A Novel scheme of Image Encryption and Machine Learning-Training the Network with Encrypted images

T. Naga Lakshmi
Lecturer,
Department of Computer Science
SWR Govt. Degree College, Kanchikacherla
Email: lakshmi.nag04@gmail.com

S. Jyothi
Professor,
Department of Computer Science
SPMVV, Tirupathi
jyothi.spmvv@gmail.com

Article Info
Page Number: 1490 - 1495
Publication Issue:
Vol 71 No. 4 (2022)

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Abstract

Image Encryption plays major role to handle privacy issues in the network. For the researchers it is difficult to train the encrypted images because of privacy issues. However in some applications the researchers need to collect the image datain order to train the network using machine learning algorithm. This difficulty can be achieved by using the proposed algorithm. A novel scheme of image encryption and machine learning algorithm is used to train the network with encrypted images. The idea behind the proposed algorithm is to encrypt the images in order to secure the image from humans but not for the network to train the data. Here the network is trained directly with the encrypted images without decrypting them. The proposed algorithm can be applied in Deep learning surveillance applications. With the help of this algorithm, any kind of network can train the data.

Keywords: Image Encryption, Machine Learning, Deep Learning

1. Introduction

In computer vision applications[1], Machine Learning and Deep learning are very powerful tools that are used. The most important application field in Deep Learning is close observation or surveillance on data set. To obtain best performance huge training data set is required. But in surveillance application, it is difficult to collect the large training data sets by keeping the privacy of one's data. Developers can directly identify one's behaviour if their photos are included into datasets. Image encryption is one of the important techniques to maintain privacy. The process of converting original image in to encrypted image where people cannot recognize the original contents of the image is called image encryption. Different image encryption algorithms have been

developed to transmit the images securely over the public network[2]. Different types of cryptographic algorithms and issues are discussed by T.Naga Lakshmi and S. Jyothi in "Cryptography Algorithms- Issues on Recent trends" [3].If any people or machine wants to recognize the contents of the encrypted imaged, it must be decrypted first then only they can access the image. If they are accessing the image means, there is no privacy for the image.

In this paper, a novel approach has been introduced to train the network using encrypted images. It is a combination of image encryption and machine learning application where to preserve the privacy of image contents.Here the network will directly be learnt by the encrypted images without performing any decryption. the proposed scheme is demonstrated using cifar datasets. The basic idea in this proposed scheme is to encrypt the images only for the humans but not for machines.

2. Problem Definition

Let us consider two scenarios i.e., operating phase and training phase. The network requires plain image dataset for both scenarios. The network is trained using plain images as shown in Fig.1.the original plain images are decrypted to train the network even though the image dataset is encrypted. Trainer is the person who trains the network and different from the person who holds the data. The data holder cannot provide the datasets to the trainer because the plain image datasets violates the data holder privacy policy. They cannot provide the image datasets to the trainer with the two existing schemes.

In another scenario, operating phase is same as training phase. The operator is the person who performs detection and classification in operating phase. It is required for the network to detect the plain images and to classify them. The images should be decrypted even the encrypted images are available in surveillance system. The operator in the surveillance system in the network checks the original plain images. In both cases the operator and trainer violate the privacy policy. To overcome this problem a novel scheme of encryption is introduced.

The major difference between existing image encryption and to the novel approach is the images are encrypted against humans and network whereas in the novel approach images are encrypted for humans and the network is trained with the encoded images. We call this image encryption as a novel scheme of image encryption and machine learning. It encrypts the images for human that means the dataset can be provided without any privacy issues. The encrypted images can be trained directly by the trainers. The data holder and trainer can avoid privacy issues and very helpful to develop the networks to train. The network is trained directly with the encrypted images and detects or classify the objects without decrypting the plain images.

3. A Novel scheme of image encryption and machine Learning- Proposed Algorithm

A new algorithm is proposed for image encryption and to be trained by encrypted images is block wise shuffling pixels algorithm. The network is trained with plain images as shown in Fig. 1. In this method the plain images are trained by the network directly and the privacy issue is very

poor. The networks are trained with existing image encryption is as shown in Fig 2. Firstly, the images are encrypted and decrypted and then the images are trained in the network and the privacy is less because the plain images only trained. As shown in Fig 3. the network is trained with novel scheme of image encryption. In this approach the network is trained directly with the encrypted images with out decrypting. The procedure of the proposed algorithm for RGB image with 8-bit can be discussed as follows:

1. Consider 8-bit RGB image and divide them in NxN sized blocks.
2. Every block is divided into 4-bit upper and 4-bit lower images. Then we have 6 channel image blocks.
3. Some of the pixels are randomly chosen and the intensities are reversed
4. Random pixel shuffling is applied for every image.
5. It produces the encrypted image which cannot be understand by the humans.
   The network structure should adjust to the proposed novel scheme image encryption and machine learning. The adaptation in neural network can be done very easily[4]

Fig 1. Network Training with plain images

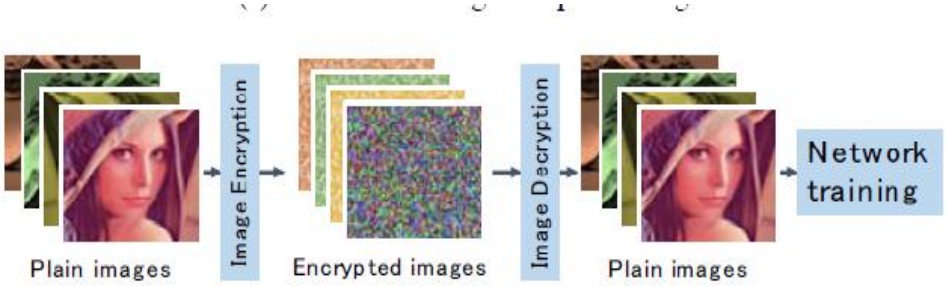


Fig 2. Network training with existing image encryption

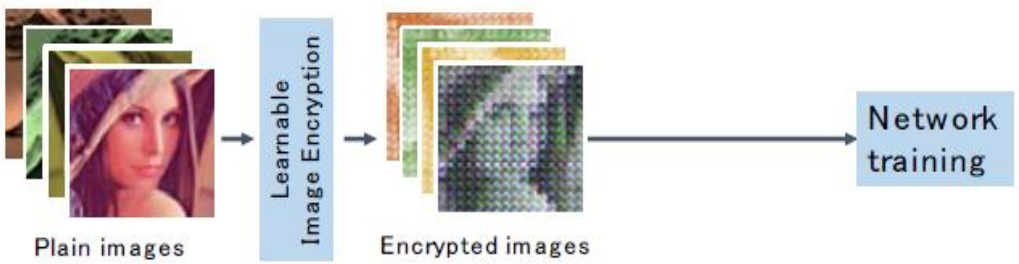


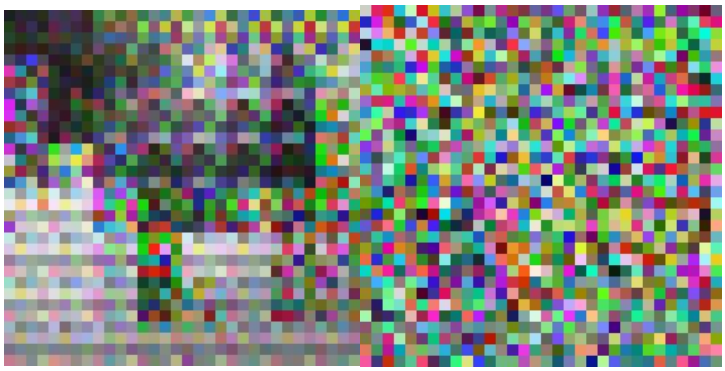
Fig 3. Network trained with novel scheme of image encryption and machine learning

The network should adjust to the novel scheme of image encryption. A convolution layer with NxN stride and NxN sized filter is put for the first layer to handle block wise image encryption. Several network- in-network style layers[5] are stacked, by using sub-pixel convolution[6], the feature map is sampled to original sized resolution. After performing this adaptation any type of network can be followed.

4. Experiments

By considering cifar dataset[7], experiments were conducted. The cifar dataset with the image size is 32x32. The block size of the proposed algorithm is set to four. After block adaptation networks[8][9] the pyramidal residual networks were constructed. Here the datasets are compared among plain images, naïve block wise pixel shuffle, combined cat map[10] and the proposed algorithm are compared. Fig.4 shows the image encryption results.

a) Plain image b) Combined cat map



c) Naïve blockwise pixel shuffle d) Proposed

Fig.4. Image Encryption Results

From the Fig. 4, in plain image and naïve block wise pixel shuffle it is easy to someone to identify the borders whereas in combined cat and proposed encryption we are not able to identify but it will be useful for the network to be trained. The validation accuracies are mentioned in Table 1. The method with higher validation gives better results. The accuracy of the combined cat algorithm is very low when compared to the other encryption techniques even though it gives the

same presentation. The accuracy of the proposed algorithm is same as plain images. The proposed algorithm satisfies the properties of the image encryption and machine learning.

	CIFAR 10	CIFAR 100
Plain image	0.884	0.591
Combined Cat map	0.468	0.209
Naïve block wise pixel shuffle	0.872	0.602
Proposed	0.863	0.568

Table 1. Validation accuracies of cifar dataset

5.Conclusion

A novel scheme is introduced to encrypt the images only for humans but not for machine. The proposed algorithm allows to build the networks without any privacy issues. The algorithm is validated with cifar dataset and gives better results when compared to the other encryption methods.

References:

[1] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, nature, vol. 521, no.7553, pp. 436-444, 2015.

[2] S. Assad, M. Farajallah, and C. Valdeanu, Chaos-based block ciphers:An overview, IEEE International Conference on Communications(COMM), pp. 1-4, 2014.

[3] T. Naga Lakshmi, S. Jyothi, Cryptography Algorithms- Issues on Recent trends,International Journal of Innovative Research and Advanced Studies (IJIRAS) Volume 5 Issue 7, July 2018, ISSN: 2394-4404

[4] Shobhna Yadav, ApoorviSood, Adaptation in Neural Networks:A review, International journal of engineering and computer Science ISSN: -, Vol. @ Issue 11,2013

[5] M. Lin, Q. Chen, and S. Yan, Network in network, InternationalConference on Learning Representations (ICLR), 2014.

[6] W. Shi, J. Caballero, F. Huszar, J. Totz, A. Aitken, R. Bishop, D.Rueckert, and Z. Wang, Real-time single image and video superresolutionusing an efficient sub-pixel convolutional neural network,IEEE Conference on Computer Vision and Pattern Recognition(CVPR), pp. 1874--1883, 2016.

[7]A.Krizhevsky, Learning multiple layers of features from tiny images, Tech Report, 2009.

[8] Y. Yamada, M. Iwamura, and K. Kise, Deep pyramidal residualnetworks with separated stochastic depth, arXiv preprintarXiv:1612.01230, 2016.

[9] D. Han, J. Kim, and J. Kim, Deep pyramidal residual networks, arXivpreprint arXiv:1610.02915, 2016.

[10] X. Wang, L. Liu, and Y. Zhang, A novel chaotic block image encryptionalgorithm based on dynamic random growth technique, Optics andLasers in Engineering, vol. 66, pp. 10--18, 2015.