社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

量子化画像を用いた機械学習法とその影響

長我部恭行† 　木下　裕磨† 　貴家　仁志†

† 首都大学東京〒191–0065 東京都日野市旭が丘 6-6
E-mail: †{osakabe-takayuki,kinoshita-yuma}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

あらまし　近年，量子化された画像の機械学習への適用が，敵対的攻撃 (Adversarial Example) を中心として機械学習のセキュリティ強化の観点から注目されている．しかし，データの量子化は機械学習の精度に影響を与えてしまう．本稿では，線形量子化，ロイドマックス誤差法，誤差拡散法の 3 種類の量子化方法を画像に適用し，深層学習を含む複数の機械学習法の画像分類における分類精度への影響を考察する．実験の結果，統計的機械学習法においては本稿で使用する SVM，KNN，ロジスティック回帰の各モデルに共通して 1，2 ビットの低ビット数ではロイドマックス誤差法を使用することで高い分類精度が得られることを確認した．また，それぞれのモデルに対して量子化手法と量子化ビット数を適切に設定することで，ベースラインの分類精度と同等以上の分類精度を与えることを確認した．ResNet-20 を使用した深層学習においては，誤差拡散法を使用して，学習用画像とテスト画像のビット数を合わせることで高い分類精度が得られることを実験して確認した．

キーワード　線形量子化，ロイドマックス誤差法，誤差拡散法，機械学習，深層学習

Machine learning algorithms with quantized images and their influence

Takayuki OSAKABE†, Yuma KINOSHITA†, and Hitoshi KIYA†

† Tokyo Metropolitan University
E-mail: †{osakabe-takayuki,kinoshita-yuma}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

Abstract　Recently, appling quantized images to machine learning algorithms is expected to enhance robustness against adversarial examples. However, quantizing data affects the performance of machine learning algorithms. In this paper, three quantized methods: linear quantization, lloyd-max quantization and error diffusion are applied to images respectively, and we consider the influence of the quantization in some machine learning algorithms including deep learning for image classification. Experimental results show that we can get high classification accuracy even when low bits (1 or 2bit) images quantized by lloyd-max quantization are used in SVM, KNN and Logistic Regression. The results also demonstrate that we can obtain almost the same classification accuracy as that of baseline if we carefully choose a quantized method and the number of bits under the use of each model. In deep learning with ResNet-20, the model gives high classification accuracy if both of training and test images are quantized by using error diffusion with the same number of bits.

Key words　linear-quantization，lloyd-max quantization, error diffusion, machine learning, deep learning

1. ま え が き

近年，機械学習の普及に伴い，画像の機械学習を用いた分析，分類などが盛んに研究されている．一方，画像を誤分類させるなどの攻撃手法として敵対的攻撃 (Adversarial Example) [1]〜[3] の存在が指摘され，大きな問題になっている．その対策の 1 つとして，画像の量子化が注目されている [4]〜[6]．しかしながら，画像の量子化は敵対的攻撃に対しては有効であるが，画像分類の精度を下げてしまうといった問題点を抱えている．

このような背景から，本稿では，画像を量子化することで機械学習の分類精度にどのような影響を与えるのかを考察する．実験では，統計的機械学習および深層学習に学習用画像とテスト画像の両方にそれぞれ 1 から 7 ビットに量子化した画像と，量子化前の 8 ビットの画像を適用する．また，量子化には線形量子化，ロイドマックス誤差法，誤差拡散法の 3 つを使用する．実験の結果，統計的機械学習においてはそれぞれのモデルに対して適切な量子化手法，量子化ビット数で量子化された画像を使用することで，ベースラインの精度と同等以上の分類精

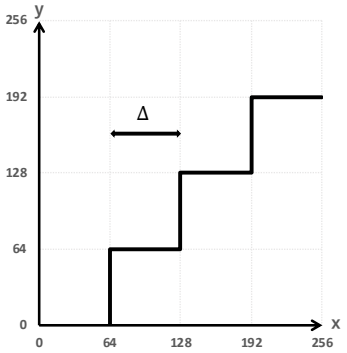


図 1: ミッドトレッド型線形量子化の変換関数例 ($l = 8, M = 2$)

度が得られることを確認した．深層学習に量子化画像を適用する際には，学習用画像とテスト画像のビット数を合わせることで低ビット数の画像を用いても高い分類精度を与えることを確認した．

2. 代表的量子化手法

本稿では，各チャンネルの画素値が 8bit で与えられる画像に量子化を施す．以下に本稿で用いる量子化手法を要約する．

2.1 線形量子化

線形量子化とは，量子化幅が一定な量子化手法のことである．一般に，2 つの線形量子化法:ミッドトレッド型とミッドライザ型が知られている [7]．本稿では，ミッドトレッド型を線形量子化法として使用する．ミッドトレッド型では，画素値 x の定義域を $[0, 255]$ の整数値とすると，次式によって量子化値 y が与えられる．

$$y = \lfloor \frac{x}{\Delta} \rfloor \times \Delta \tag{1}$$

ここで，$\Delta = 2^{l-M}$ とする．l は画素値のビット長であり，本稿では $l = 8$ とする．また，M は量子化ビット数であり，画像の 2 値化では $M = 1$ となる．この時，量子化後の値 (代表値)y の個数は $L = 2^M$ となる (図 1 参照)．図 3(b) に量子化画像例を示す．

2.2 ロイドマックス誤差法

ロイドマックス誤差法 [8] では，与えられた量子化ビット数 M の下で，量子化誤差の 2 乗平均 (MSE) が最小になるように量子化が実行される．ここで，代表値 y_i に対応する x の区間を $[x_{i-1}, x_i]$ とする時，量子化誤差の 2 乗平均 N は式 (2) のように表せる．

$$N = \sum_{i=1}^{L} \int_{x_{i-1}}^{x_i} (x - y_i)^2 p(x) dx \tag{2}$$

ここで，$p(x)$ は x に対する確率密度関数である．ロイドマックス誤差法の実行手順を以下に示す．

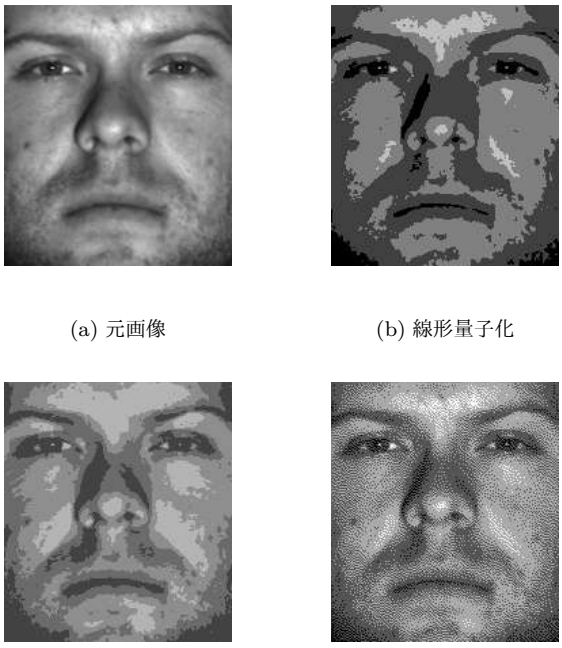
（a） L 個の量子化代表値をランダムに決定する．ただし，$y_1 < y_2 < \ldots < y_L$ とする．

（b） 量子化しきい値 x_i を $x_i = \frac{1}{2}(y_i + y_{i+1})$ $(i = 1, 2, \ldots, L-1)$ により求める．ただし，$x_0 = 0, x_L = 255$ とする．

（c） 代表値を $y_i = \frac{\int_{x_{i-1}}^{x_i} x \cdot p(x) dx}{\int_{x_{i-1}}^{x_i} p(x) dx}$ $(i = 1, 2, \ldots, L)$ に従って更新する．

（d） (b)，(c) を式 (2) の N が改善されなくなるまで繰り返す．

図 3(c) に量子化画像例を示す．



(a) 元画像　(b) 線形量子化

(c) ロイドマックス誤差法　(b) 誤差拡散法

図 3: 量子化画像例 ($l = 8, M = 2$)

2.3 誤差拡散法

誤差拡散法とは，量子化の際に発生する量子化誤差を注目している画素から周りの画素へと拡散することで視覚的な量子化誤差の影響を軽減しようと提案された方法である．本稿では，Floyd と Steinberg によって提案された Floyd-Steinberg 法 [9] を用いる．座標 (i, j) に存在する量子化前の画素値を $x(i, j)$，量子化後の画像の画素値を $y(i, j)$ とすると，量子化誤差 $e(i, j) = x(i, j) - y(i, j)$ を以下の式に基づいて周りの画素へと拡散する．

$$\begin{cases} y(i, j+1) = x(i, j+1) + \frac{7}{16} e(i, j) \\ y(i+1, j-1) = x(i+1, j-1) + \frac{3}{16} e(i, j) \\ y(i+1, j) = x(i+1, j) + \frac{5}{16} e(i, j) \\ y(i+1, j+1) = (i+1, j+1) + \frac{1}{16} e(i, j) \end{cases} \tag{3}$$

すなわち，図 4 に示す誤差拡散係数に従って量子化誤差を拡散し，量子化を実行する (図 3(d) 参照)．

3. 量子化画像を用いた機械学習

2. で述べた各量子化によって生成された量子化画像を，統計的機械学習および深層学習のそれぞれに適用する．本稿では，量子化画像をすべて教師ありの機械学習法に適用し，分類精度

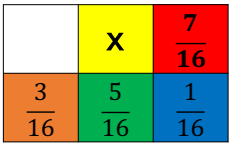


図 4: Floyd-Steinberg 法の誤差拡散係数 (x:注目画素)

の観点から，量子化による影響を考察する．

3.1 統計的機械学習への適用

本稿では，1 から 7bit で量子化された画像と 8bit の元画像を学習用画像としてモデルを学習する．次に，テスト画像に対しても同様に量子化を施し，学習されたモデルに適用する．モデルには，SVM(Support Vector Machine)，KNN(k-Nearest Neighbor)，ロジスティック回帰の 3 つを使用する．

SVM では，入力される特徴ベクトル $\boldsymbol{x}$ に対して識別関数

$$y = sign(\omega^T \boldsymbol{x} + b) \tag{4}$$

によって 2 値の出力が計算される．本稿では，入力する特徴ベクトル $\boldsymbol{x}$ には画像の画素値をそのまま用いる．また，ω は重みに対応するパラメータであり，b はバイアス項である．また，関数 $sign(x)$ は $x > 0$ のとき 1，$x \leq 0$ のとき -1 を出力する．これは，識別空間に対して入力される特徴空間を 2 つに分類することに相当する．一対多の 2 値分類を複数回行うことで多クラス分類を可能とする．また，SVM はカーネル法により，特徴ベクトルを高次元へと写像することで非線形な問題にも適用することができる．

KNN は，ベクトル空間上に学習データをプロットしておき，そこに入力ベクトルがプロットされた場合，そこからベクトル空間上で距離の近い k 個の学習データに付けられているラベルに従って多数決により入力ベクトルの分類を決定する方法である．

ロジスティック回帰は判定確率を求めることができる線形分類器である．入力の特徴ベクトル x に対してロジスティック関数 (シグモイド関数)

$$y = \frac{1}{1 + \exp\{-(\omega^T \boldsymbol{x} + b)\}} \tag{5}$$

を適用することで，y を 2 値分類における一方のクラスの予測確率であると捉えることができる．また，重みのパラメータ ω は最尤推定法により最適化される．

3.2 深層学習への適用

同様に，量子化画像を CNN(Convolutional Neural Network) へと適用する．本稿では，データセットに CIFAR-10 [10] を使用し，ネットワークに ResNet-20 [11] を使用して 1 から 8bit の画像でモデルをトレーニングする．次に，学習されたモデルに対して同様に量子化を施したテスト画像を用いて，画像のクラス分類の分類精度の評価から量子化の影響を考察する．

4. 実　　験

図 5 の手順に従い，各量子化法で量子化された画像を統計的機械学習および深層学習へと適用する．

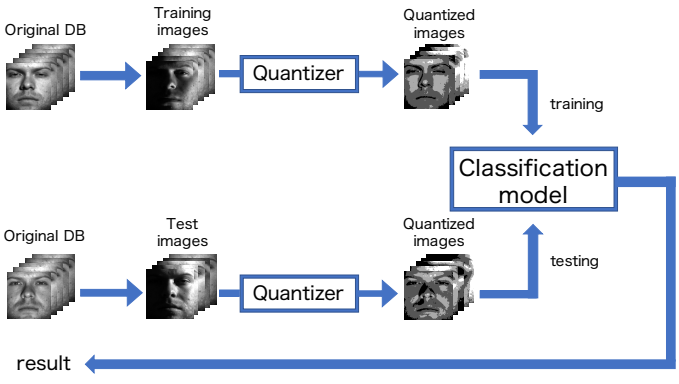


図 5: フロー図

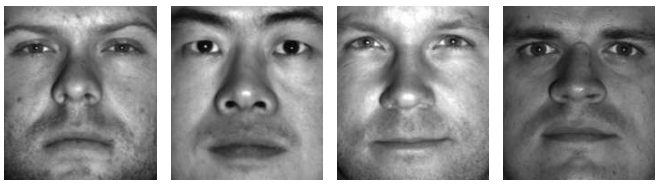


図 6: 画像例 (Extended Yale Face Database B)

4.1 実 験 条 件

実験 A(統計的機械学習への適用)

実験 A では，顔画像データセット Extended Yale Face Database B [12] を使用して実験を行なった．このデータセットはサイズが 192×168 で，計 38 人のグレースケールの顔画像各 64 枚の計 2432 枚で構成される (図 6 参照)．本稿では，画像サイズを 32×32 にリサイズしたものをデータセットとして使用する．データセットをランダムサンプリングし，70% を学習用画像に，残りの 30% をテスト画像として使用した．分類モデルにはそれぞれ SVM，KNN，ロジスティック回帰を用いて分類精度を検証した．

SVM はグリッドサーチを用いて，カーネルが RBF(Radial Basis Function) カーネル，線形カーネルの中から，コストパラメータ C が $C = 10^i$(ただし，i は $[-10, 10]$ の整数値) から最も分類精度の高いパラメータを使用した．KNN では $k = 3$ で入力ベクトルから最も近い 3 つのベクトルを採用した．ロジスティック回帰は正則化項に L2 ノルムを使用し、コストパラメータ C は 1.0 で実験を行なった．

実験 B(深層学習への適用)

実験 B では，分類モデルのネットワークには ResNet-20 を使用し，バッチサイズ 128，エポック数 160，初期学習率 0.1(40 エポック毎に 0.1 倍)，最適化には慣性項を 0.9，重みの減衰率を 0.0005 に設定した SGD(Stochastic Gradient Decent) を用いて，一般物体認識のモデル評価に広く用いられているデータセット CIFAR-10 を学習用画像 5 万枚，テスト画像 1 万枚の計 6 万枚を使用して行なった．CIFAR-10 は鳥，飛行機，猫などの計 10 クラスが存在するデータセットでサイズが 32×32 のカラー画像で構成される (図 7 参照)．また，カラー画像に対する量子化は RGB の各チャンネル毎にそれぞれ量子化を施すこ

図 7: 画像例 (CIFAR-10)

表 1: SVM を用いた画像分類精度 (線形量子化)

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

表 2: SVM を用いた画像分類精度 (ロイドマックス誤差法)

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

とで，色情報を保持しながら量子化を適用した．

4.2 実験結果

実験 A(統計的機械学習への適用)

表 1 から表 3 にモデルに SVM を使用した場合の結果を示す．これらの比較から，量子化法の違いが画像分類精度に影響を与えることがわかる．さらに，その傾向は学習用画像の量子化ビット数とテスト画像の量子化ビット数の関係に大きく依存することがわかる．また，表 4 は，表 1 から表 3 の結果を各量子化条件の下で整理したものであり，各量子化ビット数の組み合わせごとに最高精度を与える量子化法に注目してる．ただし，赤色が線形量子化，緑色がロイドマックス誤差法，青色が誤差拡散法を表す．また，表中の*は 2 つの手法で同じ精度だったもの，**はベースラインの精度を表すとする．

表 4 から以下のことがわかる．

- 学習用画像が低ビット (1，2 ビット) の場合にはロイドマックス誤差法，4 ビット以上では誤差拡散法が高い分類精度を与える．
- 学習に 3 ビット以上のビット数で量子化した画像を用いれば，ベースラインと同等以上の分類精度が期待できる．

同様に，モデルに KNN を使用した場合の結果を表 5 に示す．表 5 から以下のことがわかる．

表 3: SVM を用いた画像分類精度 (誤差拡散法)

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

表 4: SVM を用いた画像分類の最高分類精度 (赤:線形量子化，緑:ロイドマックス誤差法，青:誤差拡散法，*:2 つの手法で同精度，**:ベースライン)

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**

表 5: KNN を用いた画像分類の最高分類精度 (赤:線形量子化，緑:ロイドマックス誤差法，青:誤差拡散法，*:2 つの手法で同精度，**:ベースライン)

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**

- 学習用画像が 1 ビットの場合にはロイドマックス誤差法，2 ビット以上の場合にはテスト画像に学習用画像のビット数以下のビット数の画像を使用する場合には誤差拡散法，学習用画像のビット数より大きいビット数の画像を使用する場合には線形量子化を用いることで高い分類精度を与える．
- ベースラインの精度と同等以上の精度を絵得るには，2 ビット以上のビット数で量子化した画像を学習に用いれば良い．

モデルにロジスティック回帰を使用した場合の結果を表 6 に示す．表 6 から以下のことがわかる．

- 学習用画像に 1 ビットの画像を使用する場合にはロイドマックス誤差法，3 ビット以上の画像を使用する場合には誤差拡散法を用いることで高い分類精度が得られる．
- 学習用画像に 3 ビット以上のビット数で量子化した画像を用いることで，ベースラインと同等以上の分類精度が期待できる．

表 6: ロジスティック回帰を用いた画像分類の最高分類精度 (赤:線形量子化，緑:ロイドマックス誤差法，青:誤差拡散法，*:2 つの手法で同精度，**:ベースライン)

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**

表 7: ResNet-20 を用いた画像分類精度 (線形量子化)

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**

表 8: ResNet-20 を用いた画像分類精度 (ロイドマックス誤差法)

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**

実験 B(深層学習への適用)

実験 A と同様に ResNet-20 に各量子化法を適用した画像を用いて画像分類を行なった結果を表 7 から表 9 に示す．また，最高精度を与える量子化方法に注目し，各量子化条件の下で整理したものを表 10 に示す．表 10 から以下のことがいえる．

- 学習用画像とテスト画像の量子化ビット数を同じにしたときに高い分類精度が得られる．
- 1 ビットの画像で学習，認識を行なった場合でも量子化手法に誤差拡散法を用いることで，高い分類精度が与えられる．
- 低ビット数の画像で分類を行う場合には，量子化法に誤差拡散法を用いることで高い分類精度が得られる．

5. ま と め

本稿では，量子化画像をあらゆる機械学習法へと適用することで，分類精度に与えるその影響を考察した．実験結果より，統計的機械学習および深層学習に量子化画像を適用する際には，量子化法の違いや学習用画像の量子化ビット数とテスト画像の

表 9: ResNet-20 を用いた画像分類精度 (誤差拡散法)

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**

表 10: ResNet-20 を用いた画像分類の最高分類精度 (赤:線形量子化，緑:ロイドマックス誤差法，青:誤差拡散法，*:2 つの手法で同精度，**:ベースライン)

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**

量子化ビット数の関係に依存して，分類精度に大きな影響を与えることを確認した．量子化手法，量子化ビット数をモデルに合わせて適切に設定することで，十分な分類精度が得られる．ResNet-20 では，誤差拡散法を用いて学習用画像，テスト画像の量子化ビット数を合わせることで高い分類精度が得られることを確認した．

文　　献

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

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

[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] 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

[5] 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.

[6] 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.

[7] 電子情報通信学会 知識ベース 「知識の森」 2 群 5 編 画像符号化 6 章 量子化

[8] S.P.Lloyd, “Least Squares Quantization in PCM”, IEEE Trans. Inform. Theory., vol. IT-28, No.2, March 1982

[9] R.W. Floyd, L. Steinberg, “An adaptive algorithm for spatial grey scale.” Proceedings of the Society of Information

Display 17, (1976) 75–77
[10] The CIFAR-10 dataset http://www.cs.toronto.edu/ kriz/cifar.html
[11] K. He, X. Zhang, S. Ren, and J. Sun. “Deep residual learning for image recognition.” In Proceedings of CVPR, pages 770–778, 2016.
[12] 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.