秘密計算を用いた顔認証の構成について

辻 琉玖
Ruku Tsuji
u220039@st.pu-toyama.ac.jp

富山県立大学 工学部 情報システム工学科

14:50-18:00, Tuesday, Janualy 21, 2025
N516, Toyama Prefectural University

研究の背景

背景

- 近年, 深層学習技術の進展により顔認証の精度が大幅に向上し, イベント会場や入退室管理など多様な場面で利用が進んでいる. しかし, 顔画像は個人を特定できる生体情報であるため, プライバシー保護が重要な課題となっている. 本研究では, 秘密計算を用いて顔画像や認証結果を秘匿した 1 対 1 顔認証システムを提案する.

研究目的

本研究の目的は, 秘密計算を活用して以下を実現することである.

- 入力顔画像やデータベース内の顔画像を秘匿化
- 認証結果のプライバシー保護
- 効率的な計算設定の検討

特に, 特徴量形式や統計的距離計算の影響を評価し, 最適な設定を明らかにすることを目指した.

提案手法 - 概要

1 対 1 秘匿顔認証のフレームワーク

提案手法では, 特徴量抽出に ArcFace, 秘密計算に ABY3 および EzPC を利用する. 顔画像を入力とし, 抽出された特徴量を複数のサーバに分割して秘密計算を行い, 認証結果を得る. 図 1 にシステム全体の構成を示す.

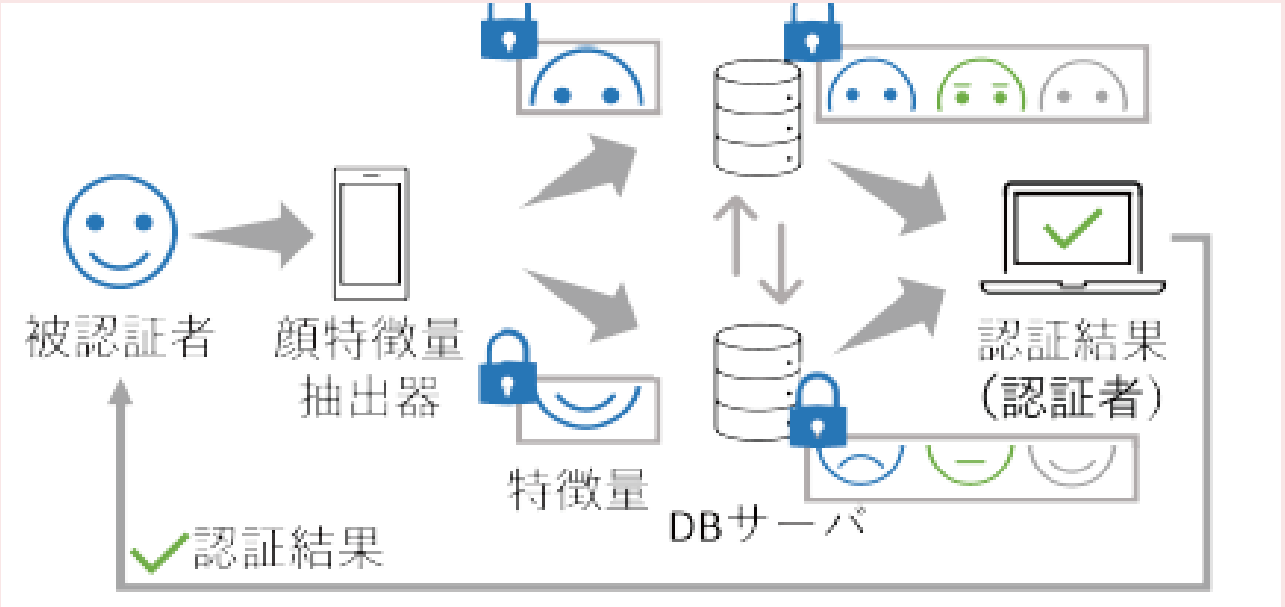

図 1: 提案システムの構成図

提案手法 - 概要

特徴量形式と統計的距離の設定

以下の特徴量形式を検討した：

- 実数値
- 整数値
- バイナリ値

統計的距離の計算には，コサイン類似度，ユークリッド距離，ハミング距離を使用した．統計的距離計算の数式は以下の通りである：

$$\text{コサイン類似度：} \quad \mathrm{sim}(\mathbf{u},\mathbf{v}) = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}, \tag{1}$$

$$\text{ユークリッド距離：} \quad d(\mathbf{u},\mathbf{v}) = \sqrt{\sum_{i=1}^{n}(u_i - v_i)^2}, \tag{2}$$

$$\text{ハミング距離：} \quad d_H(\mathbf{u},\mathbf{v}) = \sum_{i=1}^{n}\mathbf{1}(u_i \neq v_i). \tag{3}$$

評価実験

実験設定

データセット：Faces_Emore を訓練用に, CFP_dataset と FaceScrub を評価用に利用した.
実験環境：特徴量抽出には ResNet50, 秘密計算ライブラリとして ABY3 と EzPC を使用した.

評価方法

提案手法の性能を以下の指標で評価した：

- 認証精度
- 計算時間

実験結果

計算時間の評価

特徴量形式ごとの計算時間を比較した結果, 整数値形式を用いた場合に最も高速な処理が可能であることが確認された（例：次元数 128 の場合, 計算時間は約 6ms）. 図 2 および図 3 に計算時間の比較結果を示す.

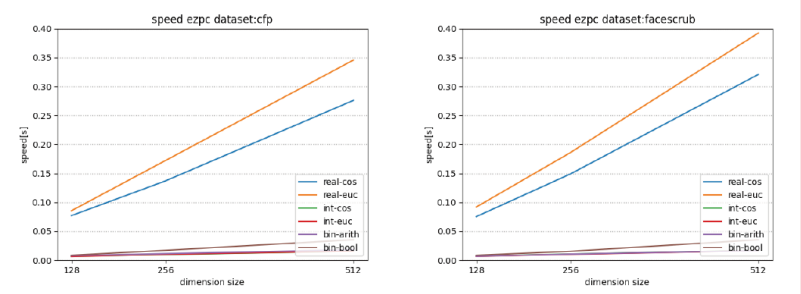

図 2: EzPC を用いた計算時間

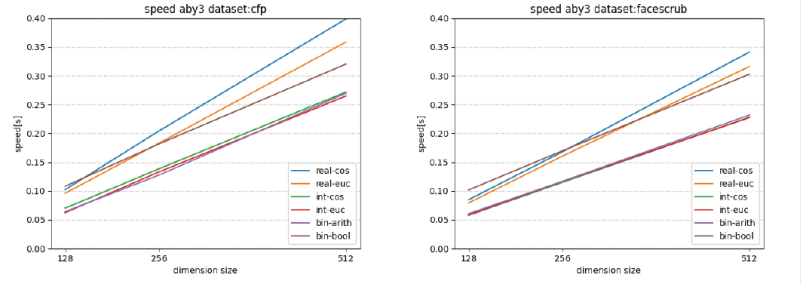

図 3: ABY3 を用いた計算時間

実験結果

認証精度の評価

実数値形式とコサイン類似度の組み合わせが最も高い精度を示したが, 整数値形式でもほぼ同等の精度を達成した. バイナリ値形式では精度がやや低下した。表 1 に認証精度の結果を示す.

表 1: 秘密計算を用いた顔認証精度

特徴量の形式	統計的距離の計算	データセット	特徴量の次元数ごとの精度					
			128 次元		256 次元		512 次元	
			平文	秘匿化	平文	秘匿化	平文	秘匿化
実数値	コサイン類似度	FaceScrub	0.9475	0.9475	0.9542	0.9542	0.9697	0.9697
		CFP_dataset	0.8787	0.8789	0.8710	0.8709	0.8913	0.8910
	ユークリッド距離	FaceScrub	0.9279	0.9278	0.9273	0.9273	0.9508	0.9508
		CFP_dataset	0.8014	0.8014	0.7973	0.7973	0.7996	0.7994
整数値	コサイン類似度	FaceScrub	0.9475	0.9475	0.9537	0.9537	0.9691	0.9691
		CFP_dataset	0.8786	0.8786	0.8729	0.8729	0.8907	0.8907
	ユークリッド距離	FaceScrub	0.9294	0.9293	0.9255	0.9252	0.9501	0.9496
		CFP_dataset	0.7717	0.7716	0.7817	0.7817	0.7819	0.7819
バイナリ値	ハミング距離	FaceScrub	0.8562	0.8562 0.8562(B)	0.9028	0.9028 0.9028(B)	0.9380	0.9380 0.9380(B)
		CFP_dataset	0.8251	0.8251 0.8251(B)	0.8444	0.8444 0.8444(B)	0.8587	0.8587 0.8587(B)

まとめ

本研究では, 1 対 1 秘匿顔認証システムの設計と評価を行い, 以下の知見を得た：

- 整数値形式とコサイン類似度が計算効率と精度の両面で優れる.
- 秘密計算を用いても実用的な高速処理が可能.

今後は, 他の機械学習モデルやバイナリ形式に適した最適化の検討が必要である.