修士論文 要旨

匿名化された顔画像のデータ利活用手法に関する研究

数理情報学専攻 48166222　出町 彰啓
指導教員　中川 裕志 教授

1　背景

近年，データサイエンス分野の研究の発展が著しい．データから知見を見つけ出すデータサイエンスは魅力的である一方，データサイエンスで用いられるデータには個人に関わる情報が含まれることも多い．そのようなデータを扱うにあたってプライバシの問題は避けては通れない．本研究では特に顔画像データの匿名化に関して議論を行う．

顔画像データは表情，年齢層や性別といった有益な情報を含むデータであり，様々なアプリケーションのために収集され利用される．顔画像データの利活用例としては例えばビジネスでの利活用が考えられる．店舗に設置されたカメラの映像などから顧客の表情や年齢層などを読み取りビジネスに応用することが考えられる．

以上のような有用性の一方で，顔画像の利活用には被写体のプライバシの問題を考える必要がある．上記のような利活用にはデータ公開の形を考える必要があり，匿名化加工を施すアプローチによる研究が存在する．顔画像の匿名化加工の研究は k-匿名化をもとになされている．k-匿名化することにより，法律などの規制を順守したうえで自由にデータのやり取りを行えることが期待されている．例えば，ビジネスにおける利活用では，店舗が集まるモールで各店舗のカメラの映像を匿名化することで共有することが可能となり，モール全体での大まかな人の流れや顧客層の分析や顧客の感情分析が行えるようになる．

2　顔画像データの匿名化手法

2.1　画像における k-匿名

匿名化の研究として k-匿名という概念が知られている．ここでは画像データにおける k-匿名を定義する．

定義 1 (画像版 k-匿名)**.**
M 次元のベクトルに直した画像を N 枚並べたデータ行列 $X_{ano} \in \mathcal{R}_+^{N\times M}$ を考える．X_{ano} が k-匿名であるとは，X_{ano} の任意の画像 $\vec{x} \in \mathcal{R}_+^{1\times M}$ に対して，自身も含めて少なくとも k 枚の完全に一致する画像が X_{ano} に存在することを指す．

2.2　Mondrian

Mondrian [3] は k-匿名加工を行う Top down 型のアルゴリズムの一種である．Mondrian は軸を選んでデータを分割していくアルゴリズムである．初期状態として，全データが区別のつかない状況を考える．これは，データ数を n としたとき，n-匿名が成立している状態を指す．そしてある軸を選び，その軸の中央値でデータを二つに分割する．分割によって得られた各部分集合に対して再帰的に分割の処理を行うことで，データ集合を徐々に細かくしていき，最終的にどの軸で分割しても k-匿名を満たさなくなることが判明した時点でアルゴリズムは終了する．

2.3　NMF

Non-negative Matrix Factorization(NMF) [2] は非負値を取る行列を二つの非負値行列に分解する．非負値行列 $X \in \mathcal{R}_+^{N\times M}$ を二つの非負値行列 $T \in \mathcal{R}_+^{N\times L}$, $V \in \mathcal{R}_+^{L\times M}$ に分解することを考える．L は行列分解のランクを表す．NMF は以下のように定式化される:

$$\min_{T,V} \quad \sum_{n,m}(x_{nm} - \sum_{l} t_{nl}v_{lm})^2 \quad s.t. \quad t_{nl}, v_{lm} \geq 0.$$

局所解を得るアルゴリズムとして，以下の更新式に基づく反復アルゴリズムが知られている．T_t,V_t を t 反復目における T,V の値として，

$$T_{t+1} = T_t \odot (XV_t^\top) \oslash (T_tV_tV_t^\top)$$
$$V_{t+1} = V_t \odot (T_{t+1}^\top X) \oslash (T_{t+1}^\top T_{t+1}V_t)$$

で T,V を更新する．$\odot$ と $\oslash$ は要素ごとの掛け算と割り算を表す．

2.4　提案手法の概要

内包する構造を保持した顔画像の匿名化のため，以下のような三段構えのアルゴリズムを提案する．

Algorithm 1 提案手法の概要

1: NMF でデータ行列 X を T と V に分解.
2: T に対して k-匿名化手法を適用し T_{ano} を作成.
3: NMF の更新式で V を V_{ano} に更新.

内包する構造は NMF で V の基底として得られており，それは保持した状態で T を k-匿名化しているため，最終的に得られる加工行列（$T_{ano}V_{ano}$ とする）は内包する構造を保持できていると考えられる．

2.5 k-匿名性の確認

提案手法が k-匿名を満たしていることを確認する．

定理 2 (k-匿名行列の性質)**.**
行列 $T_{ano} \in \mathcal{R}_{+}^{N\times L}$ が k-匿名であるとする．任意の行列 $Y \in \mathcal{R}_{+}^{L\times M}$ に対して $T_{ano}Y$ は k-匿名である．

定理 2 の Y に V または V_{ano} を代入することで，提案手法における $T_{ano}V$ や $T_{ano}V_{ano}$ が k-匿名を満たすことが分かる．

2.6 数値実験

提案手法の有用性を評価するため実際の顔画像データを匿名化する実験を行った．*Labeled Faces in the Wild* という顔認識などの分野で利用されている顔画像データセットを用いた [1]．データ行列 X を k-匿名化した．比較した手法は直接匿名化する手法，PCA を用いた既存手法 k-same [4] と提案手法である．それぞれで作成された加工行列を X_{ano}，X_{same} と $T_{ano}V_{ano}$ とする．k-匿名化手法は Mondrian を利用した．図 1 と図 2 から直接匿名化すると顔の構造が維持できないが，提案手法では維持できていることが分かる．なお，k-same でも顔の構造を維持できる．図 3 と図 4 は Mondrian の軸の選び方を分散で選んだ場合とランダムに選んだ場合における，X との二乗誤差を表した図である．k-same と提案手法の比較に関しては，分散で軸を選ぶと k-same がよく，ランダムに選ぶと提案手法が良い手法であることが分かる．

図 1. X_{ano} 画像

図 2. $T_{ano}V_{ano}$ 画像

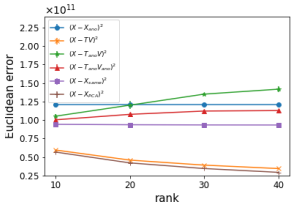

図 3. 誤差の比較
分散で軸選択

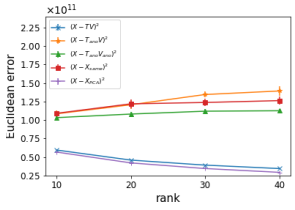

図 4. 誤差の比較
random 軸選択

3 匿名化された顔画像の利活用

匿名化された顔画像は k-匿名というプライバシ保証が与えられる．一方で，匿名加工はオリジナルの顔画像が持っていた情報を欠落させる．そこで，匿名加工された画像で笑顔分類器を構築し，その精度を評価することで匿名加工された顔画像の有用性を評価する．

3.1 理論保証

k-匿名化をはじめとするデータ加工により，SVM の目的関数の最適値及び汎化精度がどの程度変化するのかについて理論的な評価を与えた．目的関数の最適値の変化は加工による各データの移動を用いて評価した．汎化精度は，leave-one-out-error を用いて評価した．

3.2 数値実験

数値実験では，実際の顔画像データで笑顔分類器を学習した．匿名化前後でどの程度精度変化が起こるのか実験的に評価した．匿名加工後のデータでも十分な精度を保っていることが，図 5 と図 6 から確認できる．

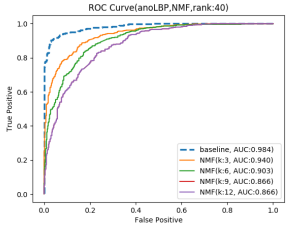

図 5. NMF での精度

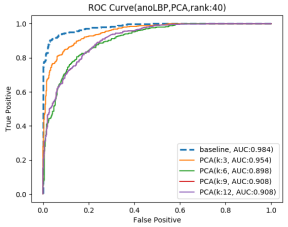

図 6. PCA での精度

4 結論

本研究では，非負性を保証し顔構造を維持できる顔画像の匿名化アルゴリズムを提案した．また，匿名化された顔画像の有用性を笑顔分類器の学習精度により実験的に評価した．加えて，SVM における加工前後での学習結果の変化について理論的に考察した．

参考文献

[1] G. B. Huang and E. Learned-Miller. Labeled faces in the wild: Updates and new reporting procedures. Technical report, University of Massachusetts, Amherst, 2014.

[2] D. D. Lee and H. S. Seung. Algorithms for Non-negative Matrix Factorization. In *Advances in Neural Information Processing Systems 13*, pages 556–562. 2001.

[3] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan. Mondrian multidimensional k-anonymity. In *Proceedings of the 2006 IEEE 22nd International Conference on Data Engineering*, pages 25–35, 2006.

[4] E. M. Newton, L. Sweeney, and B. Malin. Preserving privacy by de-identifying face images. *IEEE transactions on Knowledge and Data Engineering*, 17(2):232–243, 2005.