Journal of Information Hiding and Privacy Protection

Tech Science Press

DOI: 10.32604/jihpp.2022.039284
Review

A Survey of Privacy Preservation for Deep Learning Applications

Ling Zhang[1,*], Lina Nie[1] and Leyan Yu[2]

[1]School of Computer Science, Nanjing University of Information Science & Technology, Nanjing, 210044, China
[2]Reading Academy, Nanjing University of Information Science & Technology, Nanjing, 210044, China
*Corresponding Author: Ling Zhang. Email: jocobzling@163.com
Received: 20 January 2023; Accepted: 06 March 2023

Abstract: Deep learning is widely used in artificial intelligence fields such as computer vision, natural language recognition, and intelligent robots. With the development of deep learning, people's expectations for this technology are increasing daily. Enterprises and individuals usually need a lot of computing power to support the practical work of deep learning technology. Many cloud service providers provide and deploy cloud computing environments. However, there are severe risks of privacy leakage when transferring data to cloud service providers and using data for model training, which makes users unable to use deep learning technology in cloud computing environments confidently. This paper mainly reviews the privacy leakage problems that exist when using deep learning, then introduces deep learning algorithms that support privacy protection, compares and looks forward to these algorithms, and summarizes this aspect's development.

Keywords: Deep learning; homomorphic encryption; differential privacy; multi-party secure computing; privacy protection

1 Introduction

In recent years, with the continuous development of computer technology and the rise of artificial intelligence, deep learning has achieved remarkable achievements in various applications such as image classification [1], face recognition [2], and anomaly detection [3]. Performance improvement largely depends on massive training data, high-performance computing resources, and a well-designed model structure [4]. In the context of enormous computing volumes and computing resource requirements, we often use cloud computing resources for deep learning. Cloud computing has dramatically affected our lives as a new way of computing and data processing. By aggregating virtualized and interconnected computers and other information technology infrastructures, cloud computing provides users with on-demand and extensive network access, resource pooling, and high-quality Internet services featuring rapid elasticity and measurable services. More specifically, for individuals, cloud computing lowers the threshold for accessing computing resources, removes barriers caused by infrastructure, and makes it possible for individuals to implement complex tasks such as deep learning. For groups and companies,

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cloud computing provides greater flexibility in resource allocation, allowing them to focus more on their deep learning business.

The need for deep learning to leverage and use cloud computing resources naturally raises privacy concerns. Cloud computing providers will package and deploy their deep learning application services and directly provide users to rent. Cloud providers can quickly access critical unauthorized knowledge, such as private input data, and the classification results are modeled without proper security mechanisms. Due to privacy issues, customers may be unwilling or unable to provide data to service providers, such as assisting in medical diagnosis [5] and financial data fraud detection [6]. Data privacy requirements limit the safe delivery of deep learning application services in the cloud environment [7]. Therefore, to ensure the safe landing of deep learning application services in the cloud environment and the private security and interests of participants in the service process, it is necessary and valuable to study the corresponding privacy protection framework for related privacy issues.

2 Privacy Preserving Cryptography Technology

This section discusses cryptographic techniques applied to deep learning privacy protection, including homomorphic encryption, differential privacy, image encryption, and secure multi-party computation.

2.1 Homomorphic Encryption

Homomorphic encryption technology provides a solution to the privacy protection problem in the neural network model. Homomorphic encryption includes partial homomorphic encryption and fully homomorphic encryption. Ciphertext operations that only support a limited number of additions or multiplications are called addition or multiplication homomorphisms; if any number of addition and multiplication ciphertext operations can be performed, it is fully homomorphic encryption. The classic RSA encryption algorithm [8] and Elgamal encryption algorithm [9] have multiplicative homomorphism. In 1999, Paillier proposed a Paillier encryption scheme that satisfies additive homomorphism [10]. In 2009, Gentry proposed the first fully homomorphic encryption scheme based on ideal lattice [11].

HE supports operations in ciphertext, and the result of decryption is the same as that obtained in plaintext, that is: $Encryption(f(m_1, m_2)) = f(Encryption(m_1), Encryption(m_2))$. The homomorphic encryption scheme, like other types of encryption schemes, has the following three functional modules:

The key generation algorithm $Keygen(\lambda)$: The key generation algorithm generates and calculates the key k according to the input parameter λ, and outputs the public key pk and private key sk.

The encryption algorithm $Encryption(pk, m)$: The encryption algorithm uses the public key pk to encrypt the plaintext information m, and outputs the encrypted information s.

Decryption algorithm $Decryption(sk, s)$: Decryption algorithm uses the private key sk to decrypt the ciphertext s, and output the plaintext m.

The ciphertext homomorphic operation also includes homomorphic addition and homomorphic multiplication. The homomorphic addition operation $Decryption(k, Add(s_1, s_2)) = m_1+m_2$, s_1 and s_2 respectively correspond to m_1 under the ciphertext and m_2, the sum of the ciphertext information calculated according to the calculation key k is the corresponding ciphertext of m_1+m_2; the homomorphic multiplication operation $Decryption(k, Mul(s_1, s_2)) = m_1 \times m_2$, s_1 and s_2 corresponds to m_1 and m_2 under the ciphertext, and the product of the ciphertext information calculated according to the calculation key k is the corresponding ciphertext of $m_1 \times m_2$.

2.2 Differential Privacy

The Initial letter of each notional word in all headings is capitalized. Differential privacy [12] was originally proposed to protect databases from differential attacks. The so-called differential attack is that the attacker can distinguish whether a certain data exists in the database according to the different query results by accessing the database multiple times. The basic idea of differential privacy is to make it impossible for attackers to distinguish the changes of data in the database by adding noise, that is, the change of any piece of data in the database will not have a great impact on the overall output, so as to protect the privacy of database data. effect. As shown in the formula (1):

$$P_r[M(D_1) \in S] \leq e^{\varepsilon} \times P_r[M(D_2) \in S] + \delta\,(1) \tag{1}$$

where, D_1 and D_2 are databases with a difference of 1 record respectively, and ε is the privacy protection cost, which reflects the level of privacy protection. The smaller ε is, the higher the level of privacy protection is, and the deeper the useful information about the data set is mapped. But under the same circumstances, the smaller ε is, the lower the data availability will be. The probability that the output result of the random algorithm M is a subset of S satisfies formula (1) and satisfies differential privacy.

2.3 Image Encryption

There are many differences between digital images and traditional text data. Image encryption technology is a technology that uses the characteristics of time, space, and visual perception of images to design encryption algorithms to improve image security. Image encryption refers to the process of changing a plaintext image into a ciphertext image under the constraints of an encryption function and a key. The entire encryption, decryption and transmission process can be described as follows: the plaintext image becomes a ciphertext image after being encrypted, and the sender of the message transmits the ciphertext image to the receiver on an insecure channel, and the receiver uses the decryption key to convert the ciphertext image to the recipient. It is decrypted into a plaintext image, and the key required for encryption and decryption is transmitted on a secure channel.

Chaos has the characteristics of pseudo-randomness and sensitivity to initial conditions, which is consistent with the encryption requirements of images, and the principle of chaos is of great help to digital image encryption. Many scholars have combined chaos technology with encryption technology. Therefore, chaos Technology is widely used in image encryption, and it is also very important in using image encryption technology to protect deep learning privacy. There are three common chaotic encryption methods, namely image encryption based on grayscale replacement, image encryption based on pixel scrambling, and iterative image encryption.

2.4 Multi-Party Secure Computing

Secure Multi-Party Computation [13] mainly studies how a group of distrusting parties can jointly complete a certain calculation while protecting the privacy of their respective input data, and ensure the correctness of the output results. Secure multi-party computing is mainly used in two deep learning privacy protection scenarios, namely the prediction phase and the training phase. In the prediction stage, the data owner is the client, the cloud server has a well-trained deep learning model, and the cloud server provides inference services based on the client's private data. In the training stage, multiple users securely outsource some of their data and jointly communicate with cloud servers to obtain a trained model. The trained models are considered invisible to both personal data owners and cloud servers.

Deep learning privacy protection based on secure multi-party computing has attracted a large number of researchers to study, mainly using the following privacy protection tools, garbled circuit

[14] and secret sharing [15]. The garbled circuit technology was proposed by Yao's, which provides a general strategy for two-party security calculations. The purpose is to minimize the non-exclusive OR gates in the constructed Boolean circuit. The idea of the secret sharing scheme is to split the secret in an appropriate way. Each share after splitting is managed by different participants. A single participant cannot recover the secret information, and only several participants can cooperate to recover the secret information. More importantly, when any of the participants in the corresponding range fails, the secret can still be fully restored. Currently, there are three main types of secret sharing, namely GMW protocol [16] Shamir sharing [17] and arithmetic sharing.

3 Privacy Preservation for Deep Learning Applications

This section mainly discusses deep learning applications based on the cryptography technology introduced in Section 2, including deep learning algorithms that support privacy protection based on homomorphic encryption, differential privacy, image encryption, and secure multi-party computing.

3.1 Deep Learning Privacy Protection Algorithms Based on Homomorphic Encryption

The emergence of homomorphic encryption technology provides a way to solve the privacy problem of deep learning, which can realize the operation under the ciphertext without affecting the correct result of decryption. Using homomorphic encryption technology to protect the privacy of deep learning applications, we can directly predict the encrypted data in the prediction stage. The prediction results are ciphertexts and return the results to the user for decryption to protect user data privacy. We can also directly participate in training to protect the security of the training data uploaded by users.

In 2006, Barni et al. [18] proposed a privacy-preserving neural network classification scheme based on secure multi-party computation and homomorphic encryption. Their neural network consists of a series of scalar products, and the client uses a homomorphic encryption algorithm to encrypt the input vector. Subsequently, Orlandi et al. [19] strengthened the protocol, replacing the Paillier encryption mechanism with an extension of Damgard-Jurik, while intermediate results are no longer displayed to the client. In 2016, Microsoft's Gilad-Bachrach et al. [20] proposed the CryptoNets solution, which applied the fully homomorphic encryption scheme to the convolutional neural network, predicted the use of a simplified neural network, and replaced the ReLU with a square function with a lower multiplication depth. However, it is only suitable for small neural networks and has become a milestone in applying homomorphic encryption in deep neural networks. In 2017, Chabanne et al. [21] replaced the activation function with a polynomial function in the prediction stage. They added a batch normalization layer before each nonlinear activation layer, which can form input with a stable distribution and improve the prediction accuracy. Chillotti et al. [22] proposed the FHE-DiNN solution and designed a new type of discrete neural network.

Although the above methods can be applied to deep networks, there are still problems of low accuracy and high complexity of ciphertext calculations. In order to improve the accuracy of the homomorphic encryption scheme and the efficiency of ciphertext operations, the paper [23] proposed the MiniONN scheme. However, this solution relies on the communication between the server and the client, leading to data holders' need to participate frequently in calculations. The GAZELLE scheme was designed by Juvekar et al. [24]. Instead of fully applying fully homomorphic encryption, they alternate an additively homomorphic encryption scheme for convolutional layers with garbled circuits for activation layers. Compared with MiniONN, this scheme has reduced communication complexity but still has a significant communication overhead. In 2020, Al Badawi et al. [25] followed the framework of CryptoNets and proposed the first Graphics Processing Unit accelerated

homomorphic convolutional neural network, which increased the prediction time by 40.41 times. In 2021, Reagen et al. [26] of New York University provided a set of algorithms and hardware optimization solution frameworks for the homomorphic deep neural network on the server side, which is used to improve the ciphertext prediction speed of the neural network. In 2022, Jang et al. [27] proposed a variant scheme based on the homomorphic encryption algorithm called MatHEAAN (Matrix HEEAN), which specializes in matrix operations. The scheme implements Gated Recurrent Units to process sequential data.

3.2 Deep Learning Privacy Protection Algorithms Based on Differential Privacy

Differential privacy algorithm, which has strict mathematical proof, is one of the more popular privacy protection technologies. The basic idea of the differential privacy algorithm is to limit the sensitivity of the database query results to any piece of data to ensure that any piece of data in the data set or not in the data set has little impact on the final query output [28]. Some companies have also begun to use differential privacy technology. For example, Apple Vice President Craig Federighi announced that Apple uses local differential privacy technology to protect iOS/macOS user privacy [29].

The combination of differential privacy algorithms and deep learning has been one of the research hotspots in the field of deep learning privacy protection in recent years. This algorithm can be applied to various parts of the deep learning model. The differential privacy protection scheme of the input layer [30] can be regarded as a preprocessing operation on the data, which generates synthetic data with the same statistical characteristics as the original data by adding noise to the training data set and then uses the synthetic data for training of deep learning models. The differential privacy protection scheme of the output layer [31] is to perturb the objective function to achieve privacy protection. Some studies also propose adding noise to the polynomial expansion coefficient of the objective function. This approach has been implemented on autoencoders [32], deep belief networks [33], and deep neural networks.

Compared with the above two differential privacy protection schemes, the differential privacy protection scheme that adds noise to the training parameters in the hidden layer is more widely used. Abadi et al. [12] proposed the Differential Privacy Stochastic Gradient Descent (DPSGD) algorithm in 2016 to protect the privacy of training data most understandably and intuitively. In recent years, many improved methods have been proposed to balance the relationship between privacy and the accuracy of the differential privacy model, which is of great significance to optimizing the privacy protection model. In 2018, Lee et al. [34] proposed allocating different privacy budgets for each training iteration and ensuring that the noise on each gradient component follows the same probability distribution, making the noise added in each step more refined. In 2019, Xiang et al. [35] solved the trade-off between privacy and accuracy from an optimization perspective and improved the overall accuracy of the model while satisfying privacy constraints. Xu et al. [36] proposed replacing the simple gradient threshold pruning in the DPSGD algorithm with hierarchical gradient pruning, and the added noise depends on the size of the gradient pruning threshold. This method reduces the addition of noise to a certain extent and has a specific effect on the privacy and accuracy of the trade-off model. In 2020, Bu et al. [37] proposed to improve the privacy loss calculation mechanism of differential privacy, allowing more iterations of the model under the same privacy level, thereby improving the accuracy of training neural networks using differential privacy optimization algorithms. Lin et al. [38] proposed to adjust the order of adding noise and gradient pruning operations in the DPSGD algorithm, first adding noise and then performing gradient pruning, and then performing more accurate pruning on

the gradient after adding noise. Compared with the original algorithm, the accuracy of this algorithm has been improved to a certain extent.

3.3 Deep Learning Privacy Preservation Algorithms Based on Image Encryption

In 2018, AprilPyone et al. [39] proposed the concept of learnable encryption, the first to propose a learnable image encryption algorithm based on block scrambling, which is used in the privacy protection of deep learning. The image processing operation is as follows. First, the 8-bit RGB image is divided into $M \times M$ size blocks. Then each block is divided into upper 4-bit and lower 4-bit images to obtain a 6-channel image block, randomly select the pixel value to invert, and then shuffle all the pixel values. Subsequently, the team proposed an improvement to the algorithm in [40] and proposed a block image scrambling processing pipeline. Firstly, the image is divided into blocks by $B \times B$ pixels. The blocks' positions are shuffled, then the pixels in each block are shuffled independently, and finally, the shuffled blocks are connected. Sirichotedumrong et al. [41] proposed an image encryption algorithm based on pixel scrambling. The encryption method is to take a picture of $X \times Y$ pixels, use the key $K\mathrm{c} = \{K_\mathrm{R}, K_\mathrm{G}, K_\mathrm{B}\}$, K_C is a generated random binary integer, and then perform positive and negative transformations on each pixel value of the private image. Based on the image encryption proposed in [41], the team followed up the encryption algorithm by considering using independent encryption keys for training and testing images for the first time. It is proposed to use a set of key_1 to encrypt training pictures and another set of key_2, entirely different from key_1, to encrypt test images [42]. Ko et al. [43] used a structured image de-identification method for deep learning privacy preservation. Sequence-preserving encryption only modifies the original structure of the image, which not only achieves the purpose of protecting privacy during model training but also improves the training accuracy of the model.

3.4 Deep Learning Privacy Protection Algorithms Based on Multi-Party Secure Computing

The deep learning privacy protection algorithm based on secure multi-party computing has attracted many researchers to study. Schemes based on secure multi-party computation usually involve multiple parties, such as an additional trusted party or multiple non-colluding cloud servers, and a more significant number of interactions. In 2017, Mohassel et al. [44] proposed the SecureML method, where data owners use secure two-party computing to distribute their private data between two non-merged servers, effectively protecting the privacy of the training phase in a two-server model. In 2018, Mohassel et al. [45] proposed the ABY3 method, which enables data owners to share sensitive data in a three-party server model while providing privacy guarantees during the model training phase.

Secret sharing is a commonly used privacy protection method in secure multi-party computing. Compared with other privacy protection methods in production applications, it can reduce overhead and improve efficiency. Ma et al. [46] proposed a lightweight privacy-preserving face recognition classification framework based on additive secret sharing design, which improved the existing exponentiation function based on additive secret sharing by expanding the effective input range and logarithmic functions. Based on the work of Ma et al. [46], Liu et al. [47] proposed SecRCNN, which is the first efficient R-CNN framework for privacy protection of object detection in medical images, using the CORDIC algorithm to design a new division, Exponentiation and logarithm protocols. Liu et al. [48] used distributed double trapdoor public key cryptosystem and additive secret sharing to construct a decision tree method and designed three methods with different privacy levels. In [49], Feng et al. designed a series of multi-party interaction protocols with nonlinear activation functions through multiplicative and additive secret sharing. They constructed a simple and efficient multi-party privacy-preserving natural language processing security application. In recent years, Xia et al. [50]

inspired by additive secret sharing and multiplicative secret sharing, proposed a secure computing protocol based on the "share-transform-reveal" strategy and constructed a secure computing protocol for all essential elementary functions. This scheme illustrates its superiority by using a convolutional neural network as an example.

4 Comparison and Prospects

With the development of deep learning, more and more people have paid attention to the importance of privacy in deep learning. Some existing privacy protection schemes still have some limitations.

Homomorphic Encryption: The emergence of homomorphic encryption provides a solution to privacy computing. Nevertheless, the application of homomorphic encryption faces the following challenges: Only addition and multiplication homomorphism operations are supported in ciphertext, but complex nonlinear operations such as comparison, maximum calculation, and division operation are involved in the practice. Under the neural network model, homomorphic encryption is more challenging because the neural network structure includes many nonlinear activation functions such as Sigmoid, ReLU, etc., which cannot directly perform homomorphic operations, requiring researchers to constantly design elaborate protocols. Homomorphic encryption has large space consumption and computing overhead, leading to the bottleneck of privacy protection algorithm applications.

Differential Privacy: The combination of differential privacy and deep learning can effectively solve the privacy leakage problem of model training data. However, privacy protection employing noise brings new challenges to the deep learning model: the trade-off between model privacy and model accuracy. Therefore, when combining differential privacy and deep learning, the selection of training algorithm, gradient pruning method, model structure, and initialization method should be considered. At the same time, it is necessary to consider the privacy protection characteristics of the differential privacy algorithm and noise to better balance the privacy and accuracy of the model.

Image Encryption: Using the encrypted picture for network training trains the encrypted data, during which there is no need to decrypt, but this method still has certain limitations. First, there are some hidden dangers in the security performance of this method. The ability to resist differential and statistical attacks is weak and does not apply to the scene using the gray image. Secondly, there is also the problem of model training and detection accuracy loss. Last, this method only applies to image-related tasks and has limitations when applied to more complex deep-learning tasks.

Multi-Party Secure Computing: Secure multi-party computing is a crucial technology to achieve deep learning privacy computing, which can maintain the accuracy of the deep learning model to a large extent, but there are still the following limitations. In a multi-server environment, it is not very easy to lossless construct efficient nonlinear operations suitable for deep learning models. When multiple servers participate in the computation, the security of the model is more complex than that of other solutions. In secure multi-party computing, many interaction operations on edge servers are often required, which are costly. In short, how to efficiently, safely, and lossless secure multi-party computing technology is still a big challenge in deep learning in the future.

5 Conclusion

This paper sorts out based on the introduction of standard privacy protection methods. It summarizes the existing deep learning algorithms based on homomorphic encryption, differential privacy, image encryption, and multi-party security computing. The limitations of existing privacy

protection methods in deep learning applications are summarized systematically. In the future, as people pay more attention to privacy issues, deep learning applications supporting privacy protection will continue to evolve and improve.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Sellami and S. Tabbone, "Deep neural networks-based relevant latent representation learning for hyperspectral image classification," *Pattern Recognition*, vol. 121, no. 1, pp. 108224, 2022.
[2] A. J. A. AlBdairi, Z. Xiao, A. Alkhayyat, A. J. Humaidi, M. A. Fadhel *et al.,* "Face recognition based on deep learning and FPGA for ethnicity identification," *Applied Sciences*, vol. 12, no. 5, pp. 2605, 2022.
[3] C. Wu, S. Shao, C. Tunc, P. Satam and S. Hariri, "An explainable and efficient deep learning framework for video anomaly detection," *Cluster Computing*, vol. 25, no. 4, pp. 2715–2737, 2022.
[4] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *Int. Conf. on Machine Learning*, California, USA, vol. 97, pp. 6105–6114, 2019.
[5] M. Ahmad, S. F. Qadri, S. Qadri, I. A. Saeed, S. S. Zareen *et al.,* "A lightweight convolutional neural network model for liver segmentation in medical diagnosis," *Computational Intelligence and Neuroscience*, vol. 2022, no. 16, pp. 16, 2022.
[6] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022.
[7] H. Lee, D. Kang, Y. Lee and D. Won, "Secure three-factor anonymous user authentication scheme for cloud computing environment," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1871, pp. 1–20, 2021.
[8] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[10] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Germany, pp. 223–238, 1999.
[11] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. of the Forty-First Annual ACM Symp. on Theory of Computing*, Bethesda, MD, USA, pp. 169–178, 2009.
[12] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov *et al.,* "Deep learning with differential privacy," in *Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security*, Vienna, Austria, pp. 308–318, 2016.
[13] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in *Proc. of the 2001 Workshop on New Security Paradigms*, Cloudcroft, New Mexico, pp. 13–22, 2001.
[14] A. C. Yao, "Protocols for secure computations," in *23rd Annual Symp. on Foundations of Computer Science (sfcs 1982)*, Chicago, IL, USA, pp. 160–164, 1982.
[15] A. Beimel, "Secret-sharing schemes: A survey," in *Int. Conf. on Coding and Cryptology*, Berlin, Germany, pp. 11–46, 2011.
[16] S. Micali, O. Goldreich and A. Wigderson, "How to play any mental game," in *Proc. of the Nineteenth ACM Symp. on Theory of Computing, STOC*, New York, NY, USA, pp. 218–229, 1987.
[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[18] M. Barni, C. Orlandi and A. Piva, "A privacy-preserving protocol for neural-network-based computation," in *Proc. of the 8th Workshop on Multimedia and Security*, Geneva, Switzerland, pp. 146–151, 2006.

[19] C. Orlandi, A. Piva and M. Barni, "Oblivious neural network computing via homomorphic encryption," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–11, 2007.
[20] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig *et al.,* "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," in *Int. Conf. on Machine Learning*, New York, USA, pp. 201–210, 2016.
[21] H. Chabanne, A. De Wargny, J. Milgram, C. Morel and E. Prouff, "Privacy-preserving classification on deep neural network," *Cryptology ePrint Archive*, vol. 35, pp. 1–18, 2017.
[22] I. Chillotti, N. Gama, M. Georgieva and M. Izabachene, "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds," in *Int. Conf. on the Theory and Application of Cryptology and Information Security*, Berlin, Germany, pp. 3–33, 2016.
[23] J. Liu, M. Juuti, Y. Lu and N. Asokan, "Oblivious neural network predictions via minionn transformations," in *Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security*, Dallas, Texas, USA, pp. 619–631, 2017.
[24] C. Juvekar, V. Vaikuntanathan and A. Chandrakasan, "{GAZELLE}: A low latency framework for secure neural network inference," in *27th USENIX Security Symp. (USENIX Security 18)*, Baltimore, MD, USA, pp. 1651–1669, 2018.
[25] A. Al Badawi, C. Jin, J. Lin, C. F. Mun, S. J. Jie *et al.,* "Towards the alexnet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1330–1343, 2020.
[26] B. Reagen, W. -S. Choi, Y. Ko, V. T. Lee, H. -H. S. Lee *et al.,* "Cheetah: Optimizing and accelerating homomorphic encryption for private inference," in *2021 IEEE Int. Symp. on High-Performance Computer Architecture (HPCA)*, Seoul, Korea (South), pp. 26–39, 2021.
[27] J. Jang, Y. Lee, A. Kim, B. Na, D. Yhee *et al.,* "Privacy-preserving deep sequential model with matrix homomorphic encryption," in *Proc. of the 2022 ACM on Asia Conf. on Computer and Communications Security*, Nagasaki, Japan, pp. 377–391, 2022.
[28] C. Dwork, "Differential privacy: A survey of results," in *Int. Conf. on Theory and Applications of Models of Computation*, Berlin, Germany, pp. 1–19, 2008.
[29] Ú. Erlingsson, V. Pihur and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security*, Scottsdale, Arizona, USA, pp. 1054–1067, 2014.
[30] B. K. Beaulieu-Jones, Z. S. Wu, C. Williams, R. Lee, S. P. Bhavnani *et al.,* "Privacy-preserving generative deep neural networks support clinical data sharing," *Circulation: Cardiovascular Quality and Outcomes*, vol. 12, no. 7, pp. e005122, 2019.
[31] N. Phan, Y. Wang, X. Wu and D. Dou, "Differential privacy preservation for deep auto-encoders: An application of human behavior prediction," in *Thirtieth AAAI Conf. on Artificial Intelligence*, Phoenix, Arizona, USA, 2016.
[32] R. Lopez, J. Regier, M. I. Jordan and N. Yosef, "Information constraints on auto-encoding variational bayes," *Advances in Neural Information Processing Systems*, vol. 31, pp. 6117–6128, 2018.
[33] G. E. Hinton, S. Osindero and Y. -W. Teh, "A fast learning algorithm for deep belief nets," *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, 2006.
[34] J. Lee and D. Kifer, "Concentrated differentially private gradient descent with adaptive per-iteration privacy budget," in *Proc. of the 24th ACM SIGKDD Int. Conf. on Knowledge Discovery & Data Mining*, London, United Kingdom, pp. 1656–1665, 2018.
[35] L. Xiang, J. Yang and B. Li, "Differentially-private deep learning from an optimization perspective," in *IEEE INFOCOM 2019-IEEE Conf. on Computer Communications*, Paris, France, pp. 559–567, 2019.
[36] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin *et al.,* "GANobfuscator: Mitigating information leakage under GAN via differential privacy," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2358–2371, 2019.
[37] Z. Bu, J. Dong, Q. Long and W. J. Su, "Deep learning with gaussian differential privacy," *Harvard Data Science Review*, vol. 2020, no. 23, pp. 10–1162, 2020.

[38] Y. Lin, L. -Y. Bao, Z. -M. Li, S. -Z. Si and C. -H. Chu, "Differential privacy protection over deep learning: An investigation of its impacted factors," *Computers & Security*, vol. 99, no. 6, pp. 102061, 2020.
[39] M. AprilPyone, W. Sirichotedumrong and H. Kiya, "Adversarial test on learnable image encryption," in *2019 IEEE 8th Global Conf. on Consumer Electronics (GCCE)*, Osaka, Japan, pp. 667–669, 2019.
[40] K. Madono, M. Tanaka, M. Onishi and T. Ogawa, "Block-wise scrambled image recognition using adaptation network," arXiv preprint arXiv:2001.07761, 2020.
[41] W. Sirichotedumrong, Y. Kinoshita and H. Kiya, "Pixel-based image encryption without key management for privacy-preserving deep neural networks," *IEEE Access*, vol. 7, pp. 177844–177855, 2019.
[42] W. Sirichotedumrong, Y. Kinoshita and H. Kiya, "Privacy-preserving deep neural networks using pixel-based image encryption without common security keys," in *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conf. (APSIPA ASC)*, Lanzhou, China, pp. 1756–1761, 2019.
[43] D. -H. Ko, S. -H. Choi, J. -M. Shin, P. Liu and Y. -H. Choi, "Structural image de-identification for privacy-preserving deep learning," *IEEE Access*, vol. 8, pp. 119848–119862, 2020.
[44] P. Mohassel and Y. Zhang, "SecureML: A system for scalable privacy-preserving machine learning," in *2017 IEEE Symp. on Security and Privacy (SP)*, San Jose, CA, USA, pp. 19–38, 2017.
[45] P. Mohassel and P. Rindal, "ABY3: A mixed protocol framework for machine learning," in *Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security*, Toronto, Canada, pp. 35–52, 2018.
[46] Z. Ma, Y. Liu, X. Liu, J. Ma and K. Ren, "Lightweight privacy-preserving ensemble classification for face recognition," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5778–5790, 2019.
[47] Y. Liu, Z. Ma, X. Liu, S. Ma and K. Ren, "Privacy-preserving object detection for medical images with faster R-CNN," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 69–84, 2019.
[48] L. Liu, R. Chen, X. Liu, J. Su and L. Qiao, "Towards practical privacy-preserving decision tree training and evaluation in the cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2914–2929, 2020.
[49] Q. Feng, D. He, Z. Liu, H. Wang and K. -K. R. Choo, "SecureNLP: A system for multi-party privacy-preserving natural language processing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3709–3721, 2020.
[50] Z. Xia, Q. Gu, W. Zhou, L. Xiong, J. Weng *et al.,* "STR: Secure computation on additive shares using the share-transform-reveal strategy," *IEEE Transactions on Computers*, vol. 1, pp. 1–14, 2021. https://doi.org/10.1109/TC.2021.3073171