On the influence of using quantized images on machine learning algorithms

1st Takayuki Osakabe
Tokyo Metropolitan University
Hino, Tokyo 191-0065, Japan
osakabe-takayuki@ed.tmu.ac.jp

2nd Yuma Kinoshita
Tokyo Metropolitan University
Hino, Tokyo 191-0065, Japan
kinoshita-yuma@ed.tmu.ac.jp

3rd Hitoshi Kiya
Tokyo Metropolitan University
Hino, Tokyo 191-0065, Japan
kiya@tmu.ac.jp

***Abstract*—Recently, applying quantized images to machine learning algorithms has been expected to enhance robustness against adversarial examples. In this paper, three quantization methods: linear quantization, lloyd-max quantization and error diffusion are considered for producing quantized images, respectively, and the influence of using the quantized images is discussed in an image classification experiment under the use of typical machine learning algorithms including deep learning ones.**

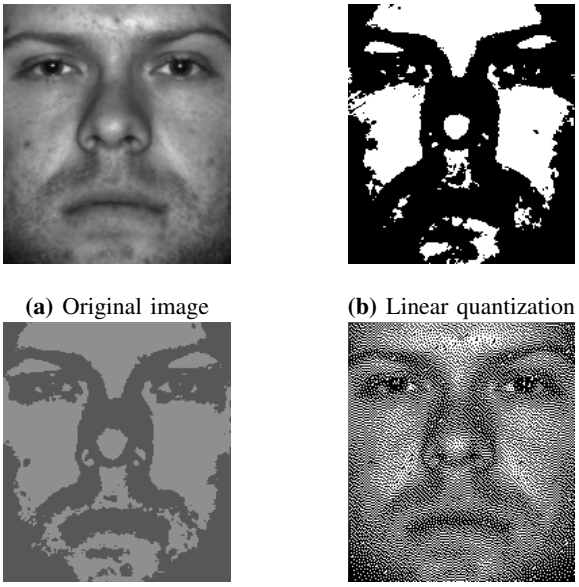
***Index Terms*—linear-quantization, lloyd-max quantization, error diffusion, machine learning, deep learning**

I. Introduction

Computer vision technologies with machine learning algorithms have been deployed in many applications including safety and security critical applications such as self-driving cars, healthcare, facial recognition. Machine learning in general suffers from attacks, so many researchers have been studied robust methods against various attacks such as privacy-preserving machine learning [1]–[5] and adversarial attacks [6]–[8], where adversarial attacks aim to misclassify images. As one of the countermeasures, using quantized image has been shown to enhance robustness against the adversarial attack [9]–[12]. However, image quantization decreases the accuracy of image classification in general.

For the above reasons, in this paper, we consider the influence of image quantization on machine learning algorithms for image classification. In an experiment, we apply three quantization methods: linear quantization, lloyd-max quantization and error diffusion, to images for producing quantized images, and the quantized images are used for carrying out some machine learning algorithms including deep learning ones for image classification.

In an image classification experiment, various quantized images are applied to not only statistical machine learning algorithms such as SVM (Support Vector Machine), KNN (k-Nearests Neighbor) and logistic regression, but also deep residual learning as a ResNet. Experimental results show that the classification accuracy depends on both the number of quantization bits and the selection of quantization methods. By carefully choosing these requirements for each model, the classification accuracy is shown to be almost the same as that of using 8-bit images. In paticular, in an experiment with ResNet-20 on the CIFAR10 dataset, quantized images are shown to be able to maintain high accuracy even when very low bit-images as 1 or 2 bits are applied, under the use of a common bit-depth between training images and test ones.



(a) Original image **(b)** Linear quantization **(c)** Lloyd-max method **(d)** Error diffusion method

Fig. 1: Example of quantized images with a bit-depth of 1bit

II. Machine learning algorithms with quantized images

In this paper, we apply three quantization methods: linear quantization, lloyd-max quantization and error diffusion, to images for producing quantized images with a bit depth of 1 to 7 bits from 8-bit images, and the quantized images are used for carrying out some machine learning algorithms including deep learning ones for image classification. Figure.1 shows the images quantized by each quantization method. Following the procedure in Fig.2, images quantized by each quantization method are applied to statistical machine learning and deep residual learning.

A. Experiment A

In experiment A, we used the face data set "Extended Yale Face Database B." [13], which consists of $38 \times 64 = 2432$ gray scale facial images with 192×168 pixels. We resized

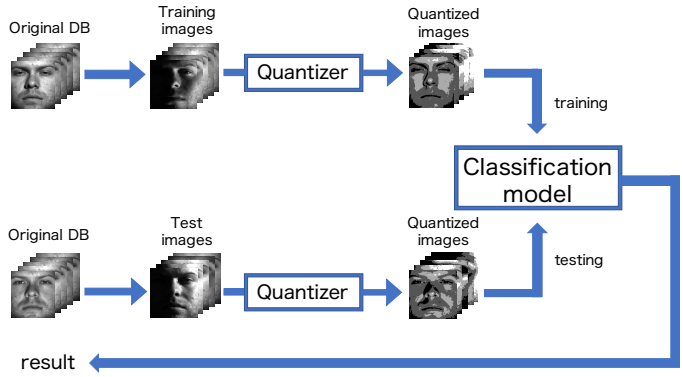


Fig. 2: Procedure of image classification with quantized images

TABLE I: Classification accuracy of using SVM (linear quantization)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	**0.689**	0.497	0.356	0.300	0.268	0.259	0.245	0.237
2bit	0.522	0.885	**0.911**	0.900	0.877	0.853	0.848	0.844
3bit	0.447	0.875	0.916	0.927	0.937	0.940	0.941	**0.942**
4bit	0.408	0.864	0.907	0.923	0.933	0.937	**0.940**	**0.940**
5bit	0.412	0.851	0.901	0.921	0.932	0.932	**0.934**	**0.934**
6bit	0.392	0.842	0.904	0.919	**0.936**	0.933	0.934	0.934
7bit	0.381	0.837	0.903	0.918	**0.934**	0.933	**0.934**	**0.934**
8bit	0.370	0.833	0.901	0.916	**0.936**	0.933	0.934	0.934

images from 192×168 pixels to 32×32 pixels and used it as dataset. Quantized images were applied to SVM, KNN, and logistic regression, respectively.

B. Experiment B

In experiment B, we used ResNet-20 as a model for image classification. The model with ResNet-20 was trained by using stochastic gradient descent (SGD) with momentum for 160 epochs. The learning rate was initially set to 0.1 and was decreased by a factor of 10 at 40, 80, and 120 epochs. We also used a weight decay of 0.0005, a momentum of 0.9, and a batch size of 128. We employed the CIFAR10 data set, which contains 32×32 color pixel images and consists of 50,000 training images and 10,000 test images in 10 classes. Also, color image quantization was performed by applying a quantization method to each channel in RGB color images.

III. Experiment Results

A. Experiment A

Tables I, II and III show results when images quantized by the linear quantization, the lloyd-max method and the error diffusion method were applied to SVM, respectively. In using SVM, the grid search was carried out with parameters that gave the best accuracy in using linear kernel and RBF (Radial Basis Funcation) kernel and a cost parameter $C = 10^i$ (i is an integer value in the range from -10 to 10).

Also, Table IV summarizes the results of Tables I, II and III, focusing on the quantization method that gave the highest accuracy.

TABLE II: Classification accuracy of using SVM (lloyd-max method)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.851	0.884	0.881	0.892	**0.897**	**0.897**	0.896	**0.897**
2bit	0.803	0.908	0.921	0.925	0.925	**0.930**	0.927	0.929
3bit	0.784	0.919	0.932	0.933	0.934	**0.936**	**0.936**	0.934
4bit	0.774	0.914	0.930	**0.934**	**0.934**	**0.934**	**0.934**	**0.934**
5bit	0.773	0.918	0.929	**0.936**	0.934	0.934	0.934	0.934
6bit	0.768	0.919	0.929	**0.936**	0.934	0.934	**0.936**	**0.936**
7bit	0.764	0.918	0.932	**0.936**	0.934	0.934	**0.936**	**0.936**
8bit	0.770	0.918	0.932	**0.936**	0.933	0.934	**0.936**	0.934

TABLE III: Classification accuracy of using SVM (error diffusion method)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.508	**0.637**	0.622	0.626	0.615	0.612	0.614	0.615
2bit	0.767	**0.905**	0.901	0.897	0.901	0.896	0.900	0.900
3bit	0.767	0.938	**0.944**	0.940	0.933	0.933	0.930	0.930
4bit	0.811	0.936	**0.940**	**0.940**	0.937	0.937	0.933	0.937
5bit	0.821	0.938	**0.942**	**0.942**	0.937	0.940	0.936	0.937
6bit	0.842	0.940	**0.944**	0.940	0.936	0.940	0.936	0.936
7bit	0.834	0.940	**0.944**	0.938	0.936	0.937	0.934	0.934
8bit	0.834	0.940	**0.945**	0.937	0.936	0.937	0.934	0.934

From Table IV, we can see that the accuracy highly depends on both quantization methods and the number of bits used for quantization. From Table IV, we can concluded the results as follows.

- The lloyd-max method gives a higher classification accuracy than the other quantization methods under the use of low-bit training images with 1 or 2 bits.
- The error diffusion method provides a higher accuracy under the use of training images with 4bits or more.
- When quantized images with more than 3 bits are used as training images, the classification accuracy is almost same as that of the baseline with 8-bit images, even when quantized images are applied.

We also carried out an experiment with KNN, logistic regression. Table V shows classification results under the use of KNN and Table VI also shows the logistic regression's ones.

The following are concluded for KNN.

- The lloyd-max method gives a higher classification accuracy under the use of 1-bit images than the other methods.
- The error diffusion method provides the best accuracy when test images have less than or equal to the number of bits of training images.

In addition, the following are concluded for logistic regression.

- The lloyd-max method provides a higher accuracy under the use of training images with 1 bit than the other methods.
- When quantized images with more than 2 bits are used as training images, the classification accuracy is almost same as that of the baseline with 8-bit images, even when quantized images are applied.

Common properties for the three learning algorithms are:

- Quantized images can provide almost the same accuracy as that of the baseline with 8-bit images.

TABLE IV: Classification accuracy of using SVM (red:linear quantization, green:lloyd-max quantization, blue:error diffusion, *:Same accuracy with two methods, **:baseline)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.851	0.884	0.881	0.892	0.897	0.897	0.896	0.897
2bit	0.803	0.908	0.921	0.925	0.925	0.930	0.927	0.929
3bit	0.784	0.938	0.944	0.940	0.937	0.940	0.941	0.942
4bit	0.811	0.936	0.940	0.940	0.937	0.937*	0.940	0.940
5bit	0.821	0.938	0.942	0.942	0.937	0.940	0.936	0.937
6bit	0.842	0.940	0.944	0.940	0.936*	0.940	0.936*	0.936*
7bit	0.834	0.940	0.944	0.938	0.936	0.937	0.936	0.936
8bit	0.834	0.940	0.945	0.937	0.936*	0.937	0.936	0.934**

TABLE V: Classification accuracy of using KNN (red:linear quantization, green:lloyd-max quantization, blue:error diffusion, *:Same accuracy with two methods, **:baseline)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.558	0.604	0.601	0.604	0.604	0.603	0.603	0.604
2bit	0.632	0.695	0.705	0.658	0.656	0.656	0.652	0.655
3bit	0.675	0.697	0.673	0.684	0.699	0.701	0.707	0.707
4bit	0.675	0.686	0.656	0.651	0.663	0.668	0.671	0.670
5bit	0.670	0.674	0.663	0.648	0.651	0.651	0.662	0.666
6bit	0.668	0.673	0.656	0.649	0.651	0.648*	0.652	0.649
7bit	0.668	0.679	0.662	0.651	0.653	0.649	0.648	0.648
8bit	0.667	0.674	0.656	0.648	0.648	0.648	0.648	0.648**

TABLE VI: Classification accuracy of using logistic regression (red:linear quantization, green:lloyd-max quantization, blue:error diffusion, *:Same accuracy with two methods, **:baseline)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.748	0.834	0.858	0.871	0.868	0.868	0.871	0.871
2bit	0.738	0.889	0.916	0.927	0.936	0.936	0.941	0.944
3bit	0.701	0.921	0.952	0.962	0.958*	0.964	0.964	0.967
4bit	0.701	0.934	0.953	0.960	0.960	0.962	0.964	0.964
5bit	0.689	0.919	0.948	0.952	0.958	0.964	0.971	0.970
6bit	0.673	0.929	0.952	0.951	0.956	0.953	0.955	0.959
7bit	0.675	0.910	0.929	0.937	0.934	0.940	0.936*	0.941
8bit	0.658	0.885	0.915	0.925	0.927	0.925	0.926	0.926**

TABLE VII: Classification accuracy of using ResNet-20 (linear quantization)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	**0.755**	0.732	0.667	0.628	0.610	0.598	0.590	0.590
2bit	0.489	**0.855**	0.851	0.833	0.824	0.819	0.816	0.815
3bit	0.382	0.768	**0.896**	0.894	0.889	0.887	0.886	0.885
4bit	0.383	0.693	0.869	0.909	**0.910**	0.909	**0.910**	0.909
5bit	0.279	0.631	0.842	0.900	0.909	0.909	**0.910**	**0.910**
6bit	0.266	0.611	0.838	0.894	0.911	**0.914**	0.913	**0.914**
7bit	0.301	0.632	0.827	0.895	0.911	0.915	**0.916**	0.915
8bit	0.232	0.608	0.822	0.885	0.908	0.913	0.913	**0.914**

B. Experiment B

Tables from VII to IX show results in Experiment B as well as in Experiment A. From Table X, the following are summerized.

- Using a common quantization bit for training and test images proves a higher accuracy than the conditions that the number of quantization bit in training and test images is different.
- The error diffusion method can maintain high classification accuracy even when training and test images with 1-bit are used.
- The error diffusion method outperforms the other quantization methods under the use of a common quantization bit for training and test images.

IV. CONCLUSIONS

In this paper, we applied quantized images to various machine learning algorithms, and its influence on classification accuracy was experimentally evaluated. The experimental results show classification accuracy highly depends on both quantization methods and learning algorithms. In addition, using a common quantization bit for training and test images was demonstrated to prove a higher accuracy than they are different. For deep learning, it was also confirmed that high classification accuracy can be obtained by using the error diffusion method, even when 1-bit or 2-bit images are applied.

REFERENCES

[1] 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. 177 844–177 855, 2019.

[2] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and H. Kiya, "Privacypreserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain," in 2019 IEEE International Conference on Image Processing (ICIP), Sep. 2019, pp. 674–678.

[3] N.Carlini and D.Wagner, "Towards evaluating the robustness of neural networks," in 2017 IEEE Symposium on Security and Privacy(SP). IEEE, 2017, pp.39-57.

[4] T. Maekawa, A. Kawamura, T. Nakachi, and H. Kiya, "Privacypreserving support vector machine computing using random unitary transformation," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E102.A, no. 12, pp. 1849–1855, 2019.

[5] A. Kawamura, Y. Kinoshita, T. Nakachi, S. Shiota, and H. Kiya, "A Privacy-Preserving Machine Learning Scheme Using EtC Images," arXiv preprint arXiv:2007.08775, Jul. 2020.

[6] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." CoRR, abs/1412.6572, Dec. 2014. https://arxiv.org/abs/1412.6572

[7] A. Kurakin, I.Goodfellow, and S.Bengio, "Adversarial machine learning at scale," arXiv preprint arXiv:1611.01236, 2016

[8] A. MaungMaung and H. Kiya, "Encryption inspired adversarial defense for visual classification," arXiv preprint arXiv:2005.07998, May. 2020, to appear in the 27th IEEE International Conference on Image Processing (ICIP 2020).

[9] S. Miyazato, X. Wang, T. Yamasaki and K. Aizawa, "Reinforcing the robustness of a deep neural network to adversarial examples by using color quantization of training image data" in ICIP, pp.884-888, 2019

[10] April Pyone MAUNG MAUNG, Warit SIRICHOTEDUMRONG, and Hitoshi KIYA, "Adversarial Test on Learnable Image Encryption," Proc. IEEE Global Conference on Consumer Electronics, Osaka, Japan, 16th October, 2019.

[11] April Pyone MAUNG MAUNG, Yuma KINOSHITA, and Hitoshi KIYA, "Filtering Adversarial Noise with Double Quantization ," Proc. APSIPA Annual Summit and Conference, Lanzhou, China, 18th November, 2019.

[12] April Pyone MAUNG MAUNG, Yuma KINOSHITA, and Hitoshi KIYA, "Adversarial Robustness by One Bit Double Quantization for Visual Classification," IEEE Access, vol.7, no.1, pp.177932–177943, December 2019.

[13] A.S. Georghiades, P.N. Belhumeur, and D.J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," IEEE transactions on pattern analysis and machine intelligence, vol.23, no.6, pp.643–660, 2001.

TABLE VIII: Classification accuracy of using ResNet-20 (lloyd-max method)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.713	0.780	0.796	0.800	0.806	0.806	0.806	**0.807**
2bit	0.669	0.834	0.854	0.859	0.864	0.864	**0.866**	0.865
3bit	0.544	0.823	0.879	0.888	0.891	0.895	**0.896**	**0.896**
4bit	0.429	0.787	0.873	0.892	0.899	0.899	0.902	**0.903**
5bit	0.391	0.744	0.864	0.892	0.902	0.904	0.907	**0.909**
6bit	0.362	0.712	0.848	0.889	0.900	0.905	0.910	**0.912**
7bit	0.285	0.664	0.824	0.879	0.898	0.906	0.909	**0.914**
8bit	0.228	0.552	0.747	0.827	0.865	0.885	0.900	**0.914**

TABLE IX: Classification accuracy of using ResNet-20 (error diffusion method)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	**0.859**	0.838	0.822	0.814	0.811	0.809	0.808	0.808
2bit	0.416	**0.882**	0.875	0.862	0.857	0.855	0.854	0.853
3bit	0.130	0.740	**0.902**	0.895	0.891	0.887	0.886	0.887
4bit	0.137	0.271	0.849	**0.909**	0.908	0.906	0.906	0.906
5bit	0.148	0.272	0.705	0.897	0.916	**0.917**	**0.917**	0.916
6bit	0.125	0.229	0.667	0.870	0.910	**0.916**	**0.916**	**0.916**
7bit	0.114	0.293	0.613	0.836	0.902	0.913	**0.916**	**0.916**
8bit	0.155	0.272	0.635	0.846	0.901	0.910	**0.914**	**0.914**

[14] The CIFAR-10 dataset http://www.cs.toronto.edu/ kriz/cifar.html

TABLE X: Classification accuracy of using ResNet-20 (red:linear quantization, green:lloyd-max quantization, blue:error diffusion, *:Same accuracy with two methods, **:baseline)

train	test							
	1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1bit	0.859	0.838	0.822	0.814	0.811	0.809	0.808	0.808
2bit	0.669	0.882	0.875	0.862	0.864	0.864	0.866	0.865
3bit	0.544	0.823	0.902	0.895	0.891*	0.895	0.896	0.896
4bit	0.429	0.787	0.873	0.909*	0.910	0.909	0.910	0.909
5bit	0.391	0.744	0.864	0.900	0.916	0.917	0.917	0.916
6bit	0.362	0.712	0.848	0.894	0.911	0.916	0.916	0.916
7bit	0.301	0.664	0.827	0.895	0.911	0.915	0.916*	0.916
8bit	0.232	0.608	0.822	0.885	0.908	0.913	0.914	0.914**