Kerasの中間層の位相に基づく知覚ハッシュの生成法

木下研究室

201603828

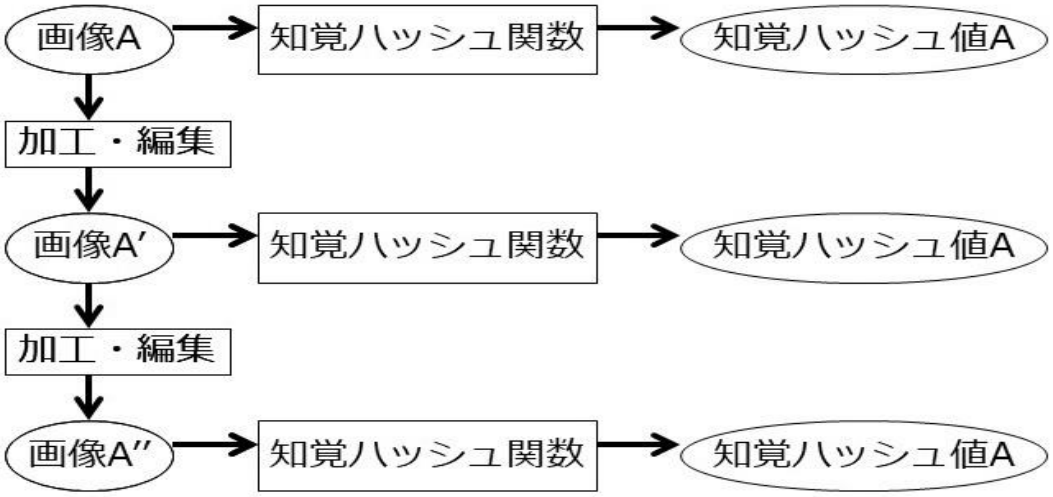
小藤田 陸

研究背景

- 近年コミックマーケットにおけるコンテンツの適切な二次利用問題などが生じてきた。
- 画像などのメディアに対して著作権管理を行う手法として電子透かしという技術があり、セキュリティ上の必要性から透かし情報は画像に固有の情報から生成される必要がある。
- さらに、透かし情報は二次利用で想定される様々な加工に対して不変のものでなければならない。
- この要件を満たす技術としては知覚ハッシュ関数の適用が考えられる。

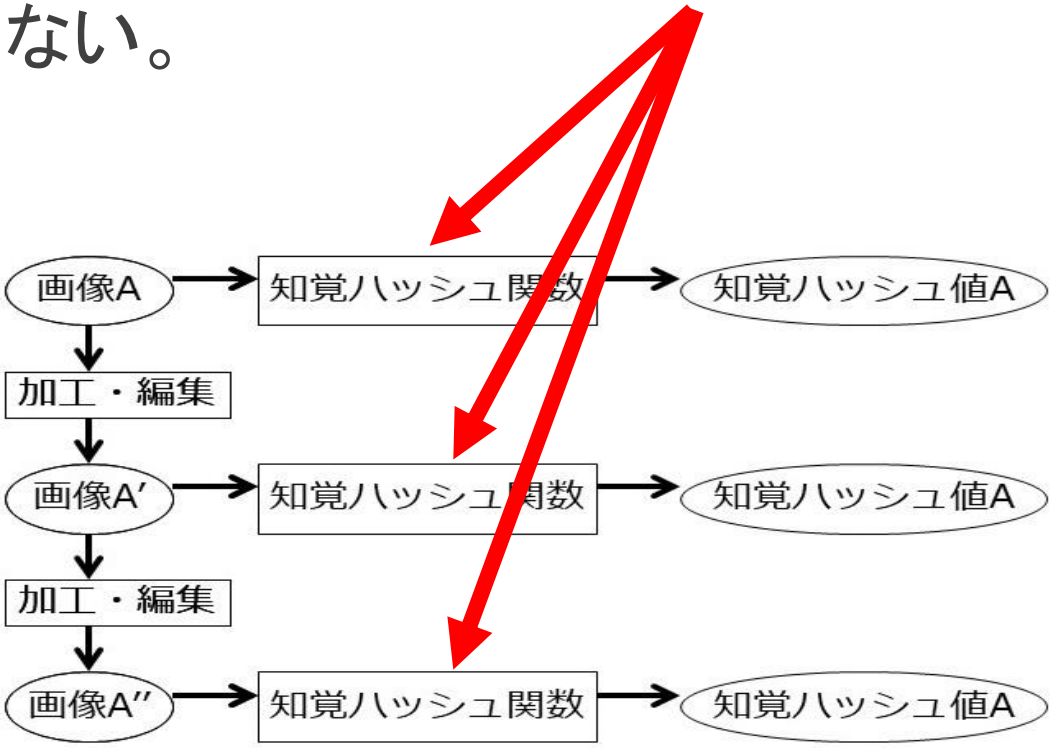
知覚ハッシュ

- 画像などのメッセージダイジェストを人間の知覚に即した形で生成する手法である。
- 知覚ハッシュでは加工や編集などを行っても原画像と同様のハッシュ値を得られる。
- これにより電子透かしに埋め込む透かし情報を他のコンテンツに流用することを防止する。



知覚ハッシュの問題点

- 加工や編集の種類に応じてそれぞれ最適な既存の知覚ハッシュ生成法のアルゴリズムを選定しなければならない。



目的

- CNN中間層出力データの位相幾何学的構造の中の不変クラスターをベイズ統計手法によって機械学習推定し、アルゴリズムが選定せず、既存の知覚ハッシュ生成法に比べ、ロバストなシステムを構成する。

そのための1つの試みとして、CNN中間層の位相構造を分析する

- 「原画像と原画像を少しずつ変形加工した画像の集合」を含む画像集合族を1つの画像集合とその部分集合の集まりと見做す。

画像集合族

=

画像集合

+

部分集合

そのための1つの試みとして、CNN中間層の位相構造を分析する

- もし「原画像と原画像を少しずつ変形加工した画像の集合」と他の画像の部分集合に分割可能であれば、「原画像と原画像を少しずつ変形加工した画像の集合」に特定の値（ハッシュ値）を付与することが可能となる。

画像集合族

＝

画像集合

＋

部分集合

ハッシュ値

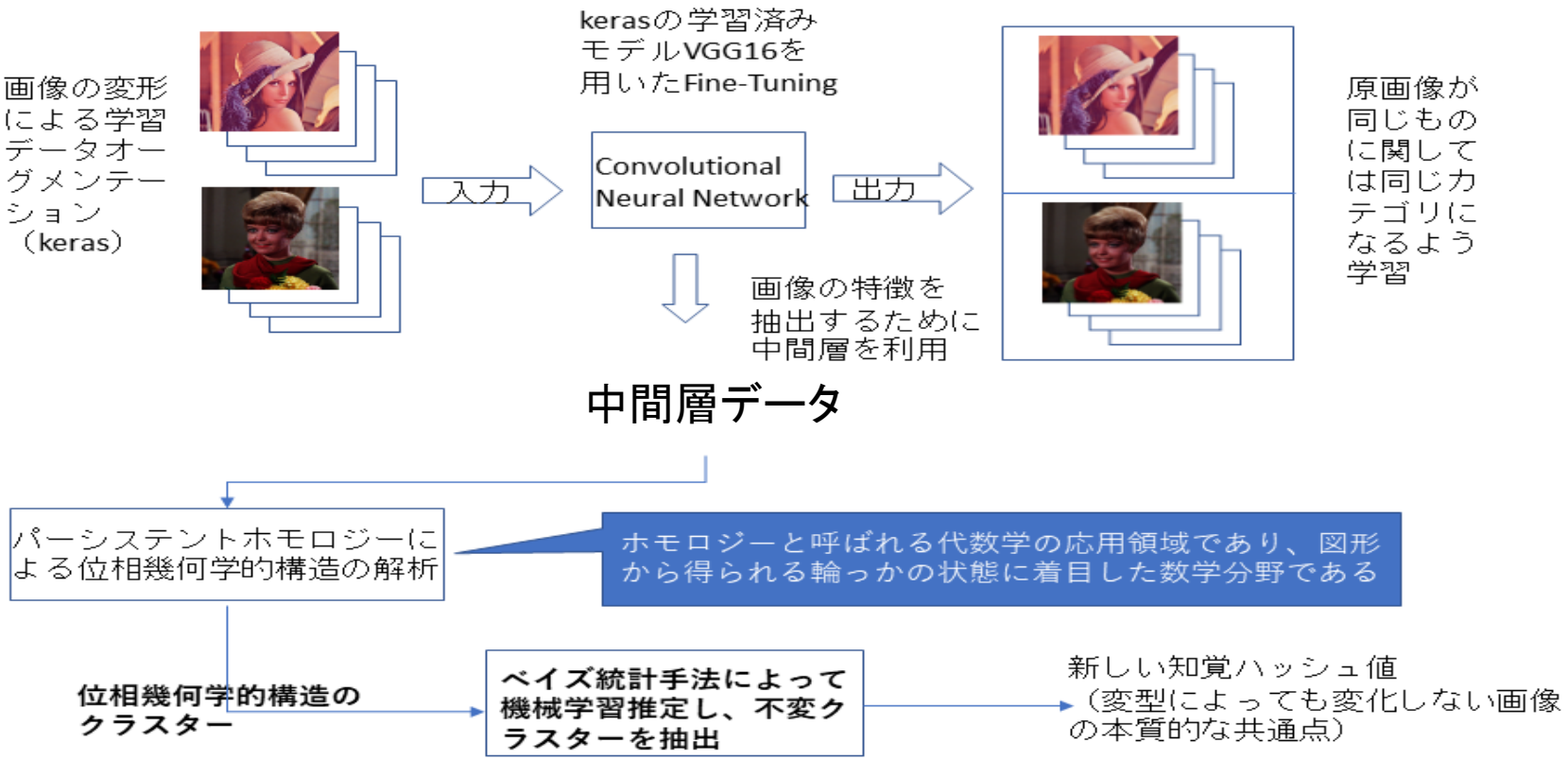
位相幾何学的構造を知覚ハッシュ生成に応用する

- 画像の類似と言う構造は数学的な「距離の概念」として還元される。
- 距離の概念を抽象化した概念は、位相幾何学が示す「位相」の概念である。
- したがって、「原画像と原画像を少しずつ変形加工した画像の集合」及びその他の画像部分集合を群と見做し、群の間に位相構造を定義すれば、知覚ハッシュに適用するべき数学的ツールになる。

位相幾何学的構造を知覚ハッシュ生成に応用する

- このような数学的構造を持つものとしてホモロジー群が考えられる。
- ホモロジー群を剰余群として定義するとき、その代表元は画像部分集合における中核的な役割、即ち「原画像と原画像を少しずつ変形加工した画像の集合」のハッシュ値を表現するものとなる。

提案システム


画像の変形による学習データオーグメンテーション（keras）
入力
kerasの学習済みモデルVGG16を用いたFine-Tuning
Convolutional Neural Network
出力
原画像が同じものに関しては同じカテゴリになるよう学習
画像の特徴を抽出するために中間層を利用
中間層データ
パーシステントホモロジーによる位相幾何学的構造の解析
ホモロジーと呼ばれる代数学の応用領域であり、図形から得られる輪っかの状態に着目した数学分野である
位相幾何学的構造のクラスター
ベイズ統計手法によって機械学習推定し、不変クラスターを抽出
新しい知覚ハッシュ値（変型によっても変化しない画像の本質的な共通点）

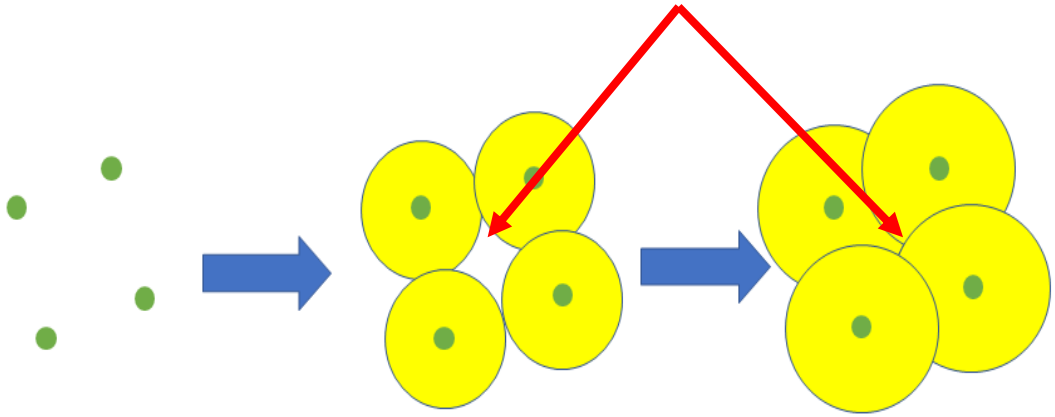
パーシステントホモロジー

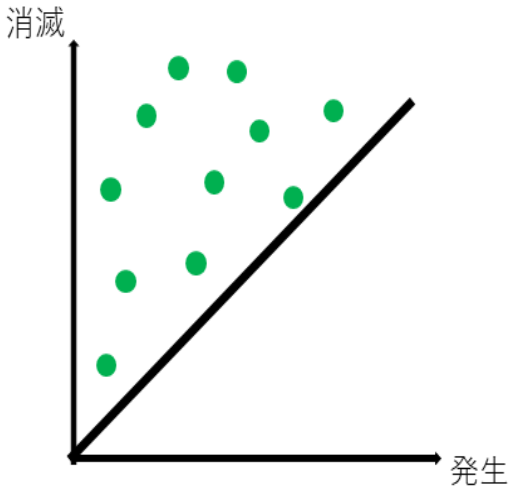
- パーシステントホモロジーは、ホモロジーと呼ばれる代数学の応用領域であり、図形から得られる位相幾何学的構造（リング等）に着目した数学分野である。

- パーシステントホモロジーは、位相的データ解析の中でも特に重要な概念であり、図形の孔、空隙、連結成分、といった構造に着目することによって、データの形の特徴を定量的かつ効率的に抽出することができる。

パーシステントホモロジー図（PD図）

- パーシステントホモロジーにより解析されたデータを可視化したものをパーシステントホモロジー図(PD 図) という。
- PD 図はデータの形の情報をうまく集約していると考えられ、実際様々なデータ解析に利用されている。

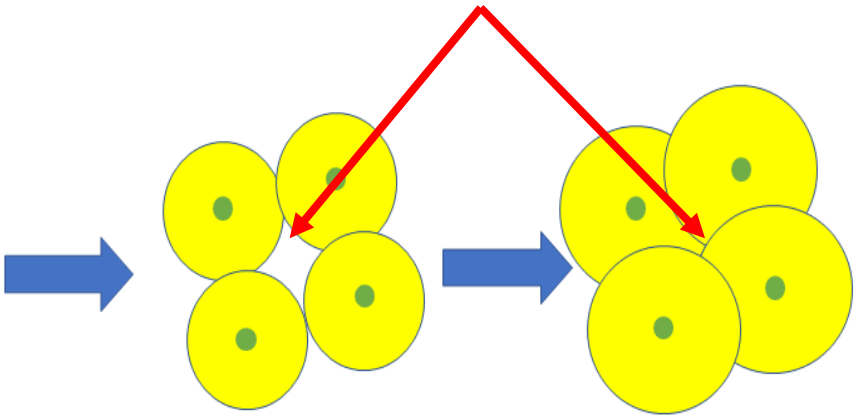


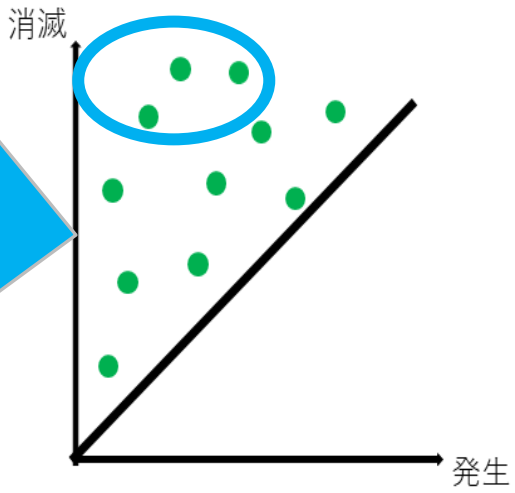


パーシステントホモロジー図（PD図）

・対角線部分の位相データはノイズと見做される。

・青丸のように対角線から離れている点は発生してから消滅するまでの時間が長いことからロバストな（強固な）データと示される。





実験内容

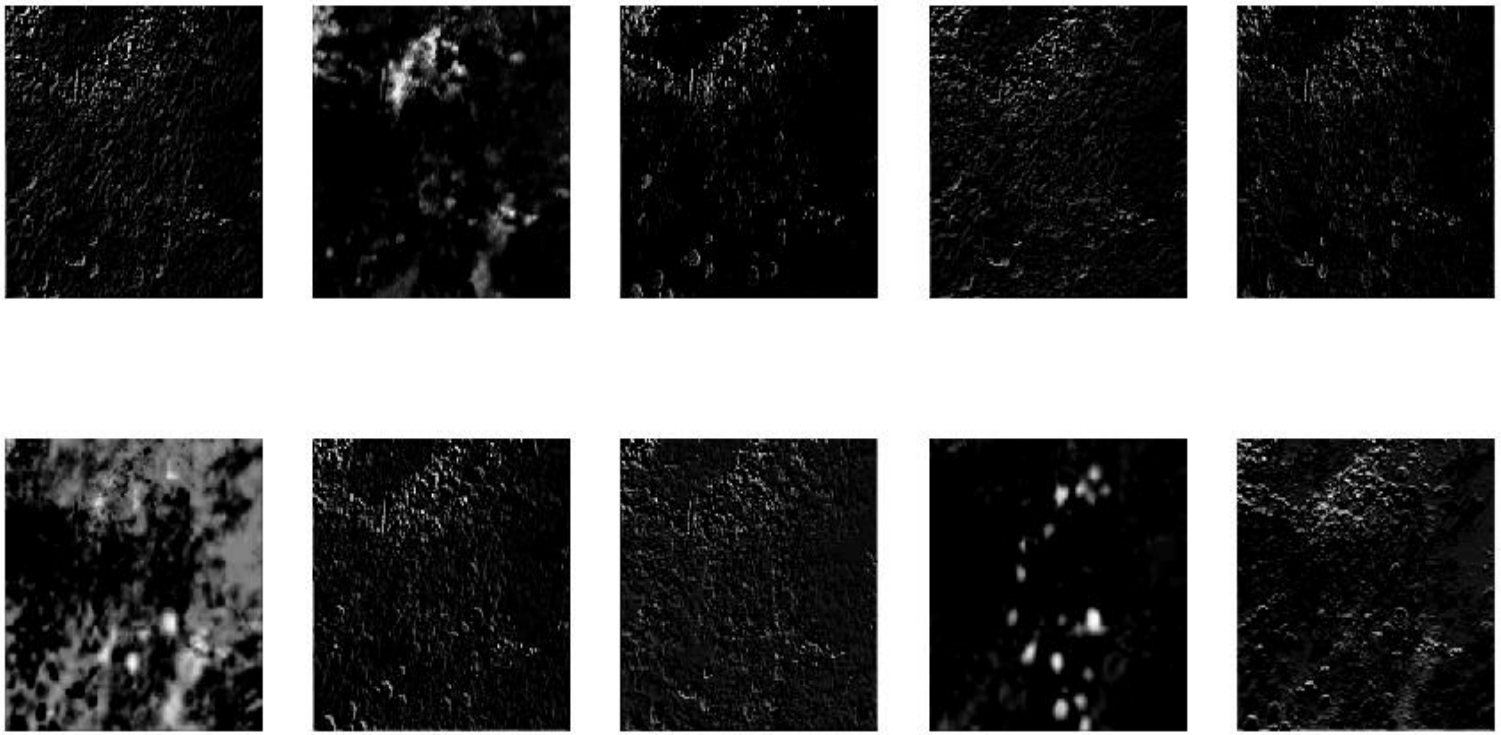
- 右の画像をCNNに入力し、中間層のPooling1層目データを可視化した10枚の画像を**HomCloud**というパーシステントホモロジーの計算ソフトウェアを使用し、PD図計算する。

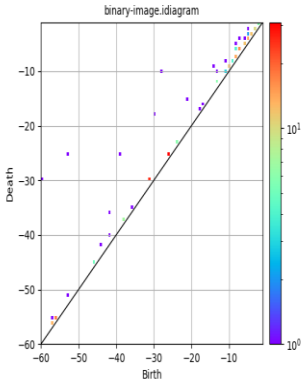
HomCloud:

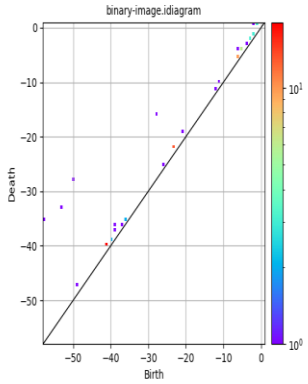
東北大学の平岡研究室大林一平を中心に開発された。dipha, phat,ripser,cgalなどを利用している。

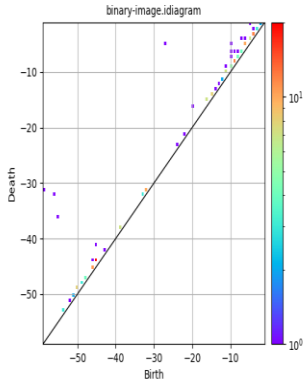
(www.wpi-aimr.tohoku.ac.jp/hiraoka_labo/homcloud/index.html)

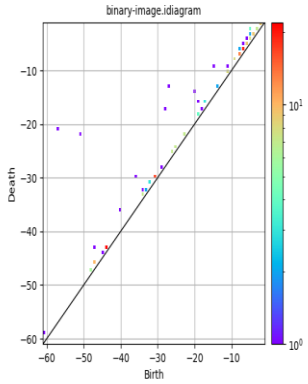
可視化した画像

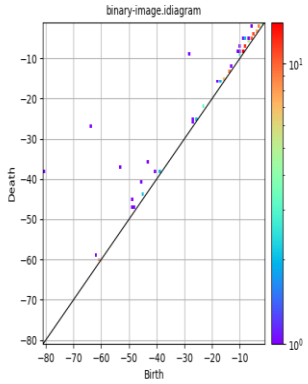


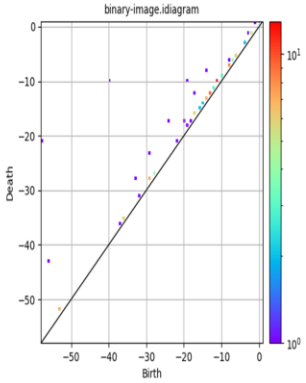


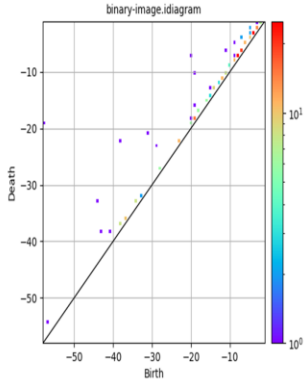


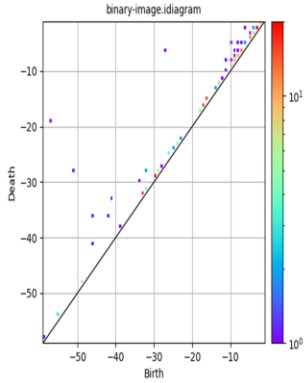


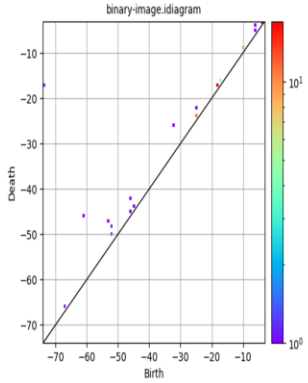


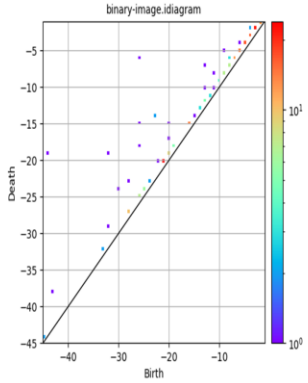






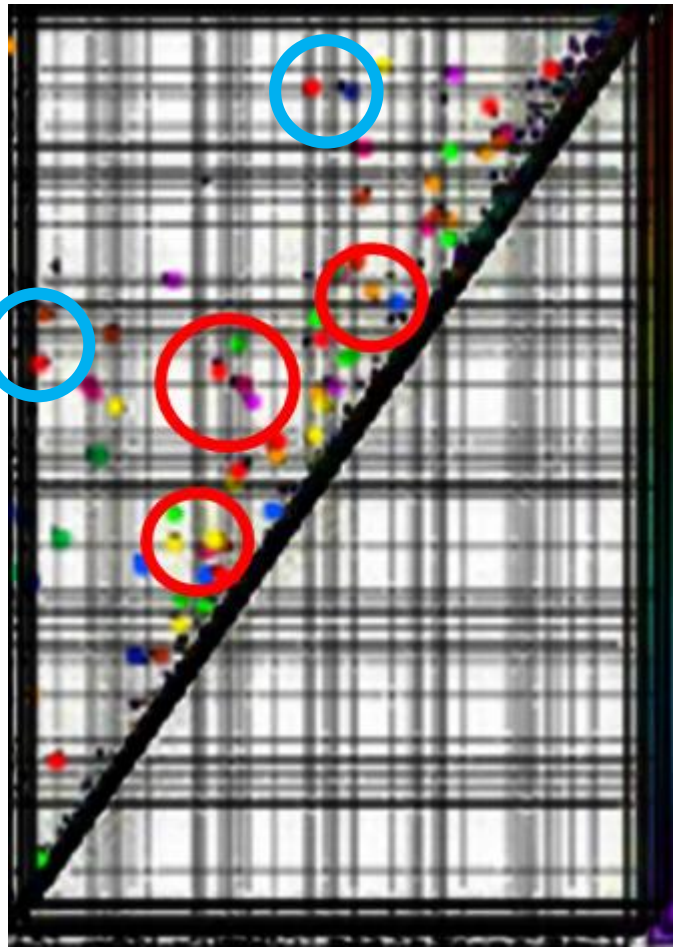






結果

結果



1. 左図は、1枚の限画像につき、CNN第一中間層10枚のPD図の位相データそれぞれに10色で着色し、重ねたPD図である。
2. 赤丸で囲った部分は6色以上の位相データが集まる部分である。
3. この試行実験における「位相が類似する部分」が分析されたことになる。
4. また、青丸の部分は位相としてロバストな(強固な)位相データであることが示される。
5. 原画像の加工による赤丸と青丸の位相データのロバスト性の変化を分析・学習し、ロバストな位相データを抽出すれば、画像加工に対して耐性のある位相データが抽出される。

結論

- パーシステントホモロジーという概念をCNN中間層データに用いてアルゴリズムが変化しない知覚ハッシュ関数の生成法を提案した。

- 実験ではパーシステントホモロジーの計算ソフトウェアである**HomCloud**の導入と実際に使用できることを確認できた。

考察

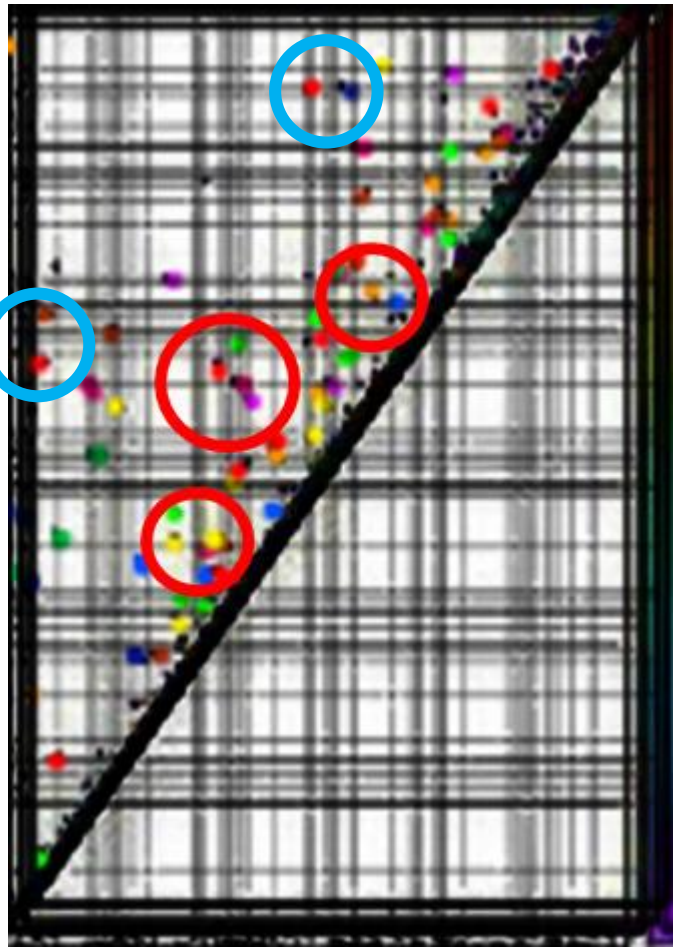
- 実際に機械学習をするためにはPooling層のすべての可視化された画像をPD図として計算する必要があると考えられる。

- もう一方で、原画像に基づくPooling１層目の１０枚の画像と加工・編集を行ったPooling１層目の１０枚の画像を各々のPD図化し、比較してみるという実験も考えられた。

今後の課題

- 入力画像データにおいて出力された中間層のPooling層データをすべてPD図化し、機械学習により知覚ハッシュ値になり得るパラメータを抽出する。

結果



1. 左図は、1枚の限画像につき、CNN第一中間層10枚のPD図の位相データそれぞれに10色で着色し、重ねたPD図である。
2. 対角線部分の位相データはノイズと見做される。
3. 赤丸で囲った部分は6色以上の位相データが集まる部分である。
4. この試行実験における「位相が類似する部分」が分析されたことになる。
5. また、青丸の部分は位相としてロバストな(強固な)位相データであることが示される。
6. 原画像の加工による赤丸と青丸の位相データのロバスト性の変化を分析・学習し、ロバストな位相データを抽出すれば、画像加工に対して耐性のある位相データが抽出される。

背景

近年ネットワーク上に様々なデジタルコンテンツが流通している。

サイトによる著作権法違反やコミックマーケットにおけるコンテンツの適切な二次利用の問題などが生じてきた。

コンテンツの著作権保護が必要不可欠となってきている。

動向

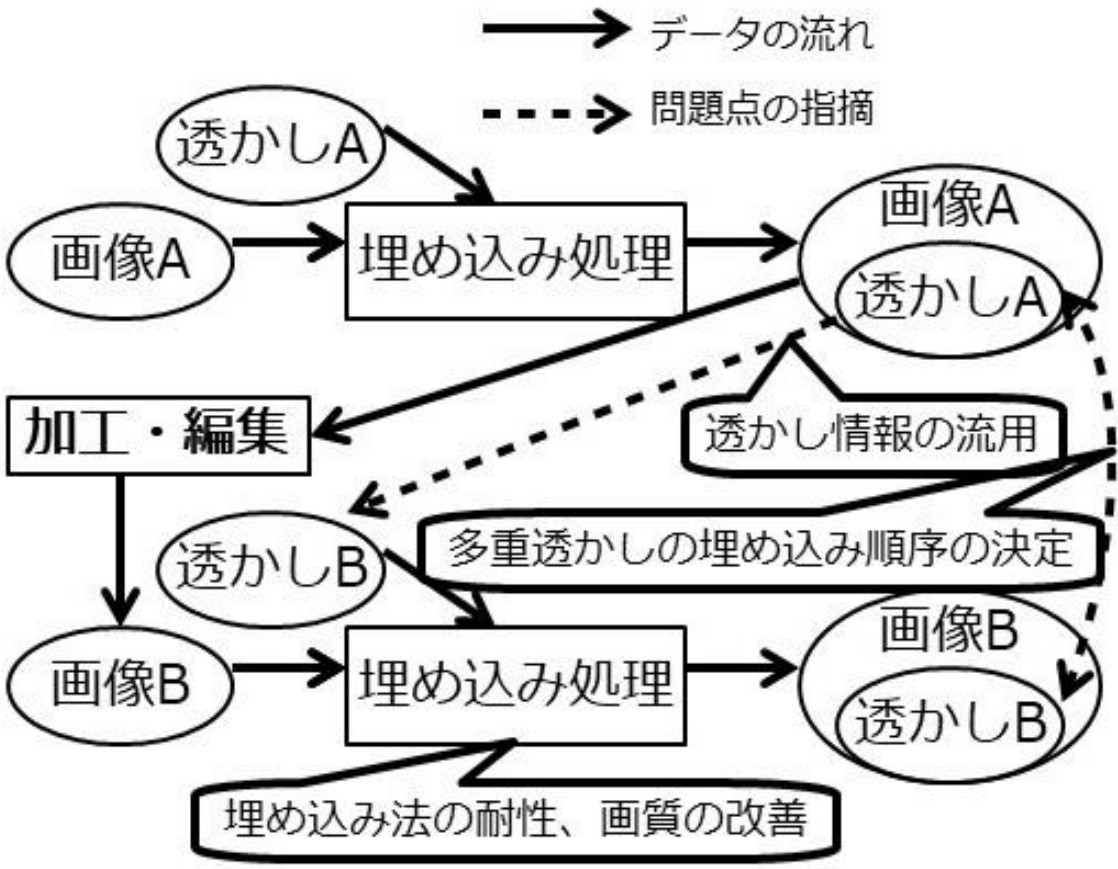
コンテンツを保護する手段としてはアクセス制御、暗号化などの秘匿による方法と権利者を示す改ざんできない証拠を残す方法がある。

画像や動画などのメディアに対して証拠を残す方法として電子透かしという技術がある。

問題点

一般的な電子透かしでは透かし情報がコピーされて他のコンテンツに流用される可能性がある。

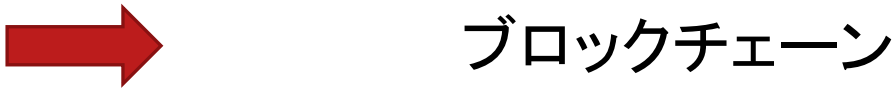
二次利用により多重に埋め込まれた電子透かしの優先順位や加工内容との対応関係を明確にできない。



問題点

コンテンツに応じた固有の情報を生成して流用を防いでいたが、それを様々な手法で加工するとその種類に応じて情報が異なってしまう。

信頼できる第三者が透かし情報を管理する方法が考えられるが、コストやプライバシー保護、セキュリティなどの点からあまり望ましくない。



ベイズの定理

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

P(A|B):事象Bが起こった状況下で事象Aが起こる確率

P(A):事象Aが起こる確率

P(B):事象Bが起こる確率

P(B|A):事象Aが起こった状況下で事象Bが起こる確率

ベイズの定理

$$\text{事後確率} = \text{事前確率} \times \frac{\text{ある場合においての、そのデータが得られる確率}}{\text{そのデータが得られる確率}}$$

進歩状況

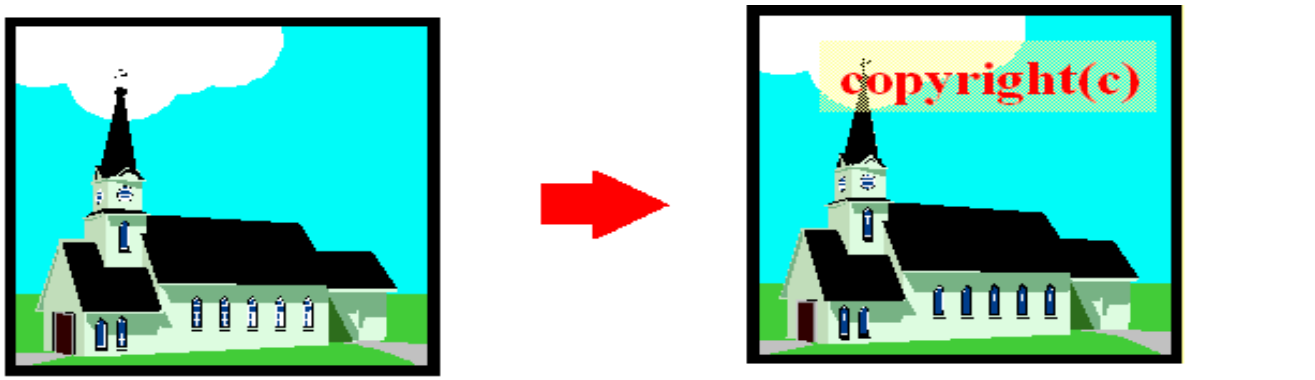
OS : Ubuntu 18.04

仮想環境 : Anaconda

ソースコード :
https://qiita.com/NoriakiOshita/items/005bb17793f15bcb48b8

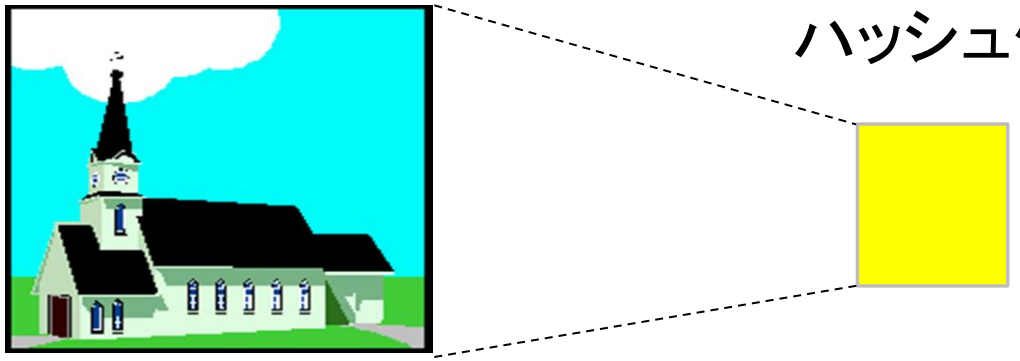
電子透かし

画像などのデジタルコンテンツに情報を埋め込む情報技術のことであり、具体的にはネット上の画像などの著作権保護のために使われる技術である。



普段，電子透かしは見えないが　　実は著作権情報が埋め込まれている

Hash



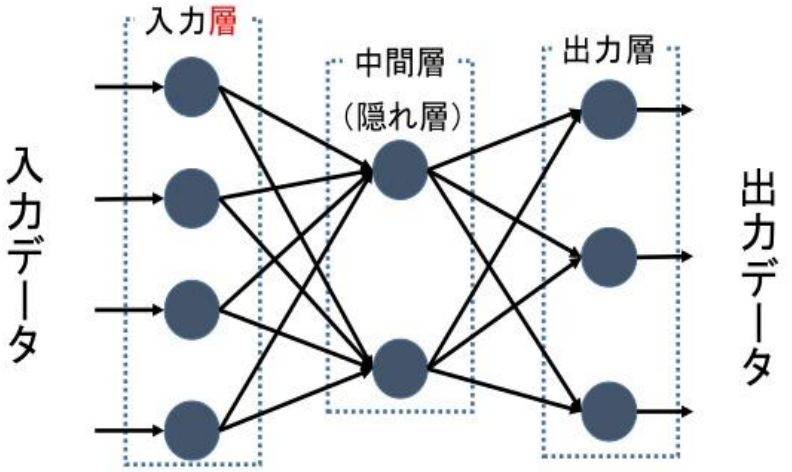
- ハッシュ値から元のデータを特定することはできない

元のデータが同じなら生成されるハッシュ値も同じ
元のデータが少し変わると生成されるハッシュ値は変わる

ニューラルネットワーク

機械学習と呼ばれる手法の1つであり、人間の脳内にある神経細胞（ニューロン）とそのつながり、つまり神経回路網を人工ニューロンという数式的なモデルで表現したもの。

ニューラルネットワークの基本構造



＊中間層は複数あっても良いが、多層になると学習が進みにくいという特徴がある。
＊中間層のユニット数は自由に調整できるが、多すぎても少なすぎてもダメだ。

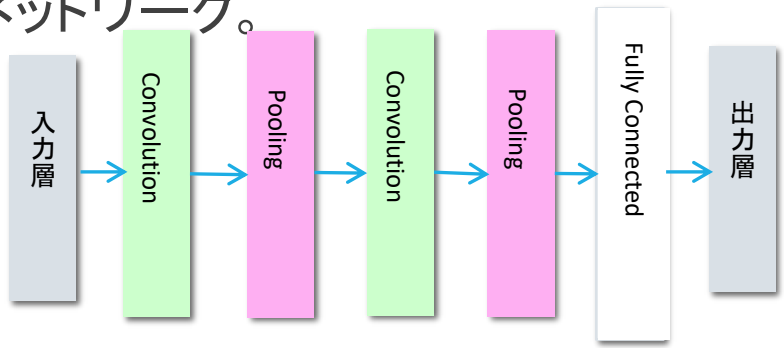
Keras

機械学習のライブラリであり、Python（言語）で書かれたTensorFlow（様々な機械学習の分野で使用するためのオープンソフトウェアライブラリ）などで実行可能なニューラルネットワークライブラリである。

→比較的短いソースコードで実装することが可能。

KerasのCNN（畳み込みニューラルネットワーク）

CNNはニューラルネットワークの中間層の部分に畳み込み層(Convolution層)とプーリング層(Pooling層)を組み込んで構成されるニューラルネットワーク。



畳み込み層(Convolution層)は画像内にある小領域を設けて特徴量のまとまりを作るフィルタのような処理を実施する。

Pooling層で特徴量を圧縮することで、画像の移動や変形に対して影響を受けにくくし、計算量を下げる。