
PRIVACY-PRESERVING HETEROGENEOUS NETWORK EMBEDDING FOR CLINICAL EVENTS

Gustavo L. de Oliveira^{*1} Ricardo M. Marccacini^{*1} Maria da Graça C. Pimentel^{*1}

ABSTRACT

Heterogeneous Information Networks (HINs) are a promising alternative for representing clinical events that contain inter-related and multi-typed data, such as patient data and their relationships with medical diagnoses, description of symptoms, anamnesis, and observations. Network embeddings methods propose mapping an information network to a latent space (i.e., embedding space) to preserve the structure in a low dimensional vector space, thereby enabling the use of machine learning methods based on vector-space models. However, since most network embeddings methods do not consider strategies for omitting users' private features, adversaries can use embeddings to infer sensitive user information. Moreover, recent proposed methods are suitable only for homogeneous networks. We propose the Private Heterogeneous Information Network Embeddings (PHINE) approach for privacy-preserving heterogeneous network embedding for clinical events. We explore Graph Autoencoders (GAE) with an objective function that simultaneously maximizes the embeddings' usefulness for classification tasks (i.e., preserving HIN properties and topology) and minimizes the effectiveness of inference attacks from embedding (i.e., hiding private information). To the best of our knowledge, this is the first privacy-preserving approach on clinical events data for heterogeneous networks. The experimental results reveal that PHINE presents a competitive trade-off between privacy-preserving and utility feature prediction.

1 INTRODUCTION

Electronic Health Records (EHR) databases have become increasingly popular in data mining and machine learning tasks (Ghassemi et al., 2020). The aim is to extract valuable knowledge from patient's health data toward supporting medical decision-making. EHR data contains unstructured textual information from medical diagnoses, including a description of symptoms, anamnesis, and observations. EHR also holds structured data, such as the patient's age, sex, weight, socioeconomic information, and different structured information from clinical examinations. Thus, a challenge is to obtain an appropriate representation from EHR datasets that considers both structured and unstructured patient data as well as their relationships (Hosseini et al., 2018).

Heterogeneous Information Networks (HINs) are a promising alternative for representing datasets that contain inter-related and multi-typed data (Shi et al., 2017). HINs have nodes of different types, such as patients and medications. Links or connections represent relationships between pa-

tients and clinical events. Because HINs are powerful for modeling complex data relationships, network embedding methods propose mapping an information network to a latent space (i.e., embedding space) to preserve the structure in a low dimensional vector space (Cui et al., 2019).

Network embedding methods have been successful in many applications (Cui et al., 2019). Many projects make the network embeddings publicly available for machine learning tasks such as classification, clustering, and recommendation, which demands omitting the original information network to preserve sensitive information. However, studies showed that inference attacks allow reconstructing the network structure to predict sensitive and private features (Kong et al., 2020). Yet, techniques to sanitize network data through noise or graph pruning have not been successful in mitigating such attacks (Cai et al., 2018; He et al., 2018).

Existing privacy-preserving network embedding methods consider only homogeneous information networks formed by a single type of node and relationship (Xu et al., 2018; Zhang & Ni, 2019; Li et al., 2020). Moreover, LGPD and GDPR data protection laws introduce the *Right to Erasure* right that obligates data holders to conceal users' private information. Thus, we raise the following question: how to learn privacy-preserving embeddings from clinical events heterogeneous networks?

^{*}Equal contribution ¹Institute of Mathematics and Computer Sciences, University of São Paulo, São Carlos, Brazil. Correspondence to: Gustavo L. de Oliveira <gustavo.lima@usp.br>.

In this paper, we propose the Privacy-Preserving Heterogeneous Information Network Embeddings (PHINE) approach for clinical events. Our approach generates embeddings in two stages. The first stage models the heterogeneous network from an EHR dataset and uses the textual information nodes to generate initial embeddings using a pre-trained neural language model. We use a network regularization framework to propagate the initial embeddings to all remaining nodes in the heterogeneous network. This stage provides embeddings for machine learning tasks that are vulnerable to inference attacks. The second stage uses a GAE (Graph Autoencoder) (Kipf & Welling, 2016) to both (i) preserve utility features with maximization of the reconstruction of the first stage embeddings and the respective HIN, and (ii) penalize the Autoencoder optimization function when inference attacks are successful. The GAE explores two advances in representation learning for graphs: graph convolutional network to learn how to preserve important HIN information (utility features) and adversarial learning to minimize inference attacks and omit sensitive information (private features).

Our experimental evaluation used a synthetic EHR dataset to generate the clinical events heterogeneous network. We evaluated PHINE considering the embedding usefulness for classification tasks and its ability to preserve private information from inference attacks. The experimental results indicate that our approach presents a competitive trade-off between privacy-preserving and utility feature prediction.

2 RELATED WORK

Heterogeneous Information Networks (HINs) have been successful in several real-world applications such as bibliographic citation networks (Zhou et al., 2019), recommender systems (Shi et al., 2019), and medical diagnosis from EHR datasets (Hosseini et al., 2018). The use of relational data representations pose challenges to network processing and analysis (Cui et al., 2019), such as high computational complexity, low parallelizability, and inapplicability of machine learning algorithms based on vector-space models. Network embeddings have been used to address these challenges (Goyal & Ferrara, 2018).

Network embeddings use a low dimensional vector representation for each node, in which topological and structural characteristics of a node are encoded in the embedding space.

Recently, authors report applying deep learning methods to network embedding. Graph Autoencoders (GAE) (Kipf & Welling, 2016) embeds a graph to a low dimensional space using Graph Convolutional Network (GCN). GCN is an extension of Convolutional Neural Network CNN for graph-structured data (Zhang et al., 2020). An advantage of GCN

is to explore node attributes, network topology, and labeled information for learning representation in a semi-supervised way (Wu et al., 2021).

Kong et al. (2020) observe that users’ private information is vulnerable in network embeddings. The *model inversion attack*, for example, uses a set of labeled data (obtained from trading or hacking (Al-Rubaie & Chang, 2019)), trains classification or regression models, and infers private attributes from the embeddings (Ellers et al., 2019).

Towards preventing attacks, Xu et al. (2018) and Zhang & Ni (2019) implement differential privacy by adding and removing links among and nodes in the network. However, these methods do not deal with inference attacks on users’ private features. Jia & Gong (2018), Cai et al. (2018) and He et al. (2018) propose achieving privacy preservation by direct sanitization of graphs topology. Sanitization can fail in cases of no prior knowledge about the domain because it requires identifying which attributes, links and nodes are the most correlated with private information. To tackle those gaps, Li et al. (2020) developed the Adversarial Privacy Graph Embedding (APGE) framework for homogeneous networks. Their approach combines graph convolutional networks and adversarial training to integrate the Privacy-Disentangled and Privacy-Purged mechanisms.

Given the promising results for privacy-preserving embedding achieved by Li et al. (2020), we extend their approach for heterogeneous networks of clinical events.

3 PRIVATE HETEROGENEOUS INFORMATION NETWORK EMBEDDING

3.1 Problem Definition

Patient data from EHR (Electronic Health Records) datasets can be organized into clinical events. In particular, we are interested in textual excerpts from the EHR, such as treatment descriptions, laboratory tests, symptoms and prescriptions. A clinical event can be defined as a triple $e = (\vec{p}_i, t_j, \vec{u}_{t_j})$, where \vec{p}_i represents the feature vector of the i -th patient, t_j represents some textual information extracted from the patient’s EHR, and \vec{u}_{t_j} represents the feature vector generated from the textual information t_j after the use of some word embedding model.

A set of n clinical events $E = \{e_1, e_2, \dots, e_n\}$ extracted from an EHR dataset is very useful for a wide variety of machine learning algorithms and medical applications. In clinical events, the \vec{p}_i features of each patient are private (e.g. gender, age, ethnicity, location, and other personal information) and should not be available for these algorithms. On the other hand, \vec{u}_{t_j} represent utility features and contain relevant knowledge for machine learning algorithms.

A trivial strategy for dealing with private features is to re-

move the \vec{p}_i from clinical events. However, several works in the literature demonstrate that inference attacks from the utility features allow to recover the private features with significant accuracy. Thus, in addition to removing such private features from clinical events, we aim to obtain a new representation of clinical events that respects two conditions: (1) preserve the relevant knowledge of the utility features and (2) avoid inference attacks of the private features from utility features.

Formally, we aim to learn a mapping function $f : E \rightarrow \mathbf{Z}^d$ from clinical events E to a d -dimensional representation \mathbf{Z} , in which \mathbf{Z} respects the two conditions above. Our representation learning approach explores clinical events as a heterogeneous network, followed by a privacy-preserving network embedding method.

3.2 Heterogeneous Network for Clinical Events

Let $\mathcal{N} = (\mathcal{O}, \mathcal{R}, \mathcal{W})$ be a heterogeneous network where \mathcal{O} is a set of nodes, \mathcal{R} is a set of relations between the nodes and \mathcal{W} represents the weights of the relations. Clinical events are mapped on a heterogeneous network using two types of nodes: (i) patients and (ii) textual excerpts extracted from the EHR, as shown in Figure 1. The patient-type nodes have their respective private vector features \vec{p} . The links indicate when a patient is related to some textual information extracted from the EHR. Moreover, the network topology indicates when two or more patients share the same utility features extracted from the texts.

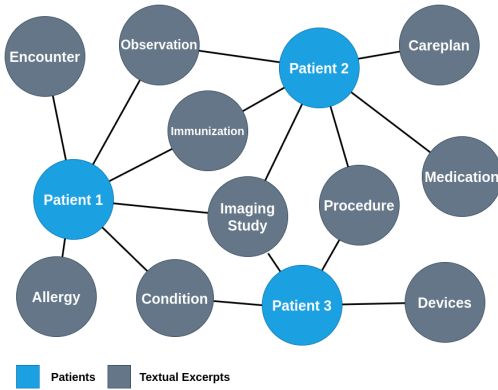


Figure 1. Example of heterogeneous network of clinical events.

To obtain the utility features for patients, we use a regularization framework for graph-based learning. The general idea is to propagate the utility features information to the patient nodes considering the network topology. We extend the regularization framework for heterogeneous networks proposed by Li et al. (2020) to deal with specific characteristics of clinical events, in which two assumptions need to be satisfied: (1) patients who share neighboring nodes must have similar utility features; and (2) textual nodes must

preserve their original utility features.

$$Q(\mathbf{X}) = \frac{1}{2} \sum_{o_i, o_j \in \mathcal{O}} w_{o_i, o_j} (\vec{x}_{o_i} - \vec{x}_{o_j})^2 + \mu \sum_{o_k \in \mathcal{O}_T} (\vec{x}_{o_k} - \vec{u}_{o_k})^2 \quad (1)$$

Equation 1 defines the objective function to be minimized for the utility feature propagation process. The first term of the equation is related to the first assumption, where the utility features \vec{x}_{o_i} and \vec{x}_{o_j} generated for two neighboring nodes o_i and o_j must be similar, for all pairs of nodes with weight $w_{o_i, o_j} > 0$ ($w_{o_i, o_j} \in \mathcal{W}$). The second term is related to the second assumption, in which \mathcal{O}_T indicates the subset of nodes that represent the textual information extracted from the EHR and $(\vec{x}_{o_k} - \vec{u}_{o_k})^2$ indicates that the learned utility features \vec{x}_{o_k} must be similar to the original utility features \vec{u}_{o_k} . The higher the value of the μ parameter ($\mu > 0$), the more the original utility features are preserved. After regularization, \mathbf{X} is a learned utility features matrix for all nodes in the heterogeneous network, including patient-type nodes.

Equation 1 is a convex optimization problem and different solvers can be used for minimization. In this paper, we use the traditional iterative technique based on label propagation proposed in (Zhou & Schölkopf, 2004), since it obtains solutions close to conventional solvers and is suitable for dealing with large heterogeneous networks.

3.3 Privacy-Preserving Heterogeneous Network Embedding

In the previous step, we generated utility features for node patients, but without considering possible inference attacks of the private features. If the feature matrix \mathbf{X} is made publicly available for machine learning tasks, then an attacker who obtains a partial set of private features Y can train a classifier (or regressor) in \mathbf{X} (as input data) and Y (as labels) to infer the other users' private features.

The embeddings learning from the heterogeneous network can be adapted to mitigate the inference attacks of the private features. PHINE employs Graph Convolutional Networks (GCN) to generate an embedding $\mathbf{Z} = \text{GCN}(\mathbf{A}, \mathbf{X})$, where \mathbf{A} is an adjacency matrix derived from the weights of relationships \mathcal{W} between nodes in the heterogeneous network and \mathbf{X} is the utility feature matrix. A GCN has the steps of encoder and decoder. Equation 2 represents the encoder step, where $\mathbf{H}^{(l)}$ is the output of the l -th graph convolutional layer. The input layer is the feature matrix itself, *i.e.*, $\mathbf{H}^{(0)} = \mathbf{X}$. The last layer q represents the embeddings $\mathbf{Z} = \mathbf{H}^{(q)}$. The matrix $\mathbf{L} = \mathbf{D}^{-\frac{1}{2}} \mathbf{S} \mathbf{D}^{-\frac{1}{2}}$ is the symmetrically normalized graph Laplacian. In this case, \mathbf{S} is the adjacency matrix \mathbf{A} with all diagonal elements set to 1 (with self-loops), and $\mathbf{D}_{ii} = \sum_j \mathbf{S}_{ij}$ is a matrix with the degree of node $o_i \in \mathcal{O}$.

Finally, $\mathbf{W}^{(l)}$ denotes the weights of the l -th GCN layer and σ represents the neuron activation function.

$$\mathbf{H}^{(l+1)} = \sigma(\mathbf{LH}^{(l)}\mathbf{W}^{(l)}) \quad (2)$$

The GCN encoder step aims to generate the embeddings \mathbf{Z} that maintain topological properties of the heterogeneous network and preserve utility matrix \mathbf{X} from EHR data, i.e., to reconstruct an approximate adjacency matrix $\hat{\mathbf{A}} = \sigma(\mathbf{ZZ}^T)$ in the GCN decoder step, where \mathbf{Z}^T denotes the transpose of a matrix \mathbf{Z} . Thus, GCN loss function optimizes the link prediction according to Equation 3, where \mathbf{A} is the original adjacency matrix and $\hat{\mathbf{A}}$ is the approximate adjacency matrix through the embeddings.

$$L_{adj} = -\frac{1}{|\mathcal{O}|^2} \sum_{i=1}^{|\mathcal{O}|} \sum_{j=1}^{|\mathcal{O}|} \mathbf{A}_{ij} \log(\hat{\mathbf{A}}_{ij}) \quad (3)$$

Now, we want to extend the GCN decoder step to consider the reconstruction of utility features and private features, in addition to reconstruction via link prediction. In this sense, we adapted the privacy-preserving embedding technique for homogeneous networks proposed by (Li et al., 2020) to deal with heterogeneous networks. Equation 4 defines the inference of labels related to private features y_i^{priv} of the i -th node from the embeddings \mathbf{z}_i , where $\hat{y}_i^{priv} = \text{softmax}(\mathbf{z}_i)$ represents a node o_i classification output by using the embedding \mathbf{z}_i as input and the one-hot generated by private features as labels. An important aspect that we consider during training is that this step is related to patient-type nodes. Thus, we use a trick that generates a fake private label for all nodes that do not belong to the patient type, thereby allowing the model training for heterogeneous networks.

$$L_{attk} = -\frac{1}{|\mathcal{O}|} \sum_{i=1}^{|\mathcal{O}|} y_i^{priv} \log(\hat{y}_i^{priv}) \quad (4)$$

Similarly, Equation 5 defines the inference of labels related to utility features. In this case, we feed the network with the utility features labels that the embeddings must preserve. The classification of a node o_i is given by means of $\hat{y}_i^{util} = \text{softmax}(\mathbf{z}_i^+)$, where \mathbf{z}_i^+ is a concatenation of the embedding \mathbf{z}_i with the privacy labels of node o_i . This strategy allows to extract from the private features the minimum information necessary for the utility prediction. To deal only with patient-type nodes, we use the same trick described previously for heterogeneous networks, where a fake utility label is used to identify when the node belongs to the patient type.

$$L_{util} = -\frac{1}{|\mathcal{O}|} \sum_{i=1}^{|\mathcal{O}|} y_i^{util} \log(\hat{y}_i^{util}) \quad (5)$$

The GCN final loss function is described in Equation 6. Note that while the terms L_{adj} and L_{util} must be minimized during training to reduce the reconstruction error of the links and the utility features prediction, the term L_{attk} receives a negative sign to penalize the loss function when embeddings can infer private features. Thus, during training we want a trade-off between preserving utility features and avoiding inference attacks.

$$Loss = L_{adj} + L_{util} - L_{attk} \quad (6)$$

Different architectures can be used for network embedding. We follow the original architecture proposed by (Li et al., 2020), which uses two convolutional layers combined with a generative adversarial network for the encoder step. Thus, a discriminator is incorporated into the encoder step to classify real nodes or noisy nodes generated from some predetermined distribution. Moreover, the proposed fake label trick to enable privacy-preserving embeddings in heterogeneous networks incorporates structural information into embeddings to determine when a node represents a patient or represents a clinical diagnosis, such as treatment, descriptions, laboratory tests, symptoms and prescriptions.

4 EXPERIMENTAL EVALUATION

4.1 Datasets and Baselines

We used a synthetic EHR generator called Synthea¹ for the experimental evaluation. In the experimental evaluation, patient data about care plans payments (e.g. payers, organizations, and payer_transitions) or that isn't directly related to patients (e.g. supplies and providers) were disregarded during heterogeneous network construction. The network was constructed as described in Section 3.2. Patient nodes have eight attributes: node_type, ethnicity, birth, death, gender, age_category, marital and city. Textual information extracted from medical diagnoses, treatments, symptoms and observations were added as nodes in the heterogeneous network and connected to the respective patients. Network final structure was composed of 1834 nodes and 78055 edges. We compared PHINE to the following baselines:

- **kNN-HN: Utility and private label prediction without privacy-preserving mechanisms.** We apply kNN classifiers directly from the utility features matrix \mathbf{X} derived from the regularization framework, for both utility and private feature predictions. The idea is to make a comparison on how

¹<https://github.com/synthetichealth/>

Table 1. Utility feature (Prediabetes) and Private feature (Gender) evaluation.

	Utility Feature (Prediabetes)		Private Feature (Gender)	
	ACC	F1	ACC	F1
kNN-HN	0.87 ± 0.01	0.83 ± 0.03	0.70 ± 0.03	0.70 ± 0.04
Data Sanitization + GCN	0.87 ± 0.02	0.85 ± 0.02	0.69 ± 0.03	0.68 ± 0.03
PHINE	0.77 ± 0.02	0.72 ± 0.02	0.66 ± 0.02	0.66 ± 0.02
Inferences by class distribution	0.61 ± 0.01	0.50 ± 0.04	0.49 ± 0.02	0.49 ± 0.03

Table 2. Utility feature (Otitis media) and Private feature (Marital) evaluation.

	Utility Feature (Otitis media)		Private Feature (Marital)	
	ACC	F1	ACC	F1
kNN-HN	0.92 ± 0.02	0.80 ± 0.06	0.74 ± 0.01	0.62 ± 0.01
Data Sanitization + GCN	0.92 ± 0.02	0.80 ± 0.04	0.75 ± 0.03	0.59 ± 0.02
PHINE	0.90 ± 0.01	0.73 ± 0.02	0.60 ± 0.03	0.49 ± 0.01
Inferences by class distribution	0.79 ± 0.01	0.50 ± 0.02	0.33 ± 0.02	0.44 ± 0.03

much our privacy-preserving mechanism in heterogeneous networks allows to reduce the inference attacks.

- **Data Sanitization + GCN.** We use a recent strategy for defending inference attacks by perturbing the graph structure, as discussed in (Cai et al., 2018). In our context, we generate different noisy versions of the heterogeneous network using link removal and then network embeddings is obtained via GCN.

- **Inferences by class distribution.** Both utility labels and private labels are predicted in a pseudo-random manner according to the training set’s class distribution.

4.2 Results

We evaluated PHINE by generating a 64-dimensional embedding via privacy-preserving heterogeneous network embedding. The generated embeddings are used as input for a kNN classifier ($k = 3$ and Euclidean distance) to predict utility features and private features. In this case, we use such features as labels during kNN classification. The Data Sanitization + GCN approach also generates 64-dimensional embeddings. The kNN-HN approach does not perform privacy-preserving network embeddings and the evaluation is performed directly on the textual embeddings generated through the regularization framework (Section 3.2). The initial embeddings are generated using Sentence-Transformers DistilBERT² language model.

We defined two experimental evaluation scenarios. In the first, we selected as (binary) label for utility features the occurrence of “Prediabetes”, and the “Gender” was selected as a private feature. In the second, the occurrence of “Otitis media” was selected as a label (binary) for the utility features and the “Marital” status (Married, Single and Others)

was selected as private feature.

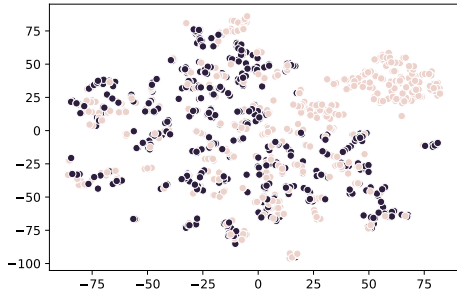
Tables 1 and 2 provide a classification performance overview for each scenario (10-fold Cross-validation). The goal is to maximize the Accuracy (ACC) and F-Measure (F1) metrics for the utility prediction task and minimize these metrics for private features prediction task (which simulates an inference attack).

The kNN-HN approach achieves greater performance for utility prediction in both scenarios. However, kNN-HN demonstrates its inefficiency in mitigating private information inference attacks. The private attributes of Gender and Marital were recovered with 0.70 of ACC in both scenarios, thereby indicating a successful inference attack. Private features Gender and Marital are inferred with 0.49 and 0.33 of ACC using the Inferences By Class Distribution approach.

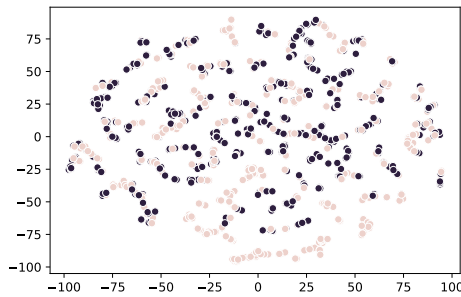
Data Sanitization approach was unsatisfactory in privacy-preserving for heterogeneous networks in medical data. Clinical events have a large number of diagnoses, laboratory tests, symptoms that are highly related to some private features, making it difficult to identify which links should be removed to avoid inference attacks. Even using data sanitization, a small reduction in ACC and F1 metrics was obtained for private feature prediction.

PHINE presented promising results for privacy-preserving, especially for the second scenario. Inference attacks for the private attribute Marital were reduced to values close to Inference by class distribution for the F1 metric. Although with lower performance, some level of privacy-preserving was also achieved in other scenario (Gender) and metrics. Note that the private attribute Gender can be closely associated with the utility prediction task itself. Thus, preserving this information in embeddings can reduce utility prediction. However, PHINE achieves a trade-off between privacy-

²<https://www.sbert.net/>



(a) 2D embeddings projection without PHINE.



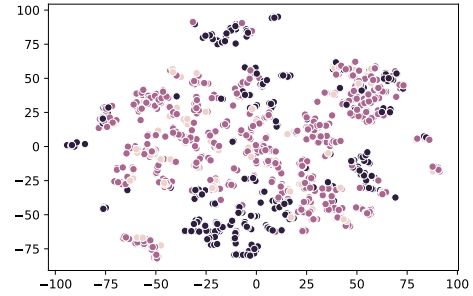
(b) 2D embeddings projection with PHINE.

Figure 2. Two-dimensional embeddings projection. The colors indicate the private Gender feature.

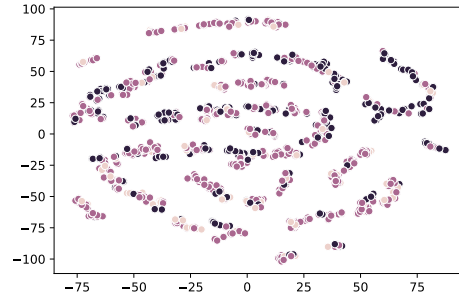
preserving and utility prediction that can be better explored in the future with some strategy to consider the importance level of each feature. To illustrate the effect of PHINE on privacy preservation, Figure 2a shows a two-dimensional projection of patient embeddings extracted directly from the regularization stage (utility features from textual data) and Figure 2b shows a projection after the privacy-preserving step for the Gender feature. The colors indicate the Gender feature. Figures 3a and 3b show this same comparison for the Marital feature.

We observed that embeddings without privacy-preserving (Figures 2a and 3a) have some clustering structures correlated with private features, which explains the good performance of inference attacks. On the other hand, embeddings generated via privacy-preserving (Figures 2b and 3b) hide such structures in relation to private features, without reducing the embedding usefulness for classification tasks.

The experimental results provide evidence that PHINE incorporates privacy preservation during heterogeneous network embedding for clinical events. Moreover, PHINE differs from the Data Sanitization approach because the latter depends on a detailed analysis of the removal of links and some human supervision in real-world scenarios.



(a) 2D embeddings projection without PHINE.



(b) 2D embeddings projection with PHINE.

Figure 3. 2D embeddings projection. The colors indicate the private Marital feature.

5 CONCLUDING REMARKS

PHINE is a novel approach to concealing private information against inference attacks on heterogeneous network embeddings from Electronic Health Records (EHR). PHINE exploits network embeddings (Goyal & Ferrara, 2018) by extending, to heterogeneous networks, the privacy-preserving embedding approach proposed by Li et al. (2020).

Unlike existing approaches that sanitize datasets to remove private information, PHINE uses Graph Autoencoders to (1) maximize the embedding usefulness for classification tasks and (2) to minimize inference attacks of private features. Experimental results show that PHINE obtains a good trade-off between these two objective functions. Directions for future work involve considering different importance levels for each objective function.

ACKNOWLEDGMENT

Oliveira was supported by CAPES (Process Number 88887.500313/2020-00). Marcacini was supported by CNPq (Process Number 426663/2018-7). Pimentel received funding from FAPESP (Process Number 2016/00351-6 and 2016/50489-4), CNPq (Process Number 312058/2015-2).

We thank all the financial agencies for their support.

REFERENCES

- Al-Rubaie, M. and Chang, J. M. Privacy-preserving machine learning: Threats and solutions. *IEEE Security & Privacy*, 17(2):49–58, 2019.
- Cai, Z., He, Z., Guan, X., and Li, Y. Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Transactions on Dependable and Secure Computing*, 15(4):577–590, 2018. doi: 10.1109/TDSC.2016.2613521.
- Cui, P., Wang, X., Pei, J., and Zhu, W. A survey on network embedding. *IEEE Transactions on Knowledge and Data Engineering*, 31(5):833–852, 2019. doi: 10.1109/TKDE.2018.2849727.
- Ellers, M., Cochez, M., Schumacher, T., Strohmaier, M., and Lemmerich, F. Privacy attacks on network embeddings. *CoRR*, abs/1912.10979, 2019.
- Ghassemi, M., Naumann, T., Schulam, P., Beam, A. L., Chen, I. Y., and Ranganath, R. A Review of Challenges and Opportunities in Machine Learning for Health. *AMIA Jt Summits Transl Sci Proc*, 2020:191–200, 2020.
- Goyal, P. and Ferrara, E. Graph embedding techniques, applications, and performance: A survey. *Knowledge-Based Systems*, 151:78–94, 2018. ISSN 0950-7051. doi: <https://doi.org/10.1016/j.knosys.2018.03.022>. URL <https://www.sciencedirect.com/science/article/pii/S0950705118301540>.
- He, Z., Cai, Z., and Yu, J. Latent-data privacy preserving with customized data utility for social network data. *IEEE Transactions on Vehicular Technology*, 67(1):665–673, 2018. doi: 10.1109/TVT.2017.2738018.
- Hosseini, A., Chen, T., Wu, W., Sun, Y., and Sarrafzadeh, M. Heteromed: Heterogeneous information network for medical diagnosis. 04 2018.
- Jia, J. and Gong, N. Z. Attriguard: A practical defense against attribute inference attacks via adversarial machine learning. In Enck, W. and Felt, A. P. (eds.), *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*, pp. 513–529. USENIX Association, 2018. URL <https://www.usenix.org/conference/usenixsecurity18/presentation/jia-jinyuan>.
- Kipf, T. N. and Welling, M. Variational graph auto-encoders. *CoRR*, abs/1611.07308, 2016. URL <http://arxiv.org/abs/1611.07308>.
- Kong, C., Chen, B., Li, S., Chen, Y., Chen, J., Zhou, Q., Wang, D., and Zhang, L. Privacy attack and defense in network embedding. In *International Conference on Computational Data and Social Networks*, pp. 231–242. Springer, 2020.
- Li, K., Luo, G., Ye, Y., Li, W., Ji, S., and Cai, Z. Adversarial privacy preserving graph embedding against inference attack, 2020.
- Shi, C., Li, Y., Zhang, J., Sun, Y., and Yu, P. S. A survey of heterogeneous information network analysis. *IEEE Transactions on Knowledge and Data Engineering*, 29(1):17–37, 2017. doi: 10.1109/TKDE.2016.2598561.
- Shi, C., Hu, B., Zhao, W. X., and Yu, P. S. Heterogeneous information network embedding for recommendation. *IEEE Transactions on Knowledge and Data Engineering*, 31(2):357–370, 2019. doi: 10.1109/TKDE.2018.2833443.
- Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., and Yu, P. S. A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, 32(1):4–24, 2021. doi: 10.1109/TNNLS.2020.2978386.
- Xu, D., Yuan, S., Wu, X., and Phan, H. Dpne: Differentially private network embedding. In Phung, D., Tseng, V. S., Webb, G. I., Ho, B., Ganji, M., and Rashidi, L. (eds.), *Advances in Knowledge Discovery and Data Mining*, pp. 235–246, Cham, 2018. Springer International Publishing.
- Zhang, S. and Ni, W. Graph embedding matrix sharing with differential privacy. *IEEE Access*, 7:89390–89399, 2019. doi: 10.1109/ACCESS.2019.2927365.
- Zhang, Z., Cui, P., and Zhu, W. Deep learning on graphs: A survey. *IEEE Transactions on Knowledge and Data Engineering*, 2020.
- Zhou, D. and Schölkopf, B. A regularization framework for learning from graph data. In *ICML 2004 Workshop on Statistical Relational Learning and Its Connections to Other Fields (SRL 2004)*, pp. 132–137, 2004.
- Zhou, S., Bu, J., Wang, X., Chen, J., Hu, B., Chen, D., and Wang, C. Hahe: Hierarchical attentive heterogeneous information network embedding. 01 2019.