PUMAD: PU Metric Learning for anomaly detection

School of Industrial and Management Engineering, Korea University

Jungin Kim

• Contents

Introduction

❖ PUMAD : PU Metric learning for anomaly detection (Information Sciences, 2020)

- POSTECH에서 연구하였고 2022년 10월 7일 기준 21회 인용됨
- 소수의 이상 데이터와 레이블이 되어 있지 않은 데이터를 활용해 정확한 이상 탐지를 가능하게 하는 방법론
- Distance Hashing-base Filtering (DHF)와 Deep Metric Learning (DML) 두 단계로 구성되어 있음

Information Sciences 523 (2020) 167–183

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

PUMAD: PU Metric learning for anomaly detection

Hyunjun Ju[a], Dongha Lee[a], Junyoung Hwang[a], Junghyun Namkung[b], Hwanjo Yu[a,*]

[a] Dept. of Computer Science and Engineering, POSTECH, South Korea
[b] Data Labs, SK Telecom, South Korea

ARTICLE INFO

Article history:
Received 10 June 2019
Revised 23 January 2020
Accepted 11 March 2020
Available online 12 March 2020

Keywords:
Anomaly detection
PU Learning
Metric learning

ABSTRACT

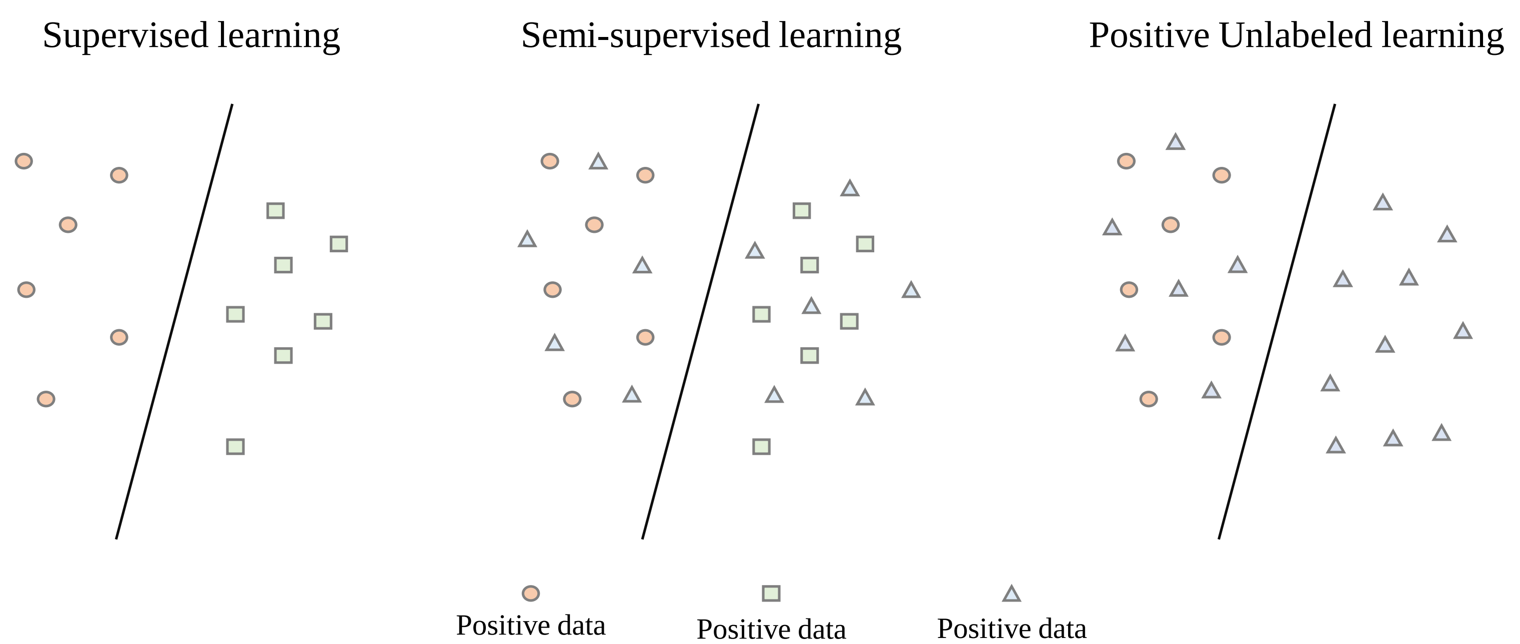
Anomaly detection task, which identifies abnormal patterns in data, has been widely applied to various domains. Most recent work on anomaly detection have focused on an accurate modeling of the normal data based on unsupervised methods. To get a satisfactory anomaly detection accuracy, they need *pure* normal data without abnormal data. This scenario requires many labels to get *pure* normal data. In many real-world scenarios, there exist abundant unlabeled data and a limited number of partially labeled anomalies. This paper proposes a novel anomaly detection method, PUMAD, which uses a Positive and Unlabeled (PU) learning approach to learn from abundant unlabeled data and a small number of partially labeled anomalies (i.e., positives). PUMAD successfully works on the anomaly detection scenario by exploiting deep metric learning with a hashing-based filtering method. Extensive experimental results on real-world benchmark datasets demonstrate that our approach based on PU learning is effective to detect anomalies. PUMAD achieves a much higher accuracy of up to 24% than state-of-the-art competitors.

Introduction

Background

❖ Positive Unlabeled (PU) learning

- Supervised learning : Positive & Negative dataset 모두 사용하여 학습 진행
- Semi-supervised learning : Positive, Negative & unlabeled dataset을 사용하여 학습 진행
- **Positive Unlabeled learning : Positive & unlabeled dataset을 사용하여 학습 진행**

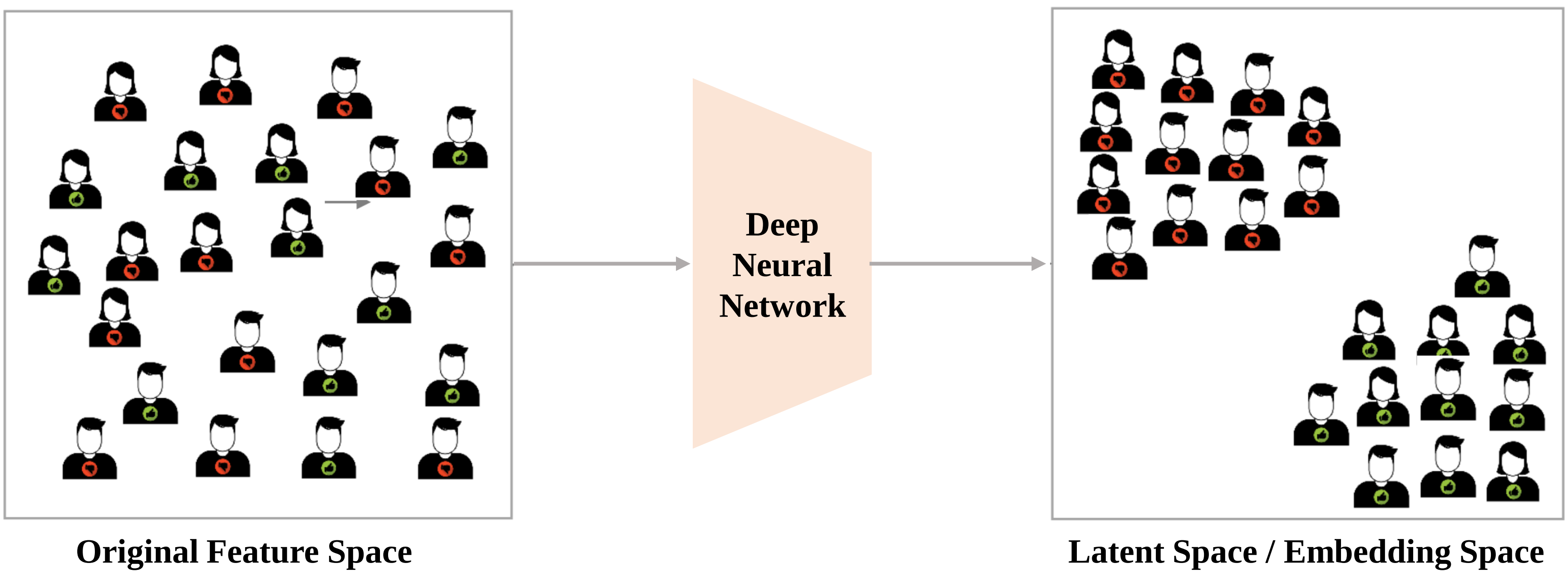


Introduction

Background

❖ Deep Metric learning

- 유사한 것(같은 클래스)끼리 가깝게 유사하지 않은 것(다른 클래스)끼리 멀게 하는 특징을 추출
- 즉, 심층 신경망으로 거리 공간을 학습
- 학습을 위해 사용하는 손실함수는 주로 contrastive loss, triplet loss 등이 존재함

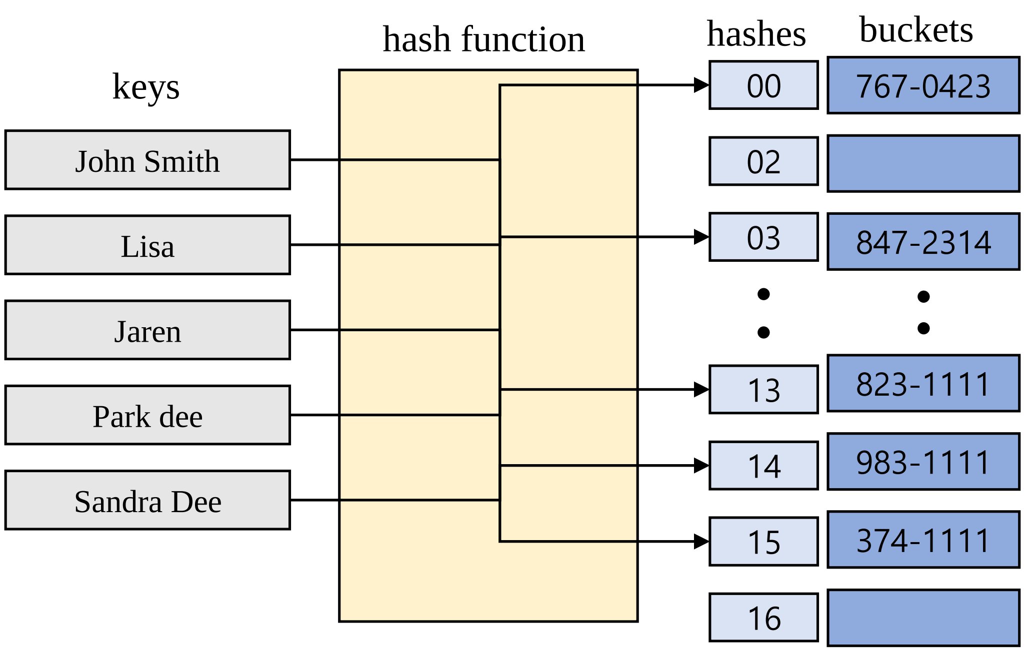


Introduction

Background

❖ Hash Function

- 데이터의 효율적 관리를 목적으로 임의의 길이의 데이터를 고정된 길이의 데이터로 매핑하는 함수
- 해시함수를 사용해 key를 hash 값으로 매핑, hash 값을 index로 사용해 데이터를 bucket에 저장



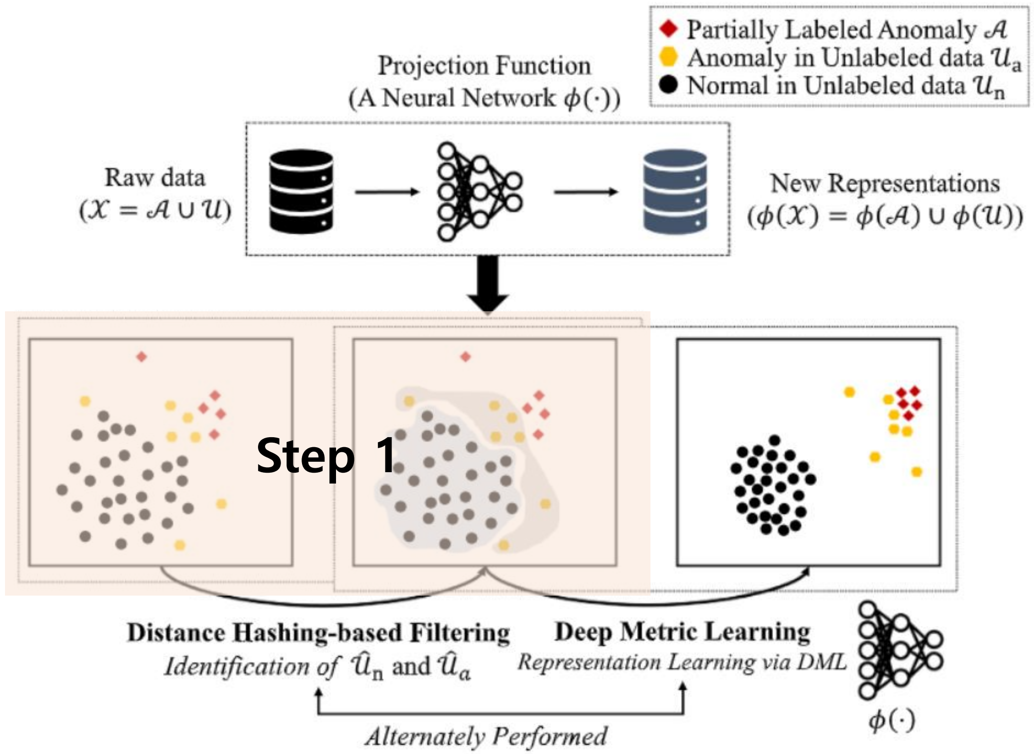
Hash Value	Data
00	767-0423
03	847-2314
13	823-1111
14	983-1111
15	374-1111

Proposed Method

Overall Framework

❖ PUMAD : PU Metric learning for anomaly detection

- 인공신경망을 통해 embedding 된 공간상에서 이상과 정상을 구분하는 함수를 학습하는 것이 목적
- Embedding은 두 단계를 번갈아 가면서 수행 → Distance Hashing-based Filtering & Deep Metric Learning
- **Distance Hashing-based Filtering: Reliable normal과 Potential abnormal data 분리**

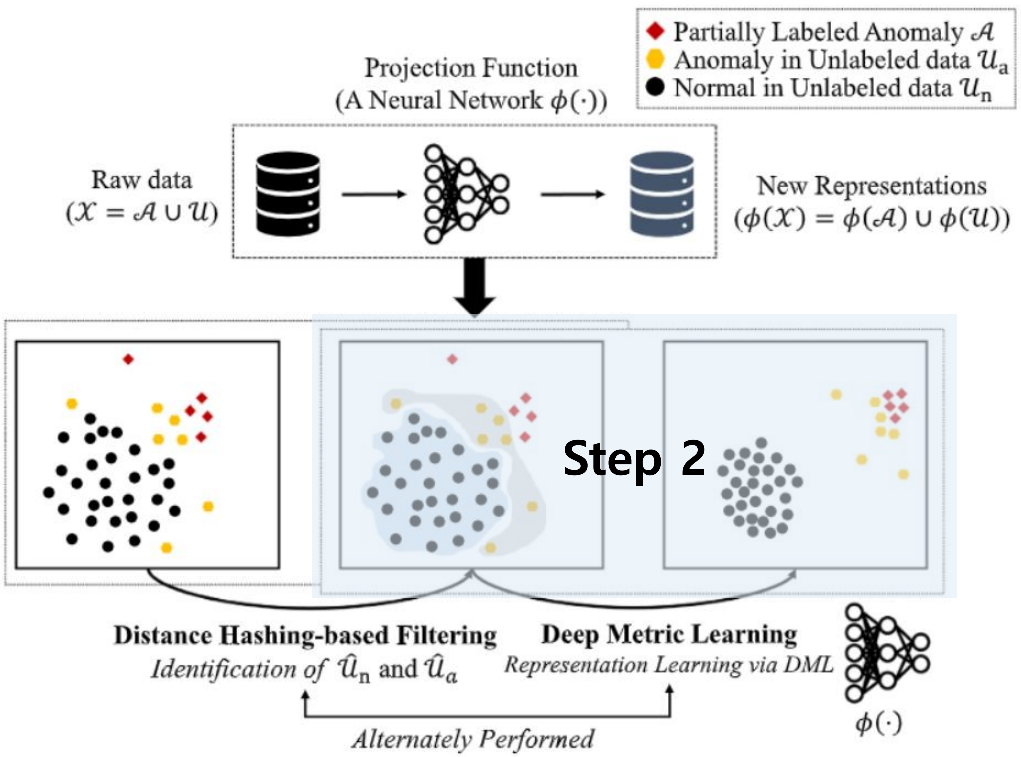


Proposed Method

Overall Framework

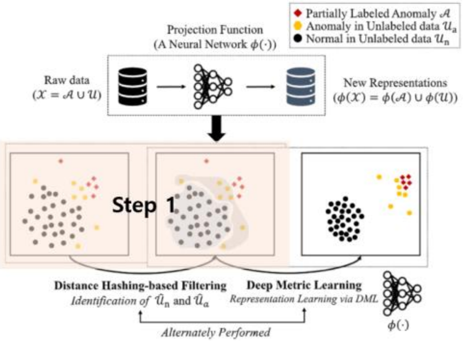
❖ PUMAD : PU Metric learning for anomaly detection

- 인공신경망을 통해 embedding 된 공간상에서 이상과 정상을 구분하는 함수를 학습하는 것이 목적
- Embedding은 두 단계를 번갈아 가면서 수행 → Distance Hashing-based Filtering & Deep Metric Learning
- **Deep Metric Learning: Distance Hashing-based Filtering을 통해 분리된 데이터를 사용해 Deep Metric Learning 진행**



DMQA

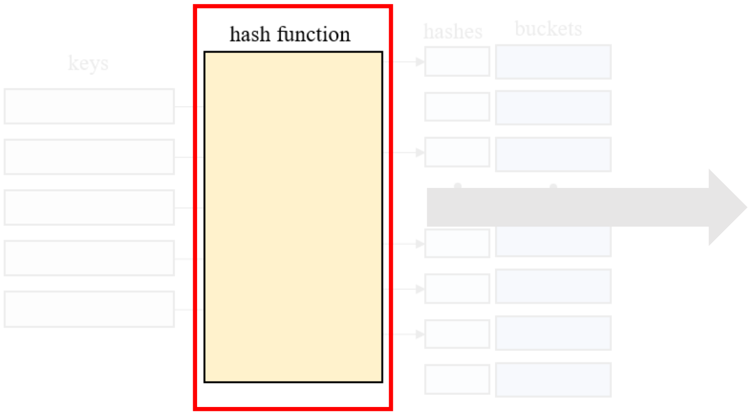
Proposed Method

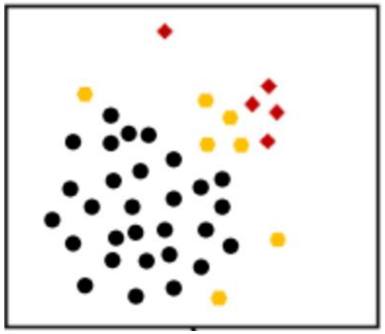


PUMAD : PU Metric learning for anomaly detection

❖ Step 1: Distance Hashing-based Filtering (DHF)

- Hash table을 구성하기 위해 hash function 정의
- Target sample u가 선택된 이상 정상 샘플 a_*에 가까우면 거리 함수($d(u; a_*, u_*)$)는 큰 값을 가짐
- Target sample u가 선택된 이상 레이블이 없는 샘플 u_*에 가까우면 거리 함수($d(u; a_*, u_*)$)는 작은 값을 가짐
- ($d(u; a_*, u_*)$)가 0보다 큰 값을 가지면 1, 0보다 작으면 0으로 리턴해주는 1-bit 해시 함수 정의





u_*: *unlabeled sample*
a_*: *labeled anomailes sample*
u: *target unlabeled sample*

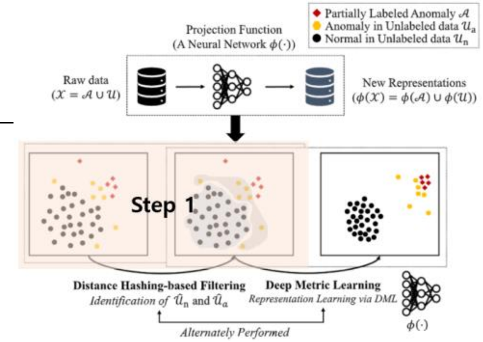
$$d(u; a_*, u_*) = ||\phi(u) - \phi(u_*)||_2^2 - ||\phi(u) - \phi(a_*)||_2^2$$

$$h(u; a_*, u_*) = \begin{cases} 1 & if\ d\ (u; a_*, u_*) \geq 0 \\ 0 & otherwise \end{cases}$$

$$\varkappa = \{h(\cdot; a_*, u_*) | \forall a_* \in \mathrm{A}, u_* \in u\}$$

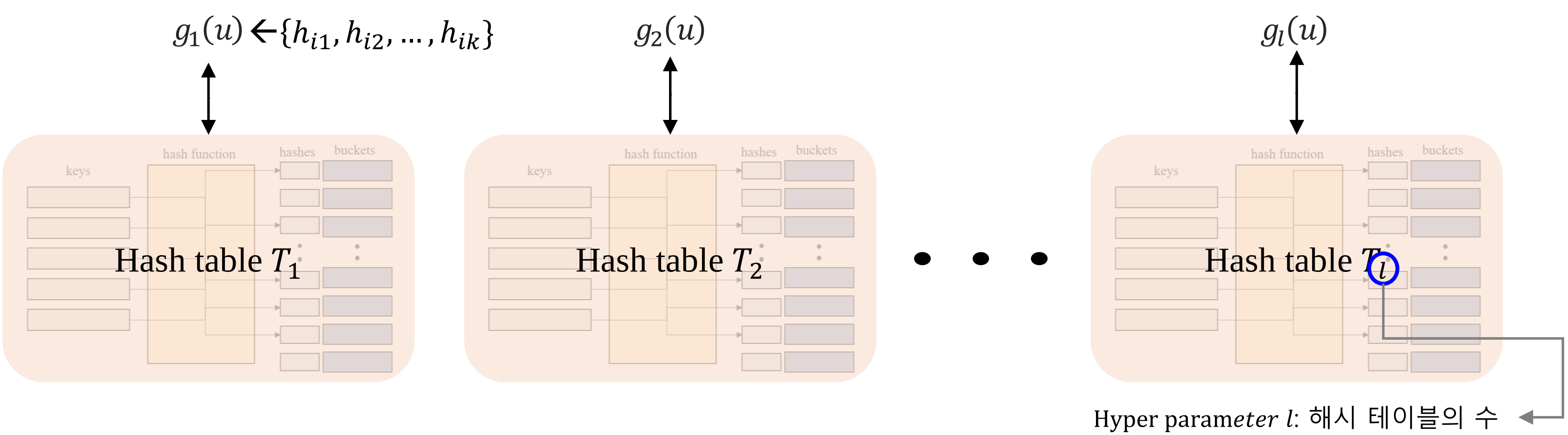
Proposed Method

PUMAD : PU Metric learning for anomaly detection



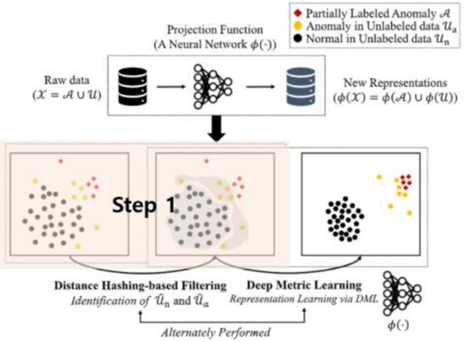
❖ Step 1: Distance Hashing-based Filtering (DHF)

- Embedding 공간에서 더 정확한 indexing을 위해 k-bit 해시 함수 $g_i(u)$ 사용
- k-bit 해시 함수는 1-bit 해시 함수의 집합 $\varkappa$ 로부터 k(1-bit 해시 함수의 수)개 만큼 랜덤 샘플링을 통해 생성함
- 하이퍼 파라미터 l의 수 만큼 해시 테이블 생성 및 k-bit 해시 함수 생성



Proposed Method

PUMAD : PU Metric learning for anomaly detection



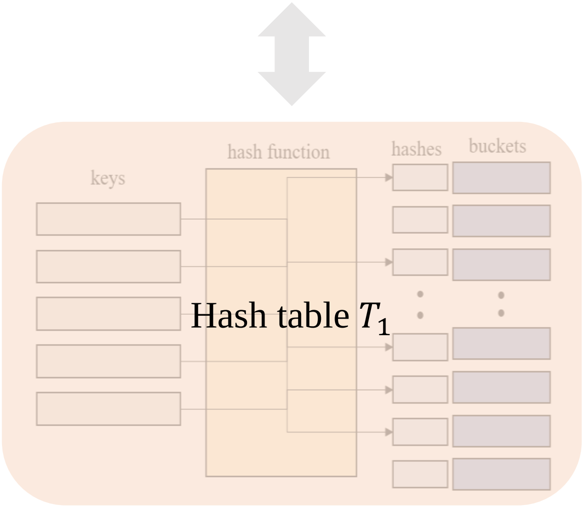
❖ Step 1: Distance Hashing-based Filtering (DHF)

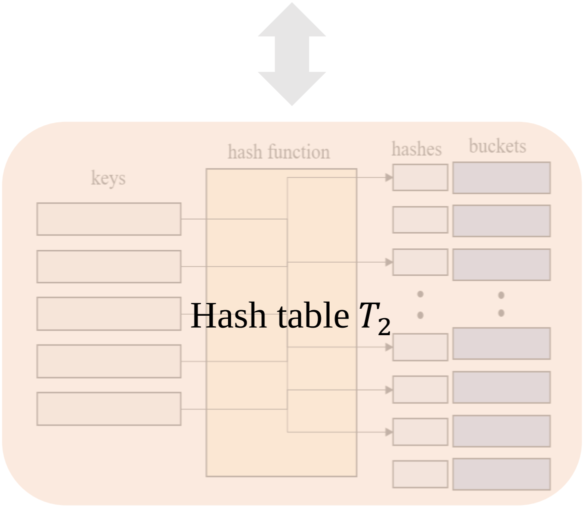
- Ex) $k = 4, l = 3$

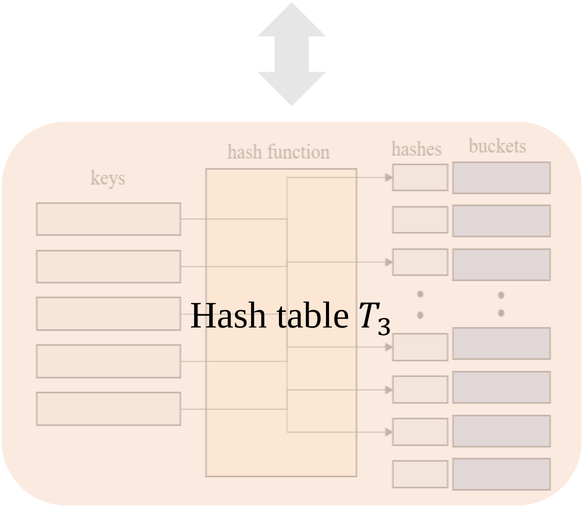
$g_1(u_j) \leftarrow \{h_{11}(u_j), h_{12}(u_j), h_{13}(u_j), h_{14}(u_j)\}$

$g_2(u_j) \leftarrow \{h_{21}(u_j), h_{22}(u_j), h_{23}(u_j), h_{24}(u_j)\}$

$g_3(u_j) \leftarrow \{h_{31}(u_j), h_{32}(u_j), h_{33}(u_j), h_{34}(u_j)\}$



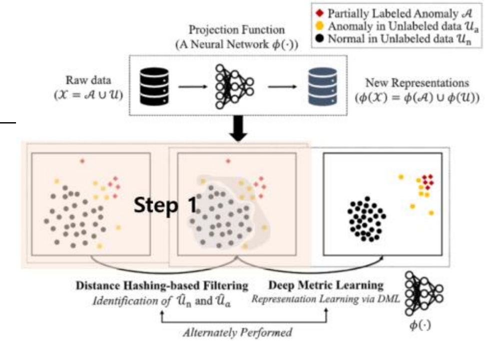




DMQA

Proposed Method

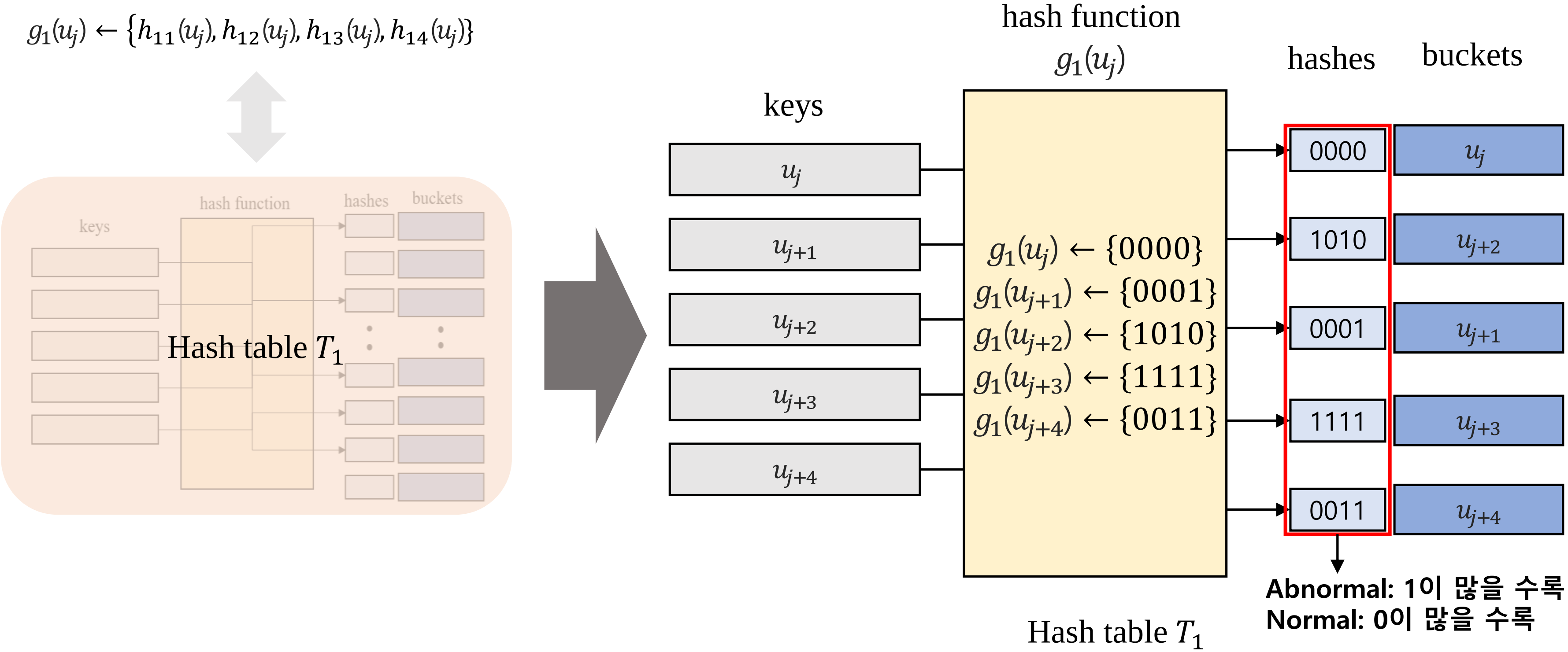
PUMAD : PU Metric learning for anomaly detection



$$h(u; a_*, u_*) = \begin{cases} 1 & if\ d(u; a_*, u_*) \geq 0 \\ 0 & otherwise \end{cases}$$

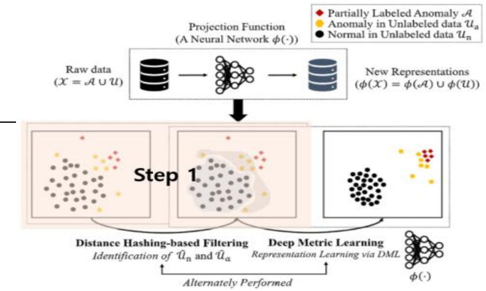
❖ Step 1: Distance Hashing-based Filtering (DHF)

- Ex) $k = 4, l = 3$
- u_j값은 unlabeled dataset(U)로부터 샘플링한 target sample



DMQA

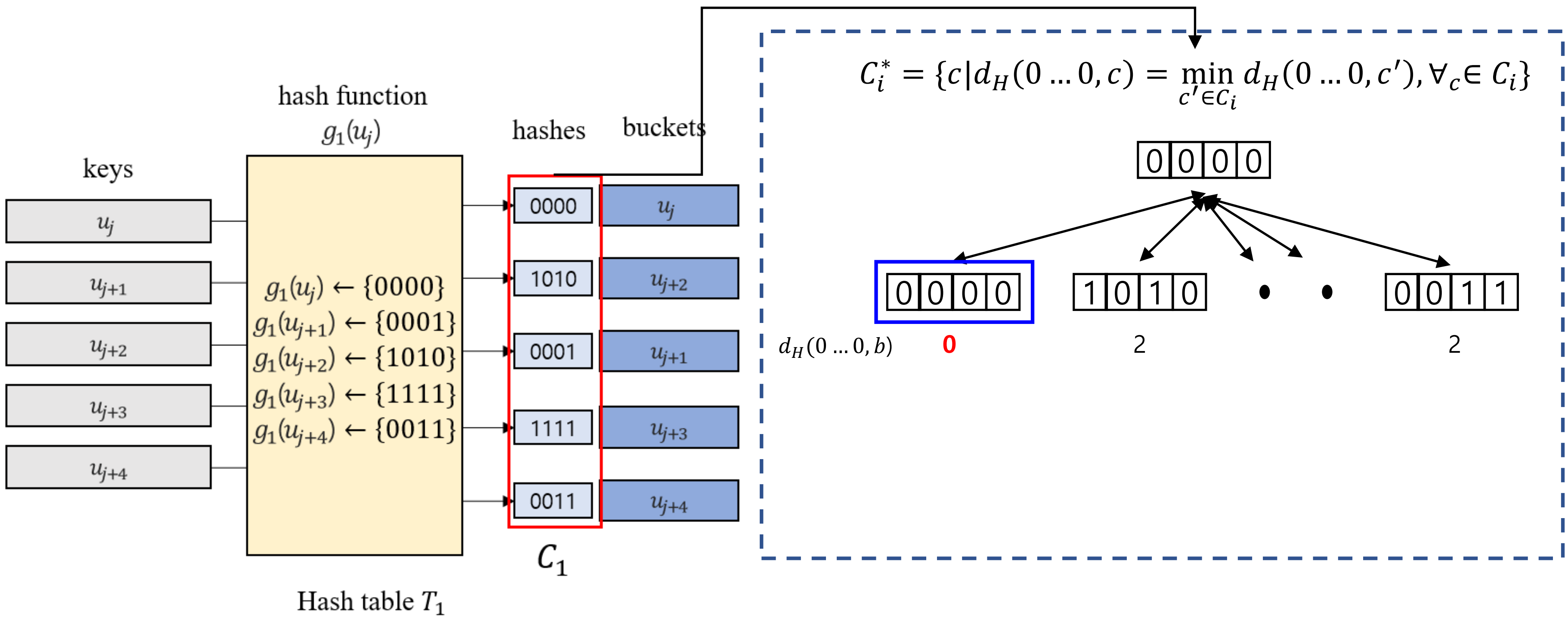
Proposed Method



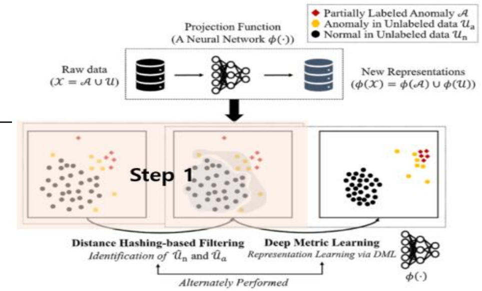
PUMAD : PU Metric learning for anomaly detection

❖ Step 1: Distance Hashing-based Filtering (DHF)

- Hamming distance를 사용해 모든 bit가 0인 해시 코드와 각 테이블(T_i)마다 존재하는 모든 해시 코드($c \in C_i$)를 비교하여 Hamming distance가 가장 작은 해시 코드(c)를 추출함
- Hamming distance($d_H(a, b)$): a, b 두 해시 코드를 비교해 다른 bit의 개수를 결과로 도출하는 함수



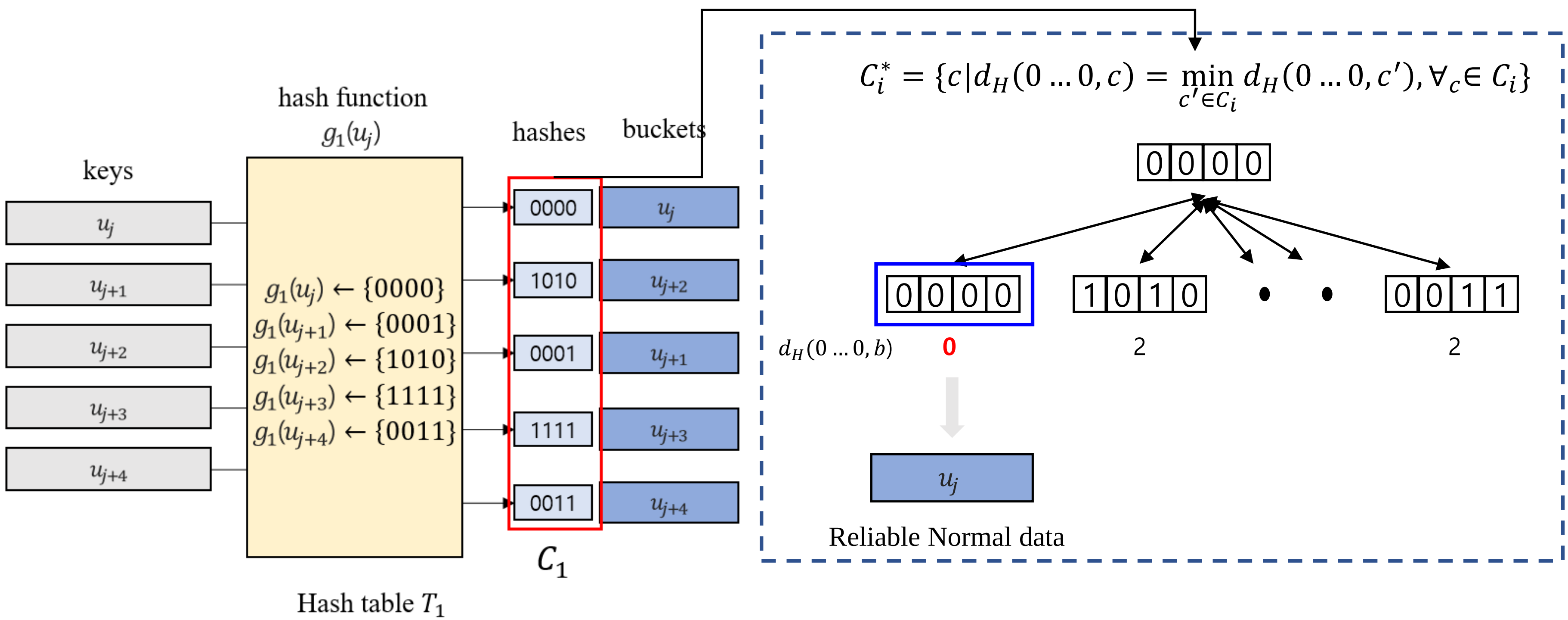
Proposed Method



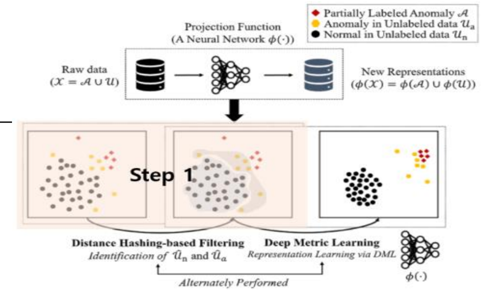
PUMAD : PU Metric learning for anomaly detection

❖ Step 1: Distance Hashing-based Filtering (DHF)

- 각 테이블 마다 나오는 C_i^*값에 해당하는 bucket에 저장되어 있는 데이터 reliable normal data로 pseudo labeling 진행



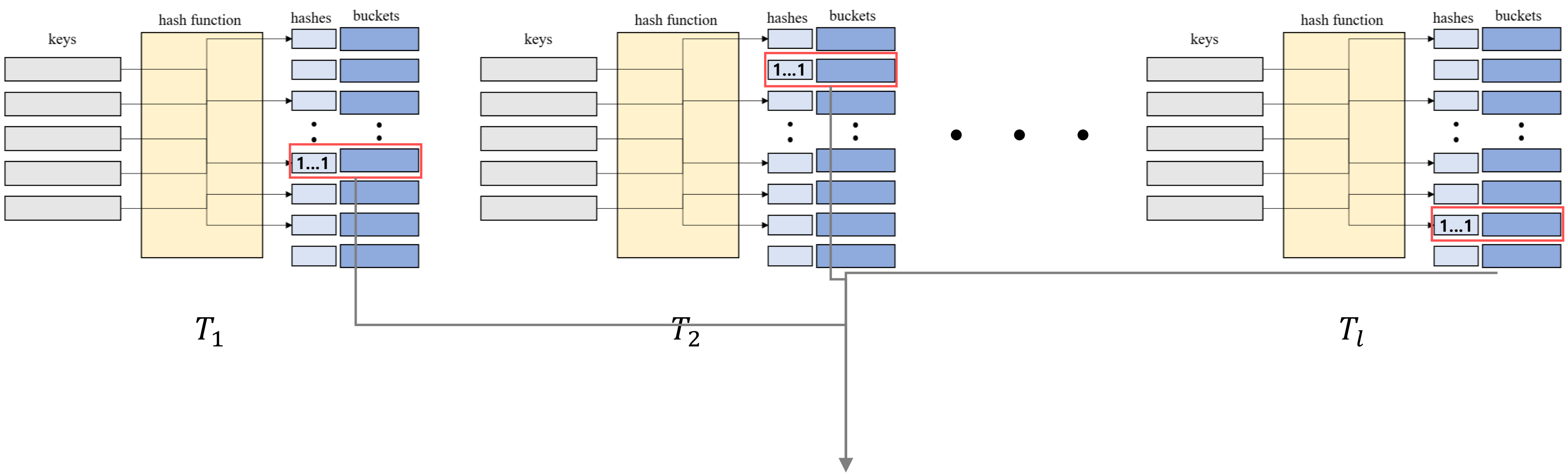
Proposed Method



PUMAD : PU Metric learning for anomaly detection

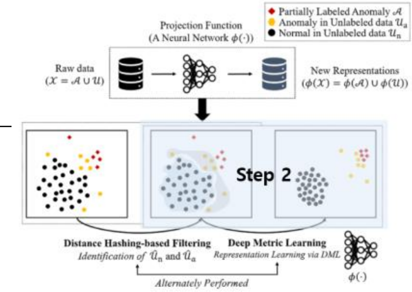
❖ Step 1: Distance Hashing-based Filtering (DHF)

- Potential anomaly data는 모든 테이블에서 해시 코드가 전부 1인 해시 값에 대응하는 target sample에 pseudo labeling 진행
- 추가로, reliable normal dataset에 있는 데이터와 중복되면 제거함



Potential anomaly data

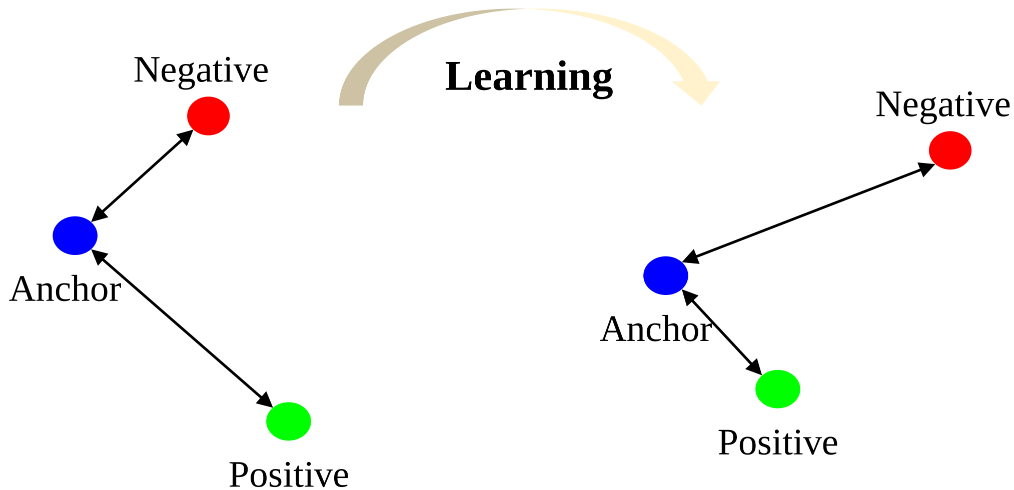
Proposed Method



PUMAD : PU Metric learning for anomaly detection

❖ Step 2: Deep Metric Learning (DML)

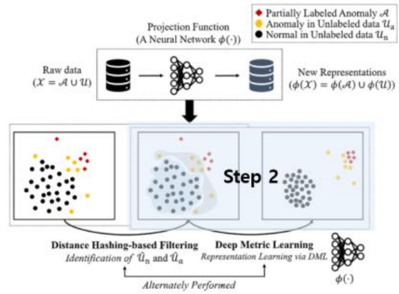
- Distance Hashing-based Filtering을 통해 분리된 데이터를 사용해 Deep Metric Learning 진행
- 분리된 Potential anomaly dataset과 Reliable normal dataset 그리고 기존 labeled anomaly dataset을 사용해 DML 진행
- Deep Metric Learning을 위한 손실 함수로 triplet loss 사용
- Triplet loss: positive sample은 가까이, negative sample은 멀리 배치하도록 학습 진행



$$L = \max(d(a,p) - d(a,n) + margin, 0)$$

DMQA

Proposed Method



PUMAD : PU Metric learning for anomaly detection

❖ Step 2: Deep Metric Learning (DML)

- 두 가지 triplet loss를 정의하여 두 값의 합이 최소화 되는 방향으로 학습 진행
  - ✓ Anchor가 정상 데이터 셋과 이상 데이터 셋에서 샘플 되는 경우를 고려함
- $\mathcal{L}_a$: labeled anomaly dataset과 potential anomaly dataset의 합집합에서 anchor와 positive pair를 샘플링하고 reliable normal dataset에서 negative를 샘플링하여 triplet loss 계산
- $\mathcal{L}_n$: labeled anomaly dataset과 potential anomaly dataset의 합집합에서 negative pair를 샘플링하고 reliable normal dataset에서 positive pair를 샘플링하여 triplet loss 계산

$$\boldsymbol{x^*, x^+ \in A \cup \widehat{U_a} \ and \ x^- \in \widehat{U_n}}$$

$$\mathcal{L}_a = \sum_{\forall (x^*, x^+, x^-) \in \mathfrak{I}_a} [\, ||\emptyset(x^*) - \emptyset(x^+)||_2^2 - ||\emptyset(x^*) - \emptyset(x^-)||_2^2 + \alpha]$$

$$\boldsymbol{x^*, x^+ \in \widehat{U_n} \ and \ x^- \in A \cup \widehat{U_a}}$$

$$\mathcal{L}_n = \sum_{\forall (x^*, x^+, x^-) \in \mathfrak{I}_n} [\, ||\emptyset(x^*) - \emptyset(x^+)||_2^2 - ||\emptyset(x^*) - \emptyset(x^-)||_2^2 + \alpha]$$

$$\min_{\emptyset(\cdot)} \mathcal{L} = \mathcal{L}_a + \mathcal{L}_n$$

$$s.t. \ ||\emptyset(x)||_2 \le 1, \forall_x \in x$$

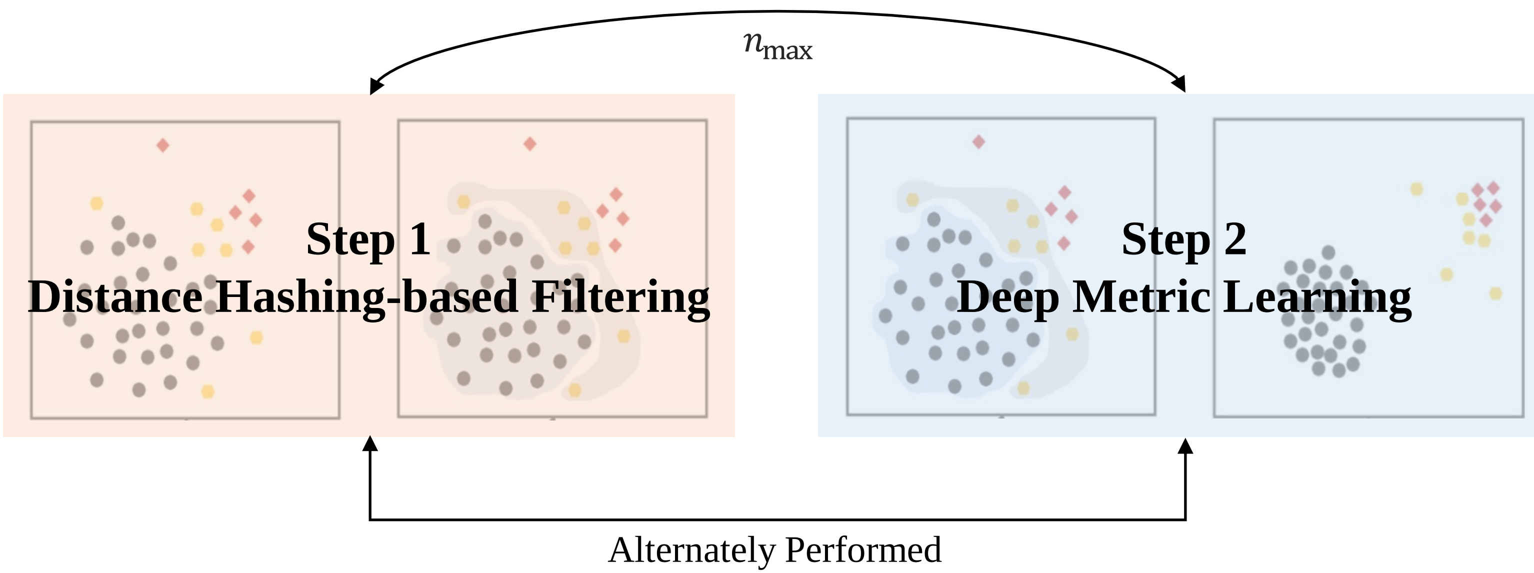
DMQA

Proposed Method

PUMAD : PU Metric learning for anomaly detection

❖ Alternative stopping criteria

- PUMAD 알고리즘 학습을 위해 반복 횟수($n_{\max}$)와 triplet loss 최소값($\mathcal{L}_{min}$) 사전에 설정
- Bucket의 평균 수($avg_{buckets}$)와 triplet loss가 작아지는 방향으로 학습 진행
- 반복 횟수만큼 학습이 진행된 embedding function($\emptyset^*(\cdot)$)을 최종 결과로 도출함



Experiment

PUMAD : PU Metric learning for anomaly detection

❖ Experiment 1

- PU learning 환경에서 실험 진행을 위해 이상 탐지에 많이 사용되는 오픈 데이터 셋에서 일부 샘플링을 진행
  - ✓ 이상 데이터의 비율을 1~10% 조절하여 기존 이상 탐지 알고리즘과 성능 비교 실험 진행
- 샘플링한 대부분의 tabular dataset에서 기존 알고리즘 대비 우수한 성능을 보임

AUC scores on tabular datasets.

	OC-SVM(Pure)	OC-SVM	DAE(Pure)	DAE	ALAD (Pure)	ALAD	PUDAE	DGM	nnPU	ADOA	$\text{PUMAD}_{\text{noDHF}}$	PUMAD
Cardio	0.9788	0.8636	0.9745	0.9650	0.9669	0.9654	0.9688	0.9794	0.8101	0.9676	0.8681	**0.9843**
Thyroid	0.9766	0.9115	0.9811	0.9759	0.9772	0.9752	0.9693	0.9773	0.9808	0.9788	0.9507	**0.9818**
KDD Cup	0.9629	0.9285	0.9252	0.8648	0.9661	0.8116	0.8990	0.9178	0.9572	0.9933	0.9658	**0.9935**
Satellite	0.6914	0.5897	0.6412	0.6380	0.6949	0.6188	0.5804	0.7885	0.6111	0.7748	0.7670	**0.8488**
Annthyroid	0.6842	0.5775	0.7292	0.7105	0.7589	0.7205	0.7100	0.8586	0.7556	0.8579	0.6759	**0.9634**
Satimage-2	0.9442	0.9002	0.9375	0.9369	0.9929	0.9892	0.9287	0.8720	0.9911	**0.9930**	0.9092	0.9929
Mammography	0.6983	0.6072	0.9209	0.8645	0.8765	0.8026	0.9295	0.9032	0.7256	0.9209	0.8307	**0.9345**
Letter	0.5506	0.5300	0.5783	0.5752	0.5428	0.5426	0.5558	0.5995	0.6229	0.6539	0.6139	**0.7397**
Shuttle	0.9948	0.8612	0.9899	0.9882	**0.9980**	0.8931	0.9893	0.9750	0.9708	0.9852	0.9762	0.9958
Arrhythmia	0.8986	0.8903	0.8975	0.8958	0.9028	0.8956	0.8958	0.7911	0.7220	0.8903	0.7121	**0.9094**
Musk	1.0000	0.9152	1.0000	1.0000	1.0000	1.0000	1.0000	0.9608	1.0000	1.0000	1.0000	**1.0000**
Ammonia	0.7366	0.6403	0.6724	0.6638	0.7174	0.6796	0.7225	0.7182	0.7473	0.7925	0.7397	**0.9828**
Acetaldehyde	0.9435	0.8041	0.8442	0.8370	0.8638	0.8354	0.8593	0.8760	0.5134	0.8802	0.7634	**0.9758**
Acetone	0.7611	0.5429	0.6960	0.6878	0.7126	0.6912	0.7471	0.7853	0.8235	0.8326	0.7241	**0.9837**
Ethylene	0.8193	0.7684	0.6937	0.6895	0.7245	0.7020	0.7166	0.5559	0.5319	0.7078	0.6525	**0.9245**
Ethanol	0.8870	0.6848	0.6271	0.6228	0.7469	0.6566	0.6536	0.7790	0.6337	0.8601	0.7237	**0.9769**
Toluene	0.9321	0.8912	0.8942	0.8884	0.9165	0.8999	0.9047	0.7908	0.6327	0.9566	0.7711	**0.9813**

Experiment

PUMAD : PU Metric learning for anomaly detection

❖ Experiment 2

- 이미지 데이터 셋(Mnist)에 대해서도 기존 알고리즘 대비 뛰어난 성능을 보임
- 한 가지 클래스만을 정상 범주로 설정하고 나머지 클래스에 대해서는 이상 범주로 설정한 후 실험 진행

AUC scores on image dataset.

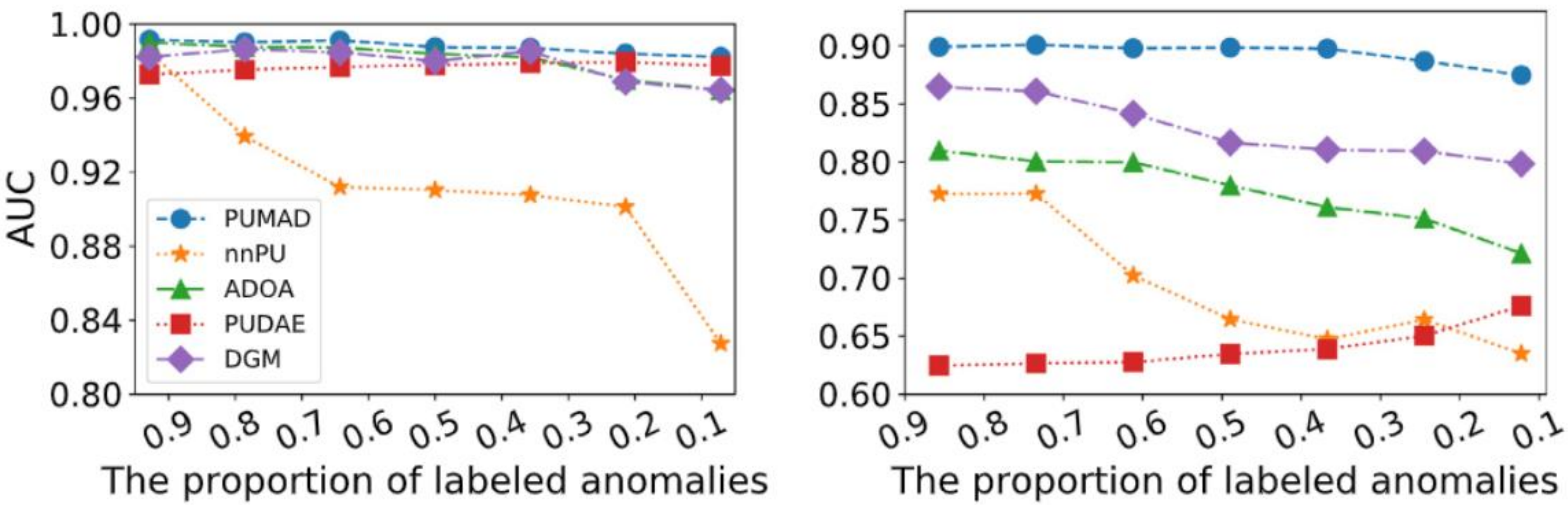
	OC-SVM(Pure)	OC-SVM	DAE(Pure)	DAE	ALAD (Pure)	ALAD	PUDAE	DGM	nnPU	ADOA	$\text{PUMAD}_{\text{noDHF}}$	PUMAD
Mnist 0	0.9423	0.8719	0.9514	0.9236	0.9514	0.9391	0.9103	0.8631	0.9169	0.8758	0.9127	**0.9954**
Mnist 1	0.9853	0.9786	0.9860	0.9815	0.9834	0.9828	0.9819	0.8512	0.8948	0.9895	0.9466	**0.9924**
Mnist 2	0.7730	0.7325	0.8199	0.7720	0.8370	0.7778	0.7612	0.7540	0.7093	0.6097	0.8339	**0.9644**
Mnist 3	0.8393	0.8077	0.8750	0.8402	0.8544	0.8414	0.8300	0.7337	0.8162	0.8000	0.7905	**0.9664**
Mnist 4	0.8774	0.8383	0.8669	0.8408	0.8310	0.8303	0.8363	0.8546	0.7708	0.8340	0.8224	**0.9813**
Mnist 5	0.7499	0.7171	0.7976	0.7515	0.8207	0.7951	0.7449	0.7932	0.7340	0.7325	0.7604	**0.9445**
Mnist 6	0.9305	0.8818	0.9315	0.9046	0.9048	0.8977	0.8986	0.8090	0.8858	0.8200	0.8745	**0.9873**
Mnist 7	0.9091	0.8582	0.9162	0.8878	0.9072	0.9043	0.8873	0.8153	0.8420	0.8944	0.8288	**0.9771**
Mnist 8	0.7916	0.7322	0.8130	0.7645	0.7721	0.7535	0.7588	0.7452	0.7389	0.6694	0.7550	**0.8701**
Mnist 9	0.9210	0.8900	0.9253	0.8995	0.9157	0.9044	0.8952	0.7011	0.6607	0.8421	0.8004	**0.9329**

Experiment

PUMAD : PU Metric learning for anomaly detection

❖ Experiment 3

- Labeled anomaly의 비율에 따른 AUC 성능 평가 실험 진행
- Anomaly 비율이 낮아지더라도 우수한 성능을 유지하는 것을 확인함



(a) Cardio (b) Satellite

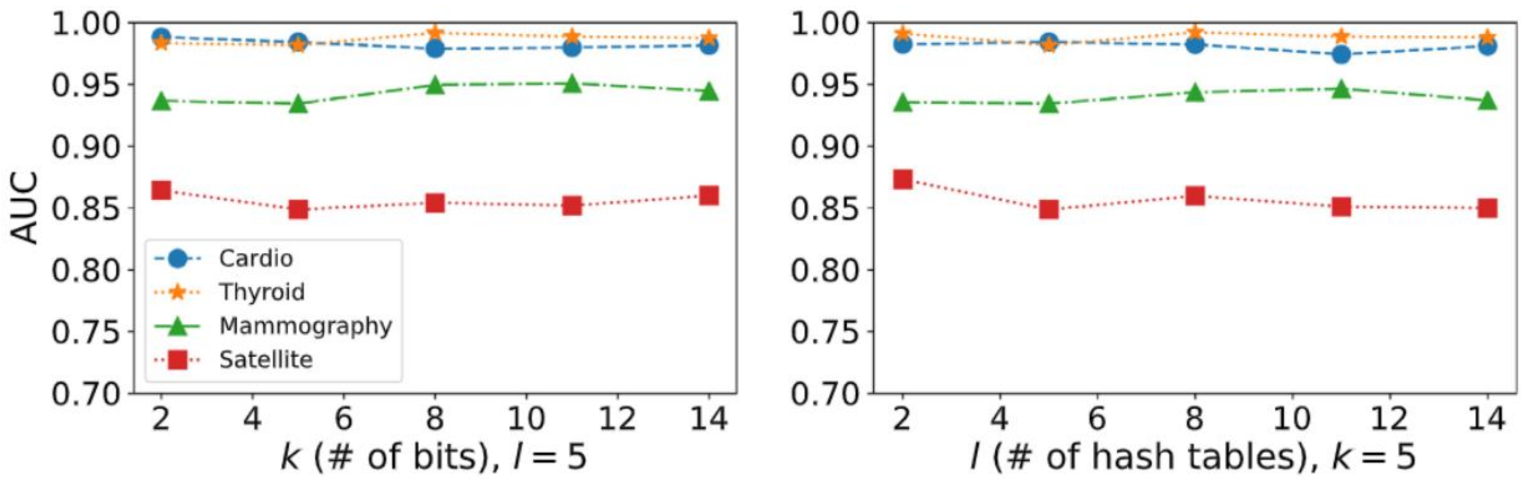
DMQA

Experiment

PUMAD : PU Metric learning for anomaly detection

❖ Experiment 4

- Hyper parameter k & l의 변화에 따른 제안 알고리즘의 성능 비교 실험을 진행함
- k값과 l 값의 변화에도 성능이 큰 변화가 없음 → Robust함을 증명



DMQA

Conclusion

PUMAD : PU Metric learning for anomaly detection

❖ Conclusion

- 현실 에서처럼 소수의 이상 데이터와 레이블이 없는 데이터만 존재할 때 이상 탐지를 위한 효과적인 방법론
- Deep Metric learning이 이상 탐지에서 성공적으로 작동함을 증명함
- Image, tabular dataset 등 다양한 데이터 셋에 적용 가능

❖ Reference

- http://dmqm.korea.ac.kr/activity/seminar/342
- http://dsba.korea.ac.kr/seminar/?mod=document&uid=1813
- https://ratsgo.github.io/data%20structure&algorithm/2017/10/25/hash/
- https://gmnam.tistory.com/59
- https://mic97.tistory.com/16
- https://velog.io/@hanseokjo/Paper-Review-Learning-from-positive-and-unlabeled-data-a-survey-Jessa

Thank You