Domain Adaptation based Data Mining for Robust Cross-Domain Surveillance Analytics: A Review and Conceptual Framework

Dr. Sivalingan H
Head and Assistant Professor, Department of Data Science
Providence College (Autonomous), Coonoor, Tamil Nadu, India
***DOI**: doi.org/10.34293/iejcsa.v4i1.64*

Abstract - *Cross-domain variability remains a critical challenge in surveillance analytics, where models trained in one environment often fail to generalize effectively to new deployment settings due to domain shift caused by variations in lighting, camera viewpoints, crowd density, and scene dynamics. Traditional surveillance data mining approaches assume identical data distributions between training and testing environments, which is unrealistic in large-scale real-world systems.*

This paper presents a comprehensive systematic review and unified conceptual framework for domain adaptation–based surveillance data mining. The study categorizes existing domain adaptation techniques into feature distribution alignment, adversarial learning, self-supervised adaptation, and multi-scene transfer mechanisms. A formal problem formulation is introduced to define source–target distribution mismatch and its impact on surveillance tasks such as anomaly detection and activity recognition.

Furthermore, we propose an integrated domain adaptation framework incorporating domain invariant feature learning and distribution alignment strategies to improve cross-domain robustness while minimizing target-domain annotation requirements. Comparative analysis reveals consistent performance improvements when adaptation mechanisms are employed. The paper also identifies key research challenges including label scarcity, real-time adaptation, scalability, interpretability, and privacy-preserving learning.

This work provides a structured research roadmap toward scalable, annotation-efficient, and generalizable surveillance analytics systems.

***Keywords:** Domain Adaptation, Surveillance Analytics, Cross-Domain Learning, Video Anomaly Detection, Domain-Invariant Representation, Feature Distribution Alignment.*

INTRODUCTION

Surveillance systems are widely implemented in cities, transportation, and public networks which produce a constant cascade in multiple visual and sensory features. The challenges like changes in lighting, viewpoints, density of crowd and environmental conditions significantly impacts the effective data mining and authenticity in surveillance data interpretation. The standard method assumes that the training data and the implementation data has a similar distribution but it is not held up in the real world framework. The model which is trained in one environment frequently breaks down the performance when it is applied in a different environment, an issue which is confessed as domain shift.

Surveillance tasks have attained an enhancement in activity recognition, object tracking, and anomaly detection, using deep learning methods, but these methods remain processing large volumes of data and dependent on environment determined explanation.

In a large-scale surveillance framework, obtaining the required annotation is often costly and impractical. So, domain adaptation has come up with a highly optimistic method to overcome these challenges which transfers the data from source domain (labeled) to target domain (unlabeled). Such methods promote a strong cross-domain generalization which is acquired through domain-invariant representation and feature distribution.

Even though the domain adaptation for surveillance tasks has enhancement, yet it is separated, which is out of the way targeting single tasks and adaptation approaches. In recent studies, there is an absence of an integrated framework that shows how domain adaptation is incorporated with surveillance pipelines, and how strengths, weaknesses, and deployment problems are evaluated. To fill this gap, this paper shows the complete survey and conceptual framework for domain adaptation data mining in surveillance administration. The study provides advancements in feature representation and distribution alignment methods, shows the perception towards the evolution of scalable, generalizable surveillance systems, and identifies key cross-domain performance characteristics.

Novelty and Contribution

The paper focuses on a complete review and conceptual framework that incorporated the domain adaptation data mining with the surveillance data interpretation, which traverses the traditional separated research areas. Existing surveys isolate the surveillance and domain adaptation, but this work integrates recent work using a surveillance lens and comes up with a high-level cross-domain learning structure. Furthermore, the study also brings integrated presentation in performance trends, real-world issues, unresolved disadvantages, creating an extensive reference and research roadmap for cross-domain surveillance methods.

RELATED WORK

Surveillance analytics has evolved as a significantly active and important research area due to wide implementation of camera networks in smart cities, transportation hubs and public areas [1,2]. This section assesses three related areas such as surveillance data mining, video anomaly detection, and domain adaptation techniques which are applied in surveillance methods and highlights the constant challenges by domain shift and acquisition of integrated cross-domain frameworks.

A. Surveillance Data Mining

Early data mining in surveillance significantly depends on handcrafted features which are integrated with the standard machine learning methods to review the behavior of human and environmental activities [3,4]. To detect the unusual activities and crowd behavior, some methods are used which are based on clustering, combination mining rule, trajectory analysis, and statistical modeling. However, these methods had effective performance of environmental constraints, but they were easily affected by the changes in camera viewpoints, light, conditions, and location configuration [5]. The usage of handcrafted features further restricted the scalability and adaptability in multiple surveillance backgrounds.

By the progress of deep learning, data centric methods have become significant in the surveillance data interpretation. To learn spatiotemporal attributes from raw surveillance video, Convolutional neural networks (CNN) and recurrent planning have been used [6,7]. These models have enhanced the feature magnificence and the dependencies on domain-specific engineering have been reduced. But most of the deep learning surveillance data mining approaches take as read that both the training and testing data emerge from the same distribution [8]. Hence, when there is a transmission of the camera network from one environment to another environment, there is a degradation in performance limiting its robustness [9].

B. Video Anomaly Detection

To identify any suspicious activities that divert the system from the trained pattern of normal behavior in the surveillance systems, the video anomaly detection is used as a central task [10].

The standard anomaly framework detection is modeled using reconstruction-based or prediction-based techniques, recognizing the anomalies as irregularity from learned patterns. To capture complex patterns and dynamicity in appearance from surveillance data, the deep autoencoders, GANs, and temporal prediction models are used [11–13].

In spite of enhancement, most of the anomaly detection systems are reviewed in single domain inference [14]. Anomalies in surveillance conditions, dependencies in context, differences in location structure, crowd density, and lighting results in significant domain mismatch. Overall, the result depends on how the models trained on one dataset provide high false-positive rates when the model is applied to unknown surveillance environments [15,16]. These challenges are addressed in recent works and highlights the importance of generalizing across domain methods without annotation [17].

C. Domain Adaptation in Surveillance Analytics

The distribution mismatch between the source domain and target domain results in performance degradation, to reduce this the domain adaptation techniques are used. In comprehensive machine learning, feature distribution, adversarial learning, and self-supervised learning methods have been traversed [18,19]. Feature distribution method includes Maximum Mean Discrepancy (MMD), an attempt to reduce the statistical variation between the source and target feature distribution [20]. Adversarial domain learning method implements discriminators in domain to improve domain-invariance [21,22].

In surveillance analytics, the domain adaptation has been significantly maximized to provide cross location recognition and detection of anomalies [23]. There are several studies to improve the generalization techniques that reveal the integrated feature distributions among varied camera network views, but the existing system focuses on a single task which is fragmented [24]. The analysis of how the domain adaptation is incorporated with surveillance data mining pipeline is lacking. Furthermore, the real-time implementation restrictions, cost of annotation, and explainability are often underrepresented in current work [26].

Summary of Limitations in Existing Work

In the existing system of surveillance applications, there are three key challenges: First, Both the standard and the deep learning methods on data mining have only finite durability when the method is applied across different environmental conditions [9,5]. Second, there is a lack of integrated review and conceptual framework and are isolated to surveillance analytics [18,23]. Third, scalability, generalization and interpretability are the challenges in implementation [26]. These challenges stimulate the requirement which should have a complete review and conceptual framework that merge domain adaptation data mining methods as presented in the paper.

CONCEPTUAL DOMAIN ADAPTATION FRAMEWORK

This section provides a conceptual framework for integration of domain adaptation and surveillance data mining applications. The framework shows how the adaptation system reduces the performance degradation in domain shifts which is in surveillance environments and increases robustness in cross domain.

A. Domain Definition

In machine learning, a domain is formally defined as a pair:

$$D = (X, P(X))$$

where

- X denotes the input feature space (e.g., spatio-temporal video representations)
- P(X) denotes the marginal probability distribution over the feature space.

A learning task within a domain is defined as:

$$T = (Y, f(.))$$

where

- Y is the label space (e.g., anomaly/normal or activity categories),
- $f: X \rightarrow Y$ is the predictive function.

In cross-domain surveillance analytics, two domains are considered:

Source Domain $Ds = (Xs, Ps(X))$

Target Domain $Dt = (Xt, Pt(X))$

Even if the feature space and task are identical:

$$Xs = Xt, Ys = Yt$$

the underlying distributions may differ:

$$Ps(X) \neq Pt(X)$$

This distribution mismatch arises from environmental variations such as lighting changes, camera angle differences, background structure, and crowd behavior patterns in surveillance systems.

The objective of domain adaptation is therefore not to redesign the task, but to learn a representation $F\theta(X)$ such that:

$$Ps(F\theta(X)) \approx Pt(F\theta(X))$$

while preserving task discriminability. By aligning feature distributions across domains, the model achieves improved generalization in previously unseen surveillance environments.

A. Problem Formulation

Surveillance in the real-world gathers the data from different environments showing variations in location layout, camera settings, lighting, and crowd behavior. These variations often result in inconsistent distribution which is known as domain shift, whereas it degrades the traditional data mining models performance across different environments.

Theoretically, the surveillance data is divided into two main domains such as Source Domain and Target Domain. The source domain is labeled data which is available for supervised learning and the target domain constitute any new or unseen environment without labeled data. Though, the activity recognition or anomaly detection are shared equally by both the domains but the data distribution differs because of environmental factors. The main aim of domain adaptation is to share the learned knowledge data from the source domain to enhance the generalization of the model to the target domain without a need of large scale annotation.

B. Domain-Invariant Feature Learning

The major role of domain adaptation in surveillance application is to study the representations of the features that are robust to domain shifts. Domain-invariant feature learning is to extract the distinguished presentation from surveillance which is raw data reducing the challenges which occur during changes in lighting, viewpoint, background, and location movements.

At a high level, both source and target inputs are encoded by a shared feature extractor into a common feature space that provides the task which is related to the semantic information, which includes motion and behavior patterns. The properties are shared across domains, which is captured by domain-invariant features, enhancing the surveillance analytics performance across different environments.

C. Feature Distribution Alignment

Even with shared representations knowledge, inconsistencies still occur within source and target feature distribution. By organizing the feature distributions, it tackles the challenges by reducing the distributional gap between feature representations across different domains. The distance between source and target feature distributions is calculated and minimized by using Maximum Mean Discrepancy (MMD) in a high dimensional area, an approach which is discussed in related work.

In surveillance analytics, the alignment allows the model to be trained on; labeled source data to generalize more capability to unlabeled target domain environments. In real-world conditions where environmental changes are high and costly annotation of new surveillance data is impractical, the conceptual alignment is significant.

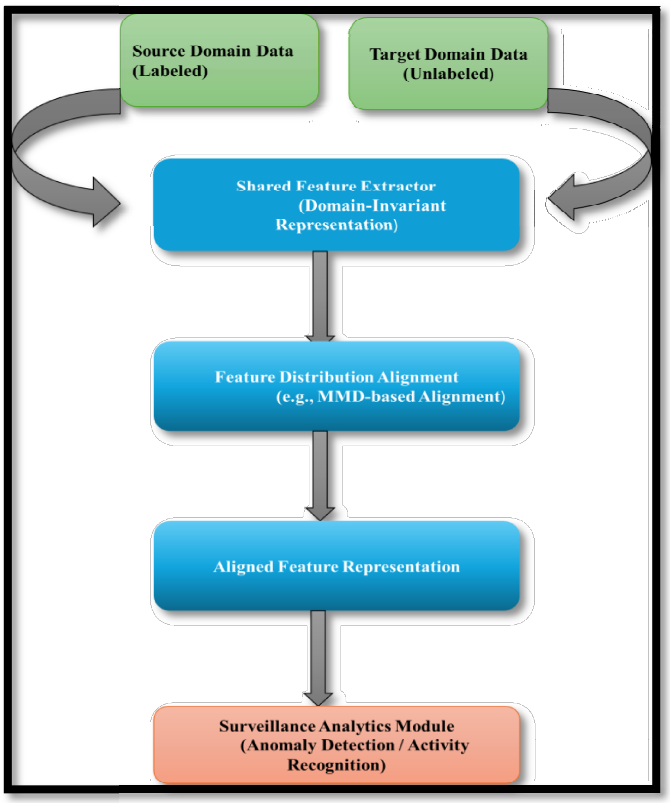

Figure 1: **Conceptual Architecture of a Domain Adaptation Data Mining Surveillance Framework**

There is source-domain data which is labeled and target-domain data which is unlabeled. They are executed between the shared feature extractor to attain domain invariant representations. A feature distribution alignment level theoretically reduces inconsistency between source and target feature distributions, which enables robust cross-domain surveillance analytics such as anomaly detection and activity recognition without requiring labeled target domain data.

The combination of representation learning and domain adaptation are incorporated into a unified processing pipeline as it is summarized in the conceptual flow of the proposed framework in figure 1. Using a common feature extraction method both the labeled and unlabeled environments are initially shown into a shared latent space which protects the task-relevant explanations while reducing the variations in the environment. The second step of an explicit alignment then processes the learned representations which significantly reduces the unused variations in the source and target domains consistently among feature distributions. This adaptation method supports effective knowledge which is transferred from annotated source domains to perform effectively in new or changing surveillance settings, parallely supporting activity recognition and anomaly detection without additional manual labeling.

D. Domain Shift in Surveillance Environments

Some of the domain shifts in surveillance analytics are created from multiple variations such as camera viewpoints, light conditions, scene configuration, crowd solidity,

sensor configurations, and environmental interactions. These are the elements that causes inconsistency between training and deployment condition, which leads to the degradation of performance of the model when adaptation mechanisms is without the conventional learning approaches.

COMPARATIVE ANALYSIS AND DISCUSSION

A. Evaluation Metrics

The recent works in surveillance analytics and domain adaptation significantly engages to calculate the models performance between standard classification and detection metrics. Accuracy is reported constantly but this alone is not sufficient for surveillance systems, which are operating under class imbalance conditions mainly in anomaly detection. Moreover, along with accuracy, Precision, Recall, and F1-score are often used to evaluate a balanced assessment in the quality of detection. And also the area under the ROC Curve (AUC) is frequently used to evaluate imbalance conditions across different decision frameworks. By constantly using these metrics, it provides comparability between cross-domain generalization and robustness.

Table 1 Comparison of Domain Adaptation Techniques in Surveillance Analytics

Approach	Alignment Strategy	Typical Task	Key Insight
MMD-based Adaptation	Feature distribution alignment	Anomaly detection	Aligns domains without target labels
Adversarial Adaptation	Domain discriminator learning	Activity recognition	Encourages invariant features
Self-Supervised Adaptation	Pseudo-labeling / contrastive learning	Anomaly detection	Reduces annotation reliance
Multi-Scene Adaptation	Scene-invariant mapping	Crowd analysis	Handles viewpoint variability
Weakly Supervised Adaptation	Limited target labels	Video anomaly detection	Balances cost and robustness

Table 1 shows the summary of key domain adaptation in surveillance analytics, demonstrating how domain shifts vary from different alignment. Distribution and adversarial methods are focusing on the learning domain-invariant representations which are without the target labels, whereas self-supervised approaches additionally reduce the annotation vulnerabilities. s Viewpoint variability is operated specifically by multi-scene adaptation, and the methods robustness and cost, are handled by weakly supervised which reflects the practical deployment is exchanged in the real-world surveillance systems.

B. Cross-Domain Performance Trends

The analysis of related works provides the consistent pattern in cross domain surveillance analytics. The models are trained only on source domain data which commonly endure significant degradation when the same trained data is applied to new unseen target domains because of domain shifts. This effect is severe in complex surveillance conditions which includes different lighting, camera settings, and crowd dynamics. Conversely, this

study incorporates domain adaptation techniques which improved balance and robustness across domains. The performance gap between source data and target data is reduced by using feature distribution alignment and domain-invariant presentation learning methods, highlighting the benefit of adaptation techniques that diminishes the environmental variations.

C. Practical Implications

From the context, domain adaptation surveillance analytics convey the key challenges which are related to scalability and annotation cost. Real world data in surveillance requests robustness to constant changes in the environment as it evolves over time. Reducing the dependencies on labeled target-domain data while decreasing the manual annotation effort and related costs. These dominance highlights the significance of domain adaptation as a critical factor in attaining scalability and cost-efficient analytics.

CHALLENGES AND RESEARCH DIRECTIONS

Table 2 Disadvantages in Cross-Domain Surveillance and Proportional Domain Adaptation Solutions

Challenges	Description	Domain Adaptation Solution
Domain Shift Across Environments	Variations in viewpoint, lighting, scene layout, and crowd behavior cause distribution mismatch	Domain-invariant feature learning to reduce sensitivity to environment-specific factors
Scarcity of Labeled Target Data	Manual annotation in new surveillance environments is costly and impractical	Unsupervised and weakly supervised domain adaptation techniques
Performance Degradation in New Domains	Models trained on source data fail to generalize to unseen target environments	Feature distribution alignment methods (e.g., MMD-based alignment)
Dynamic and Evolving Scenes	Surveillance environments change over time due to lighting, weather, or scene evolution	Incremental and continuous domain adaptation strategies
Privacy and Ethical Concerns	Cross-domain data sharing raises privacy and compliance issues	Privacy-preserving adaptation (e.g., federated learning, secure feature learning)
Scalability Constraints	Large-scale systems must handle multiple heterogeneous domains efficiently	Lightweight and transferable adaptation mechanisms
Lack of Model Interpretability	Adapted models often behave as black boxes	Explainable domain adaptation and interpretable feature analysis

Although domain adaptation surveillance analytics have attained significant attention, still it lacks several limitations in real-world applicability. Table 2 is to compare the indicative domain adaptation technique and its standard applications in surveillance analytics.

Label Scarcity: The labeled data which is in the target domain environment are costly, sparse to acquire. Still multiple methods have half target labels even domain

adaptation reduces the dependencies on annotation. Hence the future work should point out the self-supervised and weakly supervised adaptation techniques that effectively process the utmost label scarcity and enable the scalable surveillance methods.

Real-Time and Continuous Adaptation: Most of the current methods undertake the batch processing, which limits the relevance in dynamic, real world environments. Hence lightweight adaptation methods are needed to control the restrained changes in the environment while maintaining the computational efficiency and stability.

Privacy, Ethics, and Explainability: There are authenticity risks and ethical concerns in multi- domain. So by combining the federated learning with explainable adaptation frameworks which are privacy-preserving techniques is critical to ensure transparency, accountability, and trustworthiness in surveillance analytics. Explainability improves the interpretability and authenticity in decision making.

Collectively, these challenges are highlighting the path for future research in reducing annotation cost, real-time, authentic, and explainable domain adaptation methods that can be robust, ethical, and scalable surveillance analytics across multiple different environments.

CONCLUSION AND FUTURE WORK

By integrating the advancements in surveillance data mining, video anomaly detection, and domain adaptation, this paper analysis provides a conceptual framework for domain adaptation data mining in surveillance analytics. To diminish the domain shift the paper highlights how domain-invariant feature learning and feature distribution alignment are used and enhances the cross-domain robustness without large-scale target-domain annotations. Comparing the related existing works shows how the method consistently shows that the domain adaptation methods improves generalization across multiple different surveillance scenarios.

In spite of these advantages, the key challenges remain, including label scarcity, real time and continuous adaptation, privacy, ethics, and explainability. The Future work should aim on annotation-efficient, lightweight mechanisms, self-supervised adaptation methods, explainable models, and integration of privacy-preserving. Overcoming these challenges allows domain adaptation surveillance analytics to support scalable and trustworthy performance in different real world environments.

REFERENCES

1. Duong, H. T *et al.* 2023. ‘Deep learning-based anomaly detection in video surveillance: A survey’, *Sensors,* vol. 23*,* no. 11, P. 5024.
2. Sultani, W. *et al.* 2018. ‘Real-world anomaly detection in surveillance videos’, in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 6479–6488.
3. Zhou, X. *et al.* 2023. ‘Generative adversarial learning for weakly supervised anomaly detection in surveillance videos’, *Pattern Recognition*, 134, 109043.
4. Zheng, Y. *et al.* 2025. ‘Domain adaptation for video anomaly detection: A systematic review’, *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

5. Grigorescu, S. *et al.* 2020. 'A survey of deep learning techniques for autonomous driving', *Sensors,* vol. 20, no. 21, P. 5916.
6. Sun, C. *et al.* 2022. 'Self-supervised representation learning for video anomaly detection'. *IEEE Transactions on Neural Networks and Learning Systems,* vol. 33, no. 12, pp. 7486-7499.
7. Zhao, H. *et al.* 2023. 'Transformers in anomaly detection: A comprehensive review', *ACM Transactions on Intelligent Systems and Technology,* vol. 14, no. 3, Article 44.
8. Szymanowicz, S et al. 2024. 'Benchmarking cross-domain robustness in surveillance video analytics', *Neurocomputing*, 569, 127056.
9. Aich, A. *et al.* 2023. 'Cross-domain video anomaly detection without target domain adaptation'. in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, pp. 5537-5546.
10. Gupta, R. *et al.* 2025. 'Lightweight CNN–MIL models for cross-domain video anomaly detection: A reproducible evaluation framework', *Informatica*, vol. 49, no. 3, pp. 365-379.
11. Verma, U. *et al.* 2025. 'Contextual information-based anomaly detection for multi-scene aerial videos', *Scientific Reports*, 15, 25805.
12. Dilek, E. 2025. 'An overview of transformers for video anomaly detection', *Soft Computing*.
13. Jiao, L. *et al.* 2025. 'Adaptive industrial video anomaly detection empowered with domain adaptation', *Mathematics*, vol. 13, no. 17, P. 2711.
14. Tank, D. R *et al.* 2025. 'Enhancing anomaly detection in video frames using deep learning', *Journal of Information Systems Engineering and Management,* vol. 10, no. 2S, 26s.
15. Li, M. *et al.* 2024. 'Target tracking using video surveillance for edge machine vision', *Journal of Cloud Computing*, 13, 47.
16. Xu, Y. *et al.* 2022. 'Video unsupervised domain adaptation with deep learning: A comprehensive survey'. *arXiv*.
17. Zeng, X. *et al.* 2024. 'Video anomaly detection using hybrid transformer and memory networks', *Pattern Recognition Letters,* 185, pp. 44-51.
18. Raffay, Y. *et al.* 2024. 'Anomaly detection based on cascaded Swin Transformer', in *Proceedings of the Chinese Control Conference (CCC),* pp. 4532-4537.
19. un, X. *et al.* 2022. 'Transformer with spatio-temporal representation for video anomaly detection', in *Proceedings of the International Conference on Pattern Recognition (ICPR),* pp. 3561-3567.
20. Li, Y. *et al.* 2022. 'Memory-token transformer for unsupervised video anomaly detection', In *Proceedings of the International Conference on Pattern Recognition (ICPR)*, pp. 3553-3560.
21. Tian, Y. *et al.* 2022. 'Weakly supervised video anomaly detection with contrastive multiple instance learning', in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 6, pp. 6103-6111.
22. Wang, J. *et al.* 2022. 'Knowledge distillation for efficient video anomaly detection', *Pattern Recognition Letters*, 158, pp. 30-37.

23. Wu, J. *et al.* 2023. 'Context-aware multiple instance learning for video anomaly detection', *IEEE Transactions on Image Processing*, 32, pp. 2345-2357.
24. Ganin, Y. *et al.* 2016. 'Domain-adversarial training of neural networks', *Journal of Machine Learning Research*, 17, pp. 1-35.
25. Long, M. *et al.* 2015. 'Learning transferable features with deep adaptation networks', in *Proceedings of the International Conference on Machine Learning (ICML)*, pp. 97–105.
26. Chen, C. *et al.* 2021. 'Transfer learning for video anomaly detection: A domain generalization perspective', *Neurocomputing*, 421, pp. 151-161.