) 大於 25，顯示回復影像在感知層面上與原始人臉存在顯著差異；
- 在檢索應用中仍能有效維持身分一致性，同一身分之嵌入向量間餘弦相似度 (cosine similarity) 可達 0.92 以上；
- 對近似最近鄰 (ANN) 索引具備良好強韌性，得以在分散式攝影機網路中實現安全且高效的向量化搜尋。

此一設計在隱私保護與實用效能之間建立了具原則性的平衡，回應了過往可逆式系統中尚未被充分解決的核心挑戰 [1] [2] [3] [4] [6]。

(三) 鏈上／鏈下混合式儲存機制：以區塊鏈確保完整性，結合去中心化殘差保存

VectorChain 提出一種鏈上 (on-chain) 與鏈下 (off-chain) 並行的混合式儲存架構，整合以下兩項核心設計：

- 透過鏈上雜湊機制，確保人臉軌跡資料與身分殘差之完整性與不可竄改性 [18]；
- 採用去中心化儲存系統 (IPFS)，並以內容可定址識別碼 (Content Identifier, CID) 保存可逆式身分殘差資料 [17]。

此一架構對多種實務環境中的風險情境具備高度韌性，包括：

- 編碼器與解碼器之間可能產生的不一致性；
- 網路中斷或系統節點暫時不可用的狀況；
- 影音編碼所引發的特徵漂移 (codec-induced drift)，例如 H.264 壓縮效應；
- 數位鑑識流程中對資料可追溯性與可稽核性的要求。

透過將可搜尋之嵌入向量與可逆式身分殘差進行明確分離，本系統確保任一單獨元件皆不足以完成身分重建，從系統架構層面強化整體隱私保護能力 [2] [3] [19]。

(四) 數位鑑識完整性保證與選擇式身分重建授權機制

為確保證據使用之可靠性，本研究針對常見影音壓縮流程下之重建品質進行形式化分析。定理一 (Theorem 1) 刻畫了在人臉影像經 H.264 重新編碼後，可逆式重建品質之下界，確保身分回復結果仍符合數位鑑識應用之有效性要求。

此外，系統支援選擇式 ROI 重建機制，僅允許經令狀授權之特定感興趣區域進行解密與回復 [7]。此一設計可實現具細緻度的身分揭露控制，相較於整幀影像解密，更能符合隱私保護與法規遵循之要求 [19]。

貳、文獻探討

2.1 可逆式人臉去識別化 (Reversible Face De-Identification)

可逆式人臉去識別化旨在於一般使用者觀看情境下保護人臉身分，同時允許經合法授權之單位以高保真度回復原始人臉內容。相較於不可逆的遮蔽方法(例如模糊化或像素化)，可逆式方案係明確為合法檢視與數位鑑識重建流程所設計，以支援後續的司法與調查需求。**UU-Net** 以視覺監控影片為主要應用場域，強調在公開發布之影像串流中兼顧隱私保護與鑑識需求之平衡。UU-Net 建立一條可公開使用的去識別化串流，同時為具權限之單位保留私有的重建能力，並主張在假設僅限授權端可用之元件下，重建應能「僅依賴」公開資料完成 [1]。此外，該方法透過影像隱寫術將感興趣區域 (Region of Interest, ROI) 資訊嵌入公開串流，使重建階段得以沿用相同的 ROI 對齊方式；此一設計至關重要，因為 ROI 對齊誤差有可能影響重建品質。

近期有學者提出由隱寫式殘差設計轉向結合可學習的可逆模型與密碼學控制機制。**PRO-Face S** 提出一套基於安全串流模型 (flow-based invertible model) 的可逆保護統一

框架，透過生成一幅在視覺上近似於預先遮蔽目標的保護影像，並利用模型本身的可逆性恢復原始內容 [2]。其關鍵貢獻在於引入金鑰控制機制：僅於提供正確密鑰時，方能獲得正確的恢復結果；若使用錯誤密鑰，則僅會產生失真之重建影像。該設計亦考量實務部署需求，例如採用具有限參數規模的輕量化可逆網路，以提升實際可行性。

另一項互補性研究方向，則是將密碼學直接整合至身分特徵之中，以實現更強的存取控制機制。Gu 等學者提出將格式保持式加密 (Format-Preserving Encryption, FPE) 嵌入人臉置換流程 (如 FaceShifter 與 SimSwap)，在生成去識別化人臉的同時，僅允許持有金鑰之授權使用者回復原始身分 [3]。該方法採用 FF3 FPE (基於 AES-128) 結構，並詳細說明在對稱式金鑰機制下，如何於維持資料格式的前提下完成加解密。當可逆性需由明確的密碼學授權機制所治理，而非僅依賴模型保密性時，此類方法具備高度吸引力。

現有可逆式去識別化系統多半侷限於單一影像或單一影片串流層級運作，其研究重點在於生成受保護之視圖並支援後續回復。例如，UU-Net 著重於匿名化串流的發布，以及利用嵌入其中的 ROI 中繼資料於同一串流內完成重建；PRO-Face S 與基於 FPE 的方法亦同樣聚焦於保護與回復機制，未將跨攝影機的人臉軌跡檢索視為核心設計目標。

2.2 監控系統中的向量資料庫與隱私議題 (Vector Databases in Surveillance Retrieval)

近年來，向量資料庫 (Vector Databases) 已成為大規模監控分析與人臉再識別 (Face Re-identification, Re-ID) 系統中的關鍵基礎設施。代表性系統如 Milvus、Pinecone 與 FAISS，透過高效的近似最近鄰 (Approximate Nearest Neighbor, ANN) 索引結構，使高維嵌入向量得以在大規模資料集中進行即時相似度搜尋。以 Milvus 為例，其結合 HNSW (Hierarchical Navigable Small World) 索引後，可在包含百萬級以上人臉嵌入的資料庫中，維持低於 10 ms 的查詢延遲，已被廣泛應用於即時人臉搜尋與跨攝影機再識別任務 [8]。

在實務應用中，向量資料庫常被用於「以圖搜人」或「以人找軌跡」的任務流程，即由執法人員提供嫌疑人照片，系統生成對應嵌入後，於多攝影機資料庫中檢索相似影格或軌跡，以支援事後調閱與行為分析 [10]。相較於逐影片或逐攝影機比對，此類向量化檢索架構在可擴展性與即時性上具有明顯優勢，已逐漸成為智慧監控系統的主流設計。然而，既有向量資料庫導向的監控系統多半隱含一個關鍵假設，即「人臉嵌入向量本身是安全的」。近期研究已指出，這一假設在隱私層面上並不成立。多項工作顯示，攻擊者即便無法取得原始人臉影像，仍可透過生成式對抗網路 (GAN) 或專用反演模型，從嵌入向量中重建具高度可辨識性的人臉外觀 [6] [14]，在部分設定下甚至可達接近 98% 的重建成功率。此結果揭示，嵌入向量本身已構成高度敏感的生物特徵資料，其外洩風險不亞於原始影像 [5]。

此類嵌入反演風險亦與近年可逆式人臉去識別化 (Reversible Face De-identification) 研究形成對比。既有方法如 UU-Net [1]、可逆流模型 (Secure Flow) [2]、格式保持加密

(FPE) [3] 與身分解耦式操控 [4]，多著重於影像或影片層級的視覺隱私保護與授權回復機制，但普遍未將「跨攝影機向量檢索」視為核心設計目標，因此難以直接支援大規模、多攝影機的即時追蹤與搜尋需求。在此背景下，現有向量資料庫系統雖在檢索效能上表現優異，卻普遍缺乏對嵌入層級隱私威脅的系統性防護機制，亦未提供與法律授權(如令狀)相結合的存取控制與稽核設計。

2.3 嵌入隱私與重建攻擊 (Embedding Privacy and Reconstruction Attacks)

隨著深度人臉辨識技術的成熟，基於嵌入向量 (face embeddings) 的人臉表徵方式(如 ArcFace、FaceNet) 已成為監控與再識別系統中的主流設計 [10]。然而，近期研究逐漸指出，這類嵌入向量本身並非隱私安全的中介表示。多項工作證實，即使攻擊者僅能存取嵌入向量，而無法取得原始人臉影像，仍可透過深度學習模型進行有效的反演重建 [6]。特別是結合生成式對抗網路 (GAN) 的嵌入反演攻擊，已被證明可從高品質人臉嵌入中回復具高度可辨識性的人臉外觀。其中，StyleGAN 及其後續架構因其優異的生成能力，被廣泛用於嵌入反演任務，能在特定設定下生成與原始人臉在視覺與身分層面高度相符的重建結果 [14]。相關研究顯示，當嵌入向量直接對應於身分判別空間時，其反演成功率可達極高水準，凸顯嵌入向量本身已構成敏感的生物特徵資料 [6]。

針對此類隱私風險，部分研究提出在嵌入層級引入防禦機制。其中一類方法透過對抗性擾動 (adversarial perturbation) 干擾嵌入向量的可反演性，使生成模型難以重建原始人臉。Wang 等人提出的隱私保護對抗人臉特徵 (Privacy-preserving Adversarial Facial Features) 即顯示，適當設計的對抗性雜訊可顯著降低反演結果的影像品質指標 (如 FID)，在部分實驗中可將 FID 提升至 25–30 的區間，從而削弱 GAN 反演的有效性 [5]。另一類方法則引入差分隱私 (Differential Privacy) 理論，透過在嵌入生成過程中加入受控隨機雜訊，以提供形式化的隱私保證，例如在隱私參數 $\epsilon \approx 1.2$ 的設定下，限制單一樣本對嵌入分佈的影響 [15]。

然而，現有嵌入隱私防禦方法普遍面臨一項關鍵限制：隱私強化往往伴隨下游任務效能的明顯下降。無論是對抗性擾動或差分隱私噪聲，均可能破壞嵌入空間的判別結構，進而降低人臉再識別或向量檢索的準確度，使其難以直接應用於即時監控與跨攝影機搜尋等高精度需求場景 [5] [15]。相較之下，既有可逆式人臉去識別化研究 (如 UU-Net、Secure Flow、FPE-based 方法) 主要聚焦於影像或影片層級的視覺隱私保護與授權回復 [1] [2] [3]，或透過身分解耦操控實現可逆的人臉外觀轉換 [4]，但多未將「嵌入向量本身的隱私風險」與「大規模向量檢索需求」納入同一系統性設計考量。

2.4 區塊鏈鑑識溯源 (Blockchain-based Forensic Traceability)

隨著監控系統在公共安全與執法領域中的應用規模不斷擴大，如何確保監控資料於

事後鑑識流程中的完整性、可驗證性與問責性，已成為隱私保護之外的另一項關鍵研究議題。近年來，新興研究開始引入區塊鏈技術，以其去中心化與不可竄改 (immutability) 的特性，作為監控鑑識資料的可信稽核基礎 [16] [18]。在監控鑑識場景中，一類典型作法是將影像或人臉軌跡的雜湊值逐幀或逐事件記錄於區塊鏈上，以建立可驗證的時間序列證據鏈。由於區塊鏈中每筆交易皆受到密碼學雜湊與共識機制保護，任何事後對監控資料的未授權修改，皆可透過鏈上雜湊比對被即時偵測，從而提升證據於司法程序中的可信度與抗否認性 [16]。此類方法特別適用於高風險或高爭議性的執法應用情境。

然而，受限於區塊鏈的儲存成本與吞吐量，直接將大量影像或影片資料上鏈並不可行。因此，多數研究採取「鏈上索引、鏈下儲存」的混合式設計，將實際影像內容或高頻殘差資料存放於分散式檔案系統中，如 IPFS (InterPlanetary File System)，並僅於區塊鏈上記錄對應的內容識別碼 (Content Identifier, CID) 與雜湊摘要 [17]。IPFS 所提供的內容位址化 (content-addressed) 與版本控制機制，使資料可在分散式環境中被可靠定位與驗證，而區塊鏈則負責確保索引與存取紀錄的不可竄改性，兩者形成互補關係。進一步地，為因應隱私與法遵需求，部分研究開始將智能合約 (smart contracts) 納入鑑識流程中，作為敏感資料存取的自動化管控機制。透過智能合約，系統可將「誰在何時、基於何種法律依據」存取特定監控資料的行為，完整記錄於鏈上，並僅在符合預先定義之授權條件 (例如有效令狀或法官簽章)時，才允許解密或調閱相關內容 [18] [19]。此設計有助於將法律程序直接嵌入技術系統中，減少人工操作所帶來的灰色地帶。

然而，既有區塊鏈鑑識相關工作多半聚焦於影像完整性驗證或存取稽核本身，較少與大規模人臉檢索或向量化監控架構進行深度整合。特別是在向量資料庫主導的現代監控系統中，鑑識需求不僅限於單一影像的真偽驗證，更涉及跨攝影機軌跡關聯、相似性搜尋結果的可追溯性，以及嵌入與原始影像間的合法對應關係 [8] [10]。

參、方法

3.1 系統概述 (System Overview)

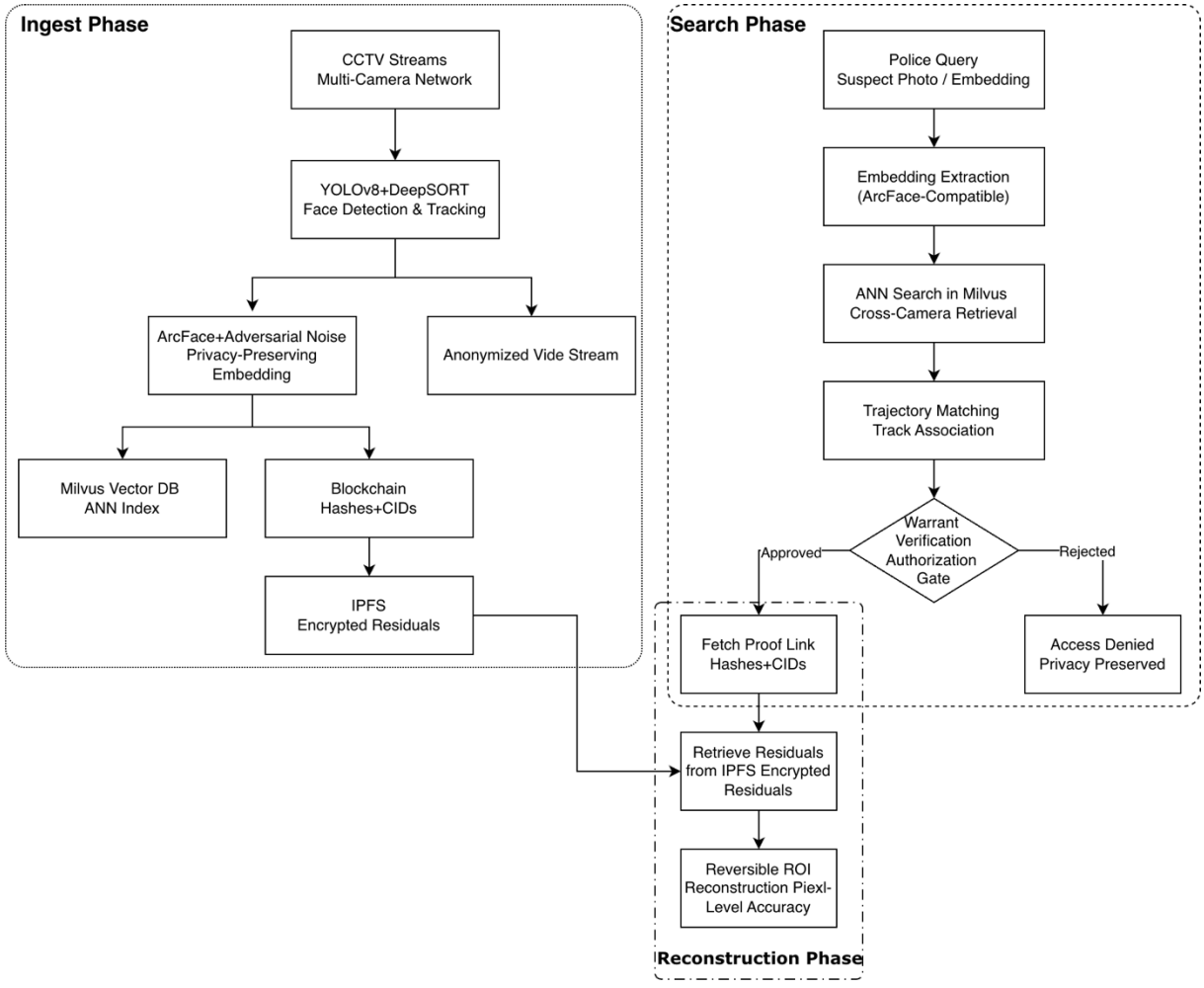
VectorChain 為一套具隱私保護特性之監控分析框架，旨在支援跨攝影機的人臉軌跡檢索，同時透過嚴格的令狀門控 (warrant-gated) 機制，實現可逆式且受授權控制的身分重建。相較於傳統以視覺呈現為核心的去識別化處理流程，該系統將「檢索能力」而非「影像可視性」視為主要的營運目標；因此，隱私保護策略主要施加於嵌入表徵層級，而可逆性則僅在經加密系統驗證之授權條件下重新引入。

如圖一所示，VectorChain 於邏輯上劃分為三個相互獨立且分工明確的運作階段：

1. **資料匯入階段 (Ingest Phase)**：多攝影機之閉路電視 (CCTV) 影像串流於邊緣端進行處理，以擷取人臉軌跡。對於每一條偵測到的人臉追蹤序列，系統會生成具隱私保護特性之嵌入向量，並將其索引至向量資料庫中，以支援大規模相似度搜

尋。

2. **檢索階段 (Search Phase)**：當提供一張嫌疑人影像時，執法人員可於嵌入空間中執行近似最近鄰 (Approximate Nearest Neighbor, ANN) 查詢，於次秒級時間內檢索出跨攝影機之候選人臉軌跡。
3. **重建階段 (Reconstruction Phase)**：僅在數位令狀經由鏈上驗證後，系統方允許啟動可逆式人臉區域重建，並利用鏈下儲存之身分殘差資料及與授權事件綁定之密碼學金鑰進行回復。



圖一：VectorChain 系統架構圖

此一分離式設計確保檢索功能在任何情境下皆可持續運作，而視覺層面的身分回復則於預設狀態下被條件性停用，僅在合法且必要時才得以啟用，從而符合隱私法規中關於比例原則 (proportionality principle) 之要求。

3.2 人臉軌跡擷取 (Face Trajectory Extraction)

人臉軌跡提取於攝影機端或邊緣節點即時執行，以確保隱私敏感資訊在離開影像擷取端前即完成必要的處理與去識別化。對於每一個時間戳 t的輸入影格 f_t，系統依序執行以下四個步驟，以建立跨影格一致的人臉軌跡表示。

(一) 人臉偵測 (Detection)

首先，系統採用 YOLOv8 進行即時人臉偵測 [12]，於影格 f_t中輸出一組人臉邊界框$\{b_1, b_2, \dots, b_n\}$，其中每一個 b_i定義一個候選人臉區域 (Region of Interest, ROI)。此步驟著重於在多目標與複雜場景下維持高召回率，以支援後續追蹤與特徵提取。

(二) 跨影格追蹤 (Tracking)

接著，系統透過 DeepSORT 對連續影格中的人臉進行資料關聯 [13]，為每一個被追蹤的人臉指派一個跨影格一致的軌跡識別碼 (track ID)。此機制可有效處理遮擋、短暫消失與視角變化等問題，從而將離散的偵測結果整合為具時間連續性的人臉軌跡。

(三) 嵌入特徵生成 (Embedding)

對於每一個已確認的 ROI，系統裁切對應的人臉區域並輸入至 ArcFace 模型，以生成一個 512 維的身份嵌入向量 $\phi_i(f_t) \in \mathbb{R}^{512}$。該嵌入向量具備高度判別性，適用於開放集合的人臉比對與跨攝影機檢索，同時其緊湊表示亦有助於降低儲存與搜尋成本。

(四) 殘差計算 (Residual Extraction)

為支援後續在合法授權條件下的人臉內容還原，系統在嵌入生成的同時，對原始 ROI 與其匿名化版本之間的差異進行殘差計算。系統於頻率域中計算 ROI 的離散餘弦轉換 (DCT)，並保留高頻係數作為殘差表示 $r_i(f_t)$。此殘差主要包含細節紋理與邊緣資訊，單獨存在時不具可視解讀性，僅能在結合對應的匿名化影像、邊界框對齊資訊與合法授權後，才能用於高保真度的人臉內容重建。

軌跡層級表示 (Trajectory Representation)

對於一條跨越多個影格 $\{t_1, t_2, \dots, t_k\}$的人臉軌跡 T_i，系統將其表示為一個有序序列如公式(1)：

$$\mathcal{T}_i = \{(\phi_i^1, r_i^1, \text{bbox}_i^1), (\phi_i^2, r_i^2, \text{bbox}_i^2), \dots, (\phi_i^k, r_i^k, \text{bbox}_i^k)\}, \quad (1)$$

其中：

- $\phi_i^j \in \mathbb{R}^{512}$為第 j個影格的人臉嵌入向量；
- r_i^j為對應影格的人臉高頻殘差資訊；
- $bbox_i^j$為人臉邊界框與空間對齊中繼資料。

在上述流程中**原始人臉影像從未被永久儲存**。系統僅保留經隱私強化的人臉嵌入與不可直接解釋的殘差資訊，而對外釋出的影片資料亦維持視覺去識別化狀態。因此，在未經授權的情況下，任何單一資料層(嵌入或殘差)皆不足以重建人臉外觀，確保人臉軌

跡提取同時滿足可檢索性、可追蹤性與隱私保護需求。

3.3 具隱私保護特性之嵌入生成 (Privacy-Preserving Embedding Generation)

在大規模監控與向量化檢索架構中，即使原始人臉影像未被儲存，深度人臉嵌入本身仍可能洩漏可重建的視覺身份資訊。因此，本研究將「嵌入層級的隱私保護」視為核心設計目標之一，並明確納入威脅模型與防禦機制加以建模。

威脅模型 (Threat Model)

本系統假設攻擊者具備以下能力：

1. 可存取向量資料庫中所儲存的人臉嵌入向量；
2. 可觀察或取得對外釋出的匿名化監控影像；
3. 可能利用既有或自行訓練的生成模型，嘗試從嵌入向量中反推出原始人臉外觀。

然而，攻擊者**不具備合法的令狀驗證結果與對應的解密金鑰**，亦無法存取經授權釋放的殘差資料。在此威脅模型下，系統必須確保：即便嵌入資料遭到外洩，亦無法有效重建具辨識度的人臉影像。

對抗性訓練防禦 (Adversarial Defense)

為抵禦近年提出的 GAN-based 嵌入反演攻擊，本研究於嵌入學習階段引入對抗性隱私約束，透過聯合最佳化方式同時考量**身份判別性**與**視覺不可逆性**。

(一) 身份判別損失：ArcFace

系統以 ArcFace 作為基礎人臉嵌入模型，其加性角度邊際損失函數定義如公式(2)：

$$\mathcal{L}_{\text{ArcFace}} = -\log \frac{e^{s(\cos\,\theta_y + m)}}{e^{s(\cos\,\theta_y + m)} + \sum_{j \neq y} e^{s\cos\,\theta_j}}, \tag{2}$$

其中 θ_y為樣本嵌入與其真實身份類別權重之間的夾角，m 為角度邊際，s 為特徵尺度參數。此損失確保嵌入在角度空間中具備高度類內緊密性與類間可分性，支援高準確率的身份比對與檢索。

(二) 嵌入反演損失 (Inversion Loss)

為模擬攻擊者行為，系統引入一個以 StyleGAN 為基礎的生成器 G，嘗試從嵌入向量 $\phi(x)$重建輸入人臉影像 x。對抗性反演損失定義為公式(3)：

$$\mathcal{L}_{\text{Invert}} = \mathbb{E}_{x\sim\text{Data}}[\| x - G(\phi(x)) \|_2^2 + \lambda_{\text{FID}} \cdot \text{FID}(G(\phi(x)),\text{Real})], \tag{3}$$

其中第一項衡量像素層級的重建誤差，第二項則以 Fréchet Inception Distance (FID) 量化生成影像與真實影像分佈之差異。透過最大化該損失，可有效破壞嵌入與可視人臉外觀之間的可學映射關係。

聯合最佳化目標 (Joint Optimization)

最終訓練目標為同時最小化身份辨識損失，並抑制嵌入反演能力，其聯合最佳化形式如公式 4：

$$\min_{\theta} \quad \mathcal{L}_{\text{ArcFace}}(\phi(x), y) + \lambda_{\text{adv}} \mathcal{L}_{\text{Invert}}(G(\phi(x))), \tag{4}$$

其中 θ表示嵌入模型參數，λ_{adv} 為隱私與辨識效能之間的權衡係數。本研究中設定 $\lambda_{\text{adv}} = 0.1$，以在不顯著犧牲檢索效能的前提下，提升對反演攻擊的防禦能力。

3.4 混合式儲存架構 (Hybrid Storage Architecture)

為同時滿足大規模人臉軌跡檢索效能、鑑識可追溯性與隱私風**險最小化**三項需求，VectorChain 採用一種三層式混合儲存架構 (Hybrid Storage Architecture)，將不同敏感度與功能目的之資料分離存放於異質系統中。此設計避免任何單一儲存子系統成為隱私洩漏的單點失效 (single point of failure)，並將法律授權與技術存取明確分開。

3.4.1 向量層：高維人臉軌跡索引 (Vector Layer: Milvus)

第一層為向量索引層，負責高效率的人臉軌跡相似度檢索。本系統使用 Milvus 向量資料庫，建立名為 face_trajectories 的集合，其資料綱要如圖二所示。

```
集合名稱: "face_trajectories"
欄位:
  - track_id (字串, 主鍵)
  - embedding (浮點向量, 維度=512)
  - camera_id (字串)
  - timestamp (64位元整數)
  - frame_range (字串) -> "1500:1510"
  - warrant_hash (字串) -> SHA256
  - ipfs_cid (字串) -> 殘差儲存指標
索引: HNSW (M=16, ef=200)
```

圖二：Milvus 集合綱要

每一筆資料對應一條人臉軌跡，包含以下欄位：

- track_id：軌跡識別碼，作為主鍵；
- embedding：512 維浮點向量，表示經隱私保護訓練後的人臉嵌入；
- camera_id 與 timestamp：記錄來源攝影機與時間資訊；
- frame_range：標示該嵌入對應之影格區間；
- warrant_hash：令狀雜湊值 (SHA-256)，用於後續授權驗證；

- ipfs_cid：指向鏈下殘差資料之內容識別碼 (CID)。

為支援大規模近似最近鄰 (Approximate Nearest Neighbor, ANN) 搜尋，系統採用 HNSW (Hierarchical Navigable Small World) 索引結構，並設定 $M = 16$、$ef = 200$，以在查詢延遲與召回率之間取得平衡。此層僅儲存嵌入向量與中繼指標，不包含任何可直接還原視覺人臉的資訊，因此即使資料庫遭未授權存取，亦無法進行人臉重建。

3.4.2 第 2 層：區塊鏈鑑識層 (Ethereum L2 / Polygon)

第二層為區塊鏈鑑識層，負責不可竄改的授權與存取紀錄管理。VectorChain 將關鏈鑑識中繼資料寫入部署於 Ethereum 相容 Layer-2 (如 Polygon) 上的智慧合約中，其結構如圖三所示。

```
struct TrajectoryRecord {
  bytes32 trackId;
  bytes32 embeddingHash;  // SHA256(embedding)
  string ipfsCID;         // 殘差位置
  uint256 timestamp;
  address officer;
  bytes32 warrantHash;    // 透過預言機驗證
}

mapping(bytes32 => TrajectoryRecord) public trajectories;

function authorizeReconstruction(bytes32 trackId, bytes memory warrant)
  public authorized(warrant)
{
  emit ReconstructionAuthorized(trackId, msg.sender, block.timestamp);
}
```

圖三：令狀智能合約範例 (Solidity)

每一筆 TrajectoryRecord 包含：

- trackId：對應向量索引層之軌跡識別碼；
- embeddingHash：嵌入向量之 SHA-256 雜湊，用於完整性驗證；
- ipfsCID：鏈下殘差資料之定位指標；
- timestamp：建立或授權時間；
- officer：提出重建請求之執法人員位址；
- warrantHash：經預言機 (oracle) 驗證之司法令狀雜湊。

智慧合約不儲存任何影像或殘差內容，而是作為法律與技術邊界的交會點。當執法人員提出重建請求時，必須呼叫 authorizeReconstruction 函式並通過令狀驗證，系統才會在鏈上觸發 ReconstructionAuthorized 事件。此設計確保所有重建行為皆具備不可否認性 (non-repudiation) 與可稽核性 (auditability)。

3.4.3 第 3 層：鏈下殘差層 (IPFS)

第三層為鏈下殘差儲存層，用以保存實現可逆人臉重建所需的視覺補償資訊。殘差資料透過 IPFS 進行內容定址式儲存，每一條軌跡對應一個獨立的殘差目錄，包含以下三類資料：

1. DCT 高頻係數殘差: 僅保留人臉 ROI 的高頻資訊，以影格級方式儲存。該資料在缺乏匿名化基底影像與空間對齊資訊時，無法獨立構成可視人臉。
2. 錯誤更正碼 (Error-Correcting Codes): 為抵抗實務監控影片常見的 H.264 壓縮失真，系統採用 Reed–Solomon 編碼 ($n = 255, k = 223$)，確保殘差在壓縮或傳輸噪聲下仍可正確解碼。
3. 元資料 (Metadata JSON): 包含邊界框歷史、姿態估計與對齊參數，用於重建階段的精確 ROI 還原。

值得注意的是，即便殘差資料位於公開可存取的 IPFS 網路中，若未同時具備：

- 區塊鏈層釋放之合法授權，
- 正確的內容識別碼，
- 以及對應的解密金鑰，

則該殘差資料在計算上仍是不可用的。

3.5 令狀門控之重建流程 (Warrant-Gated Reconstruction Pipeline)

為在隱私保護與司法鑑識需求之間建立可驗證且可追責的技術邊界，VectorChain 將人臉內容重建設計為一個**明確受令狀門控 (warrant-gated) 的例外流程**。在系統預設狀態下，所有監控影像僅以匿名化形式存在，任何像素層級的人臉還原皆必須經由司法授權、密鑰釋放與多層資料協同後方可執行。整體流程可分為四個階段：查詢、令狀驗證、重建與品質保證。

查詢階段 (Query Phase)

在查詢階段，執法人員上傳一張嫌疑人參考影像 x_{suspect}，系統即時計算其人臉嵌入 $\phi_{\text{suspect}} = \text{ArcFace}(x_{\text{suspect}})$. 隨後，系統於 Milvus 向量資料庫中執行近似最近鄰搜尋，以餘弦相似度作為匹配度量，檢索所有滿足門檻條件之人臉軌跡如公式(5)：

$$\text{topK} = \arg\max_{T_i} \cos(\phi_{\text{suspect}}, \phi_i^j) > 0.65. \tag{5}$$

此階段僅涉及嵌入層級的相似度比對，**不會觸及任何可逆或視覺資訊**，因此在無令狀的情況下仍可合法執行跨攝影機的軌跡搜尋。

令狀驗證階段 (Warrant Verification)

若查詢結果顯示有進一步鑑識需求，執法人員須提交經法官數位簽章之電子令狀。系統透過部署於區塊鏈上的智慧合約，使用對應的司法公鑰進行驗證如公式(6)：

$$\text{verify(warrant,judge\_pubkey)} =? \text{True.} \tag{6}$$

僅當驗證成功時，合約才會觸發授權事件，並允許釋放對應之解密金鑰 k_{decrypt}。所有驗證結果與授權行為皆被永久記錄於區塊鏈上，確保重建操作具備**不可否認性與事後稽核能力**。

重建階段 (Reconstruction)

在完成令狀驗證後，系統針對每一個匹配的影格 t執行人臉重建流程。具體步驟為：

1. **匿名化影格存取**：從 CCTV 儲存系統中讀取對應時間戳之匿名化影格。
2. **殘差取得**：透過區塊鏈所記錄之內容識別碼 (CID)，自 IPFS 取得對應的殘差資料：

$$r_i^t = \text{IPFS.get(ipfs\_cid)}. \tag{7}$$

3. **錯誤更正解碼**：對殘差進行 Reed–Solomon 解碼，以修復因 H.264 壓縮或傳輸噪聲所造成的資料損失：

$$\hat{r}_i^t = \text{ReedSolomon.decode}(r_i^t). \tag{8}$$

4. **ROI 還原**：

將解碼後的殘差加回匿名化人臉區域，完成像素層級的人臉重建：

$$\text{ROI}_{\text{recovered}} = \text{Anonymized\_ROI} + \hat{r}_i^t. \tag{9}$$

此加法式重建利用影片編碼中「預測結構保留、殘差可加」的特性，使系統能在不儲存原始影像的前提下，仍達到高保真度的人臉還原。

肆、實驗評估 (Experimental Evaluation)

透過標準監控資料集與多組基準方法，系統性評估 VectorChain 在跨攝影機人臉軌跡檢索能力、可逆重建品質以及隱私保護取捨三個面向的效能表現。

4.1 資料集 (Datasets)

實驗主要採用 ChokePoint 監控資料集作為評估基準 [11]。該資料集為人臉再識別 (Re-identification, Re-ID) 研究中常用之公開資料集，具備多攝影機與時間連續性等特性，適合用於模擬實際監控場域。ChokePoint 資料集具有以下特點：

- 由 25 部固定式攝影機所構成的多攝影機網路；
- 包含 48 位不同受試者；
- 總錄製時間約 25 小時影片；
- 於受控室內環境中拍攝，涵蓋顯著的人臉姿態變化、行走方向差異與短暫遮擋情境；
- 常被用作 多攝影機人臉再識別與軌跡關聯之標準基準。

該資料集提供穩定且可重現的實驗條件，使得系統在檢索效能與重建品質上的差異能被明確量化與比較。資料集官方來源為：http://arma.sourceforge.net/chokepoint/

4.2 基準方法 (Baselines)

為全面評估 VectorChain 的系統設計取捨，本研究選擇多種代表性基準方法進行比較，各基準方法分別對應不同的隱私、檢索與重建假設，用以界定系統效能的上下界。

(一) 原始儲存 (Raw Storage)

此基準直接儲存所有原始人臉影像，未進行任何去識別或隱私保護處理。該方法在重建品質上可視為理論上限 (upper bound)，但在實務上明顯違反隱私與資料保護原則，僅用於作為效能比較的參考。

(二) 僅向量搜尋 (Milvus-only)

此方法僅保留人臉嵌入向量並使用 Milvus 進行近似最近鄰搜尋，不儲存任何可逆殘差資訊。該設定可評估在完全不可重建的情況下，向量檢索本身的再識別效能，但無法支援任何像素層級的鑑識需求。

(三) UU-Net (逐影片可逆去識別)

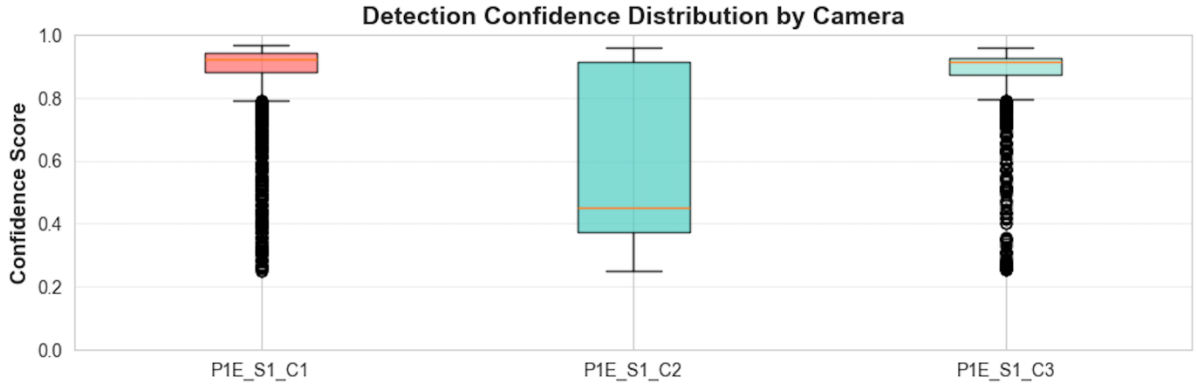
此基準代表既有可逆去識別方法的典型設計。UU-Net 將殘差資訊以隱寫方式嵌入於單一影片中，允許逐影片的重建。然而，由於其設計假設重建與搜尋皆發生於同一影片內，不支援跨攝影機的人臉檢索與軌跡關聯，因此無法直接應用於大規模多攝影機監控場景。

(四) Oracle (理想重建)

Oracle 基準假設系統可直接存取原始人臉影像，並以此作為重建結果。該設定不代表實際可部署系統，而是用於衡量在相同壓縮條件下，VectorChain 重建品質 (如 PSNR) 與「理想真值」之間的差距。

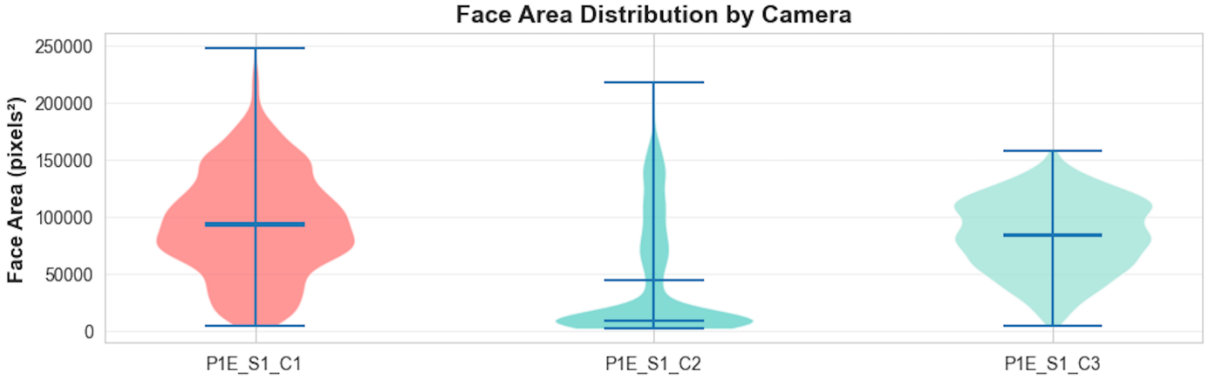
從圖四中看出 C1 (鏡頭 1) 與 C3(鏡頭 3) 的平均偵測信心值均高於 0.86，顯示其影像品質或拍攝距離較有利於模型判斷。相較之下，C2 的平均信心值僅約 0.60，且分佈範圍較廣，顯示人臉尺度變化大，或存在更多側臉、遮擋與快速移動情境。即便如此，

C2 仍產生最多偵測結果，突顯「高數量不等於高信心」的現象。



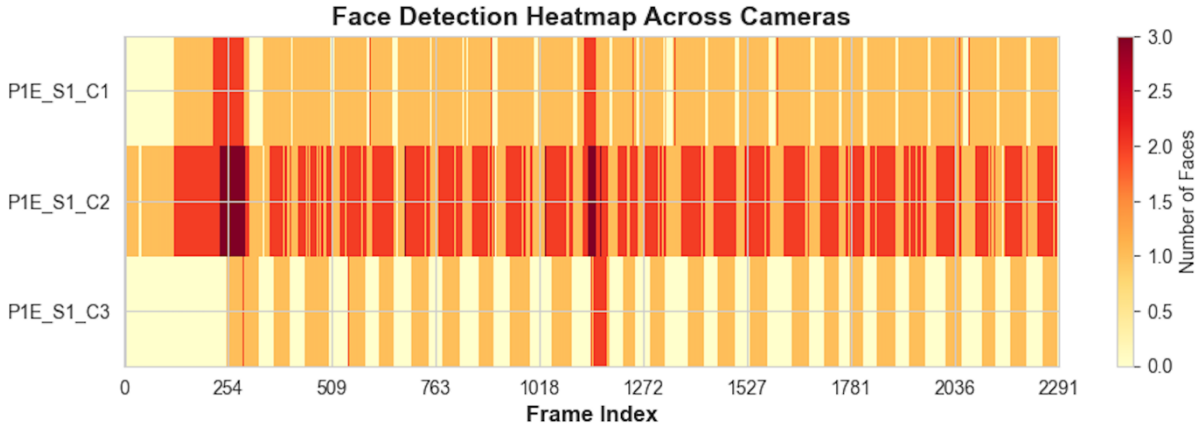
圖四：偵測信心值呈現攝影機依賴性 (Camera-dependent Confidence)

圖五顯示三部攝影機在人臉面積分佈上存在顯著差異，C1、C3 的平均人臉面積較大，推測攝影機距離較近或安裝高度較低；C2 則呈現「大量小尺寸人臉 + 少數大尺寸人臉」的雙峰趨勢。人臉尺度的差異將直接影響偵測信心值，嵌入品質，以及後續殘差重建的 PSNR 表現。在可逆重建與品質評估時，需將人臉尺度納入誤差分析模型，而非僅以壓縮參數 (CRF) 作為唯一變數。



圖五：人臉尺度 (Face Area) 分佈顯示明顯視角差異

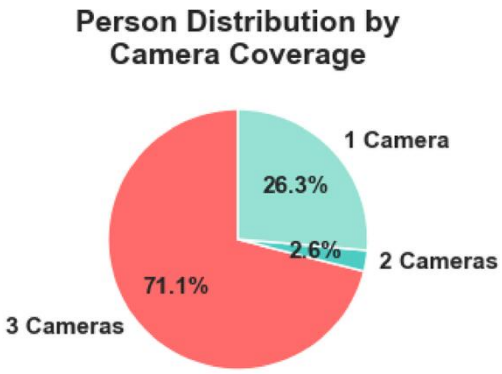
圖六為人臉偵測熱圖，顯示特定時間區段出現密集人臉活動及不同攝影機在時間軸上的活躍區段高度不一致。該現象說明單純以「單影格」或「單攝影機」進行分析，將無法完整捕捉人臉行為模式。此結果進一步說明 VectorChain 採用「人臉軌跡 (trajectory) 」作為基本檢索與儲存單位，而非孤立影格。



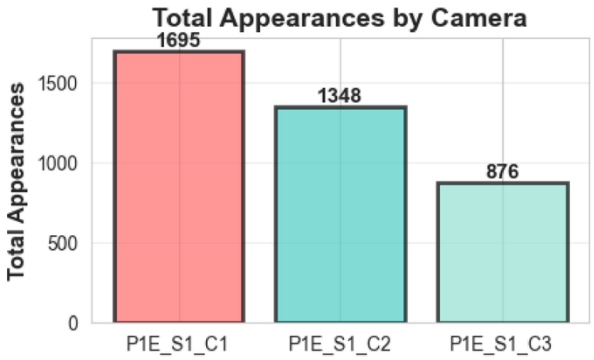
圖六：時間熱圖顯示人臉活動具高度時間結構性

在跨攝影機的人臉偵測實驗中，本次跨鏡追蹤彙整後資料為 93 筆 person-camera 記錄(每筆代表「某人於某攝影機的出現區段/統計」)，共追蹤到 38 位唯一個體，跨 3 部攝影機，總出現次數 3919。同時辨識細節結果 3995 rows，顯示 ArcFace embedding 比對在此段落具有足夠樣本量可評估跨鏡一致性與轉移行為。多數人確實在多攝影機中被一致識別根據圖七 (a) 圓餅圖與統計輸出 71.1% (27/38) 的人出現在 3 台攝影機，2.6% (1/38) 的人出現在 2 台攝影機，26.3% (10/38) 的人只出現在 1 台攝影機
這結果代表 ArcFace embedding 在此段場景中呈現高度「跨鏡可連結性」，也意味著場域動線或攝影機布局使得多數人會穿越多個視角。換句話說，跨攝影機檢索在這裡不是「可有可無」，而是必要功能；只做單鏡檢索會直接漏掉多數人的完整軌跡。

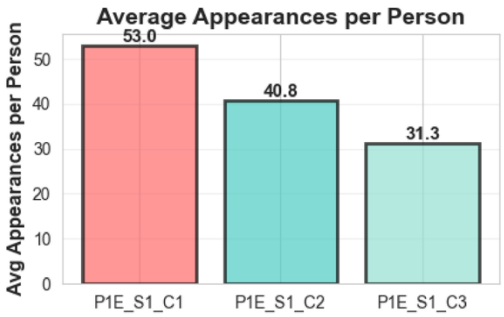
從圖七 (b) (c) (d) 三個 bar chart 可知道總出現次數 (Total Appearances) C1 = **1695** (最高)、C2 = **1348** 及 C3 = **876**(最低)，在唯一個體數 (Unique Persons Detected) 分析 C2 = **33** (最高)、C1 = **32** 及 C3 = **28**，另外在每人平均出現次數 (Average Appearances per Person) 分析 C1 = **53.0**(最高)、C2 = **40.8** 及 C3 = **31.3**。可知 C1「出現總量」與「每人出現次數」較高，推測是停留時間較長或視角較穩定(同一人被反覆觀測到)。C2「獨立個體數」最高，但平均出現較低，較像是人流分散、通過較快或尺度變化較大的視角。C3 兩者偏低，可能屬於覆蓋較窄或可見性不佳的攝影機。跨鏡系統若要公平評估，必須同時考慮「人流密度」與「停留/可視時間」，否則會誤把某一視角當作“最好”而其實只是“看得久”。



(a) 人員出現在不同鏡頭下的狀況



(b) 不同鏡頭下出現人員的次數

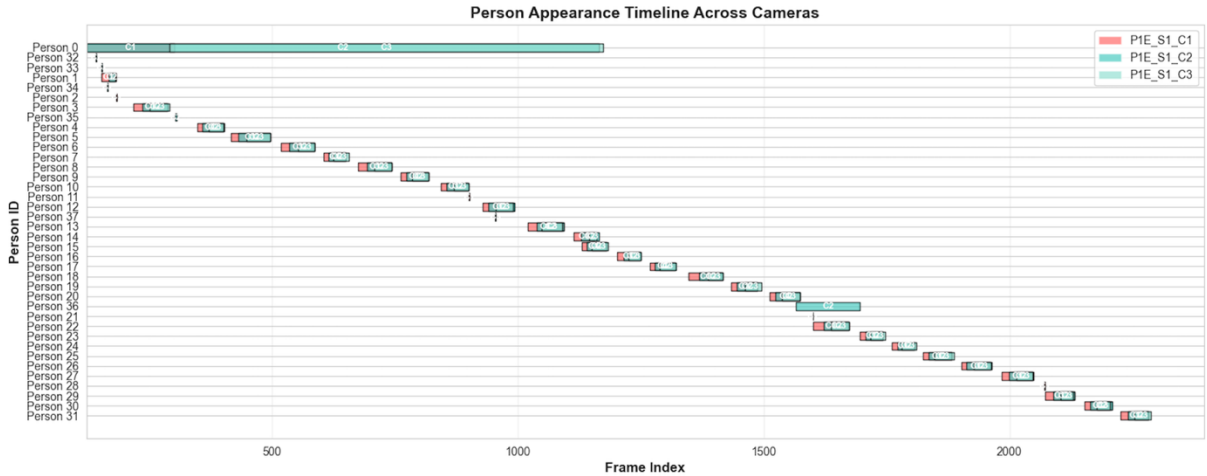


(c) 同一人員在各鏡頭平均出現次數

(d) 單獨出現在單一鏡頭下的人員數

圖七：跨攝影機人員出現 (ArcFace) 模擬

圖八時間軸 (Gantt) 顯示跨鏡軌跡具有序列性，適合做「轉移建模」，圖中「Person Appearance Timeline Across Cameras」呈現每位 Person 在不同 Camera 的 first/last frame 區段。可觀察到多數個體在不同攝影機之間呈現有序分段，而非完全重疊。這表示將人員行為建模為「跨鏡狀態轉移」而不是獨立事件集合。對 VectorChain 而言，檢索結果應以「trajectory / segment chain」呈現，而非單張影格命中；後續可引入時間一致性約束 (例如：候選匹配必須符合合理的跨鏡時間窗口)。



圖八：ArcFace 分析不同人員出現在不同攝影機之間的時間序

伍、結論

本文提出 VectorChain，一套具備授權閘控可逆重建機制的隱私保護人臉軌跡檢索架構，旨在回應現代大規模監控系統於「隱私保護、可搜尋性與可回復性」三者間長期存在的結構性衝突。相較於既有僅著重視覺匿名化或單鏡可逆重建的方法，本研究以「軌跡檢索優先、身分回復例外化」為核心設計原則，重新界定監控系統中資料儲存與存取的安全邊界。在系統設計上，VectorChain 將隱私風險明確分離至不同層級：以經對抗式訓練強化之 ArcFace 嵌入支援跨攝影機 ANN 搜尋；以 Milvus 向量資料庫實現次秒級檢索效能；以區塊鏈確保授權與鑑識事件的不可否認性；並透過 IPFS 儲存高頻殘差以支援像素級可逆重建。此三層混合式架構確保任一單獨元件均不足以完成身分還原，從系統層面降低隱私外洩風險。在隱私防護方面，本文明確建模嵌入反演攻擊威脅，並透過聯合最佳化策略。總結而言，VectorChain 提供了一種在技術與法律層面皆具可驗證性的監控系統設計範式，使隱私保護成為預設狀態，而身分揭露則成為受監管、可稽核的例外行為，為未來合規導向的智慧監控與數位鑑識系統奠定可行基礎。

誌謝

感謝 ChokePoint 資料集提供者以及所有參與系統測試的研究人員。

參考文獻

[1] H. Proença, “The UU-Net: Reversible Face De-Identification for Visual Surveillance Video Footage,” arXiv preprint arXiv:2007.04316, 2020

[2] L. Yuan et al., “Invertible Image Obfuscation for Facial Privacy Protection via Secure Flow,” in *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 34, No. 7, pp. 6077-6091, July 2024, doi: 10.1109/TCSVT.2023.3344809.

[3] H. Kim, S. Park and D. Choi, “Secure and Reversible Face De-Identification With Format-Preserving Encryption,” in *IEEE Access*, Vol. 13, pp. 116130-116142, 2025, doi: 10.1109/ACCESS.2025.3583388.

[4] J. Cao, B. Liu, Y. Wen, R. Xie, and L. Song, “Personalized and Invertible Face De-identification by Disentangled Identity Information Manipulation,” *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, Montreal, QC, Canada, 2021, pp. 3314-3322, doi: 10.1109/ICCV48922.2021.00332.

[5] Z. Wang et al., “Privacy-preserving Adversarial Facial Features,” *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Vancouver, Canada, 2023, pp. 8212-8221, doi: 10.1109/CVPR52729.2023.00794

[6] H. O. Shahreza, V. K. Hahn and S. Marcel, "Face Reconstruction from Deep Facial Embeddings using a Convolutional Neural Network," *2022 IEEE International Conference on Image Processing (ICIP)*, Bordeaux, France, 2022, pp. 1211-1215, doi: 10.1109/ICIP46576.2022.9897535.

[7] C. H., Cho, H. M. Song, and T. Y. Youn, "Practical Privacy-Preserving ROI Encryption System for Surveillance Videos Supporting Selective Decryption," *Computer Modeling in Engineering & Sciences*, Oct. 2024, Vol. 141, No. 3, pp. 1911-1931, doi: 10.32604/cmes.2024.053430

[8] Milvus Vector Database, "How Does Face Recognition Contribute to Video Search?" https://milvus.io/blog/face-recognition-video-search.md, 2025.

[9] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 770-778, doi: 10.1109/CVPR.2016.90.

[10] J. Deng, J. Guo, N. Xue and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Long Beach, CA, USA, 2019, pp. 4685-4694, doi: 10.1109/CVPR.2019.00482.

[11] Y. Wong, S. Chen, S. Mau, C. Sanderson and B. C. Lovell, "Patch-based Probabilistic Image Quality Assessment for Face Selection and Improved Video-based Face Recognition," *CVPR 2011 WORKSHOPS*, Colorado Springs, CO, USA, 2011, pp. 74-81, doi: 10.1109/CVPRW.2011.5981881.

[12] Z. Huang, L. Li, G. C. Krizek, L. Sun, "Research on Traffic Sign Detection based on Improved YOLOv8," *Journal of Computer and Communications*, Vol. 11, No. 7, pp. 226–232, 2023.

[13] N. Wojke, A. Bewley, and D. Paulus, "Simple Online and Realtime Tracking with A Deep Association Metric," *2017 IEEE International Conference on Image Processing (ICIP)*, Beijing, China, 2017, pp. 3645-3649, doi: 10.1109/ICIP.2017.8296962.

[14] T. Karras, S. Laine, and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 43, No. 12, pp. 4217-4228, 1 Dec. 2021, doi: 10.1109/TPAMI.2020.2970919.

[15] C. Dwork, "Differential Privacy," *International Colloquium on Automata, Languages, and Programming*. ICALP, 2006. https://link.springer.com/chapter/10.1007/11787006_1.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Cryptography Mailing* list at https://metzdowd.com.

[17] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint

arXiv:1407.3561, 2014.

[18] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Project Yellow Paper, Vol. 151, pp. 1–32, 2014.

[19] European Parliament and Council, “Regulation (EU) 2016/679 (General Data Protection Regulation),” Official Journal of the European Union, L 119, pp. 1–88, 2016.