

卒業論文概要書

Summary of Bachelor's Thesis

Date of submission: 02/01/2025 (MM/DD/YYYY)

学科名 Department	情報通信	氏名 Name	藤浪 優里佳	指 導 教 員 Advisor	渡辺 裕 印
研究指導名 Research guidance	オーディオビジュアル 情報処理研究	学籍番号 Student ID number	1W212339-4		
研究題目 Title	プロンプトベースの画像符号化による符号化顔画像の認識精度評価 Evaluation of Recognition Accuracy of Coded Face Images Using Prompt-Based Image Coding				

1. まえがき

近年、拡散モデルを用いた画像生成の研究が急速に進んでいる。テキストから画像、あるいはその他のプロンプトから画像への変換が主な処理である。中でも顔画像の生成においては、多くのモデルが研究され、多様で高品質な顔画像が得られている。特に、画像からプロンプト、エッジ、色情報を抽出するプロンプトベースの画像符号化方式は、顔画像の再現性に優れている。

本研究では、プロンプトに基づく画像符号化によって得られた顔画像が、顔画像認識システムに入力されたときに、どの程度の類似度で真偽判定されるかを検討する。また、Stable Diffusionによって生成された顔画像を判定する場合の、DeepFaceの顔検出器と認識モデルの適切な組み合わせも検討する。

2. 関連研究

2.1 プロンプトベースの画像符号化

プロンプトベースの画像符号化は拡散モデルに基づく手法である[1][2]。これは、プロンプト抽出とエッジ検出、色検出を組み合わせ、拡散モデルに特定の埋め込み最適化を行うことで、画像圧縮を実現する。生成される顔の特徴は、拡散モデルに採用されている Stable Diffusion 学習済みモデルの影響を強く受ける。さらに、エッジ情報が十分でない場合には、顔パーツの形状が多様に生成される。

2.2 DeepFace

DeepFace[3]は、最先端の顔認識フレームワークで、顔検出器と顔認識モデルから構成される。まず初めに検出器を用いて画像の顔領域以外の部分を破棄する。次に、目の位置に二つの角を持つ直

角二等辺三角形を構成して、特徴点の位置を基に、顔の位置合わせを行う。そして特徴点からベクトルを返すことで、元画像と比べたい画像の二つのベクトル間の距離を求め、類似度が判定される。特徴点には、目や鼻、口の視点と終点などが含まれ、個人識別に利用されている。

3. Stable Diffusion におけるエッジ制御

プロンプトベースの画像符号化では、エッジ抽出のため、Canny エッジ検出器を使用する。エッジの情報量は、Canny エッジ検出の二つの閾値によって制御できる。初めに、第一閾値以上のエッジを主要エッジとして抽出する。次に、主要エッジに接続された、第二の閾値以上のエッジを保持する。第二閾値は信頼度の低いエッジ部分に対して用いられる。したがって、第一の閾値が大きいほど、抽出するエッジの情報量は少なくなる。Canny エッジが Stable Diffusion で画像を生成する際に使用される場合、エッジは生成画像の境界を拘束し、その形状を保持する。一方、テクスチャはプロンプトとハイパーパラメータによって指定された条件に従って拡散モデルによって生成される。

4. 実験

本実験では、データセットとして(A) Male and Female faces dataset [4], (B) DeepFace dataset [3], (C) Face Research Lab London set [5] の三つを用いる。それぞれのデータセットから無作為に 20 枚ずつ顔画像を選び、男女 30 枚ずつ、計 60 枚を使用する。同一人物判定の処理過程を図 1 に示す。データセットから得られる画像それぞれから、閾値の異なる 5 種類のエッジを抽出し、Stable Diffusion により、再現度の異なる 5 種類の画像を得る。生成

表 1 エッジ情報ごとの DeepFace の True rate

Dataset	True rate [%]				
	100_100	100_150	100_200	100_250	100_300
A	100	100	85	75	55
B	95	90	80	60	50
C	85	85	75	70	35

表 2 顔認識モデルごとの非類似度

Model	Threshold	Dissimilarity
VGG-Face	0.68	0.677
FaceNet	0.40	0.516
FaceNet512	0.30	0.548
Dlib	0.07	0.073
ArcFace	0.68	0.681
SFace	0.59	0.654
GhostFaceNet	0.60	0.716
DeepID	0.02	0.034
OpenFace	0.10	0.263

画像を元画像と共に、DeepFace に入力し、同一人物かどうかを判定する。この際、DeepFace はデフォルトの設定として顔検出器に OpenCV を、認識モデルに VGG-Face を使用する。生成画像は、エッジの情報量によって元画像からの再現度が変化する。

生成画像と元画像の人物が同一であると判定された割合を表 1 に示す。エッジの情報量が少ない場合には、同一人物ではないと判定される可能性が示唆された。一方で情報量が多くなると、同一人物であると判定される割合が高くなった。つまりエッジの情報量の変化が、認識精度に大きな影響を与えることが確認された。

DeepFace は顔検出器と認識モデルから構成されている。そこで、今回の方法で生成した画像を判別するために最適な認識モデルを検討した。検出器を OpenCV に固定し、顔認識モデルを変化させた判定精度を表 2 に示す。ここで Threshold は、DeepFace の認識モデルが二つの画像が同一人物か否かを判定するための基準値である。この基準値はモデルによって異なる。表 2 から、モデルによって判定にばらつきが生じることがわかる。

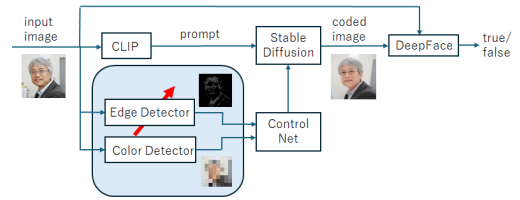


図 1 Stable Diffusion と DeepFace の処理過程[6]

したがって本実験により、生成画像の特性や生成方法によって顔認識モデルを適切に選択することが顔画像認識モデルを実用化する際に有効である可能性が示唆された。

5. 結論

本研究では、プロンプトベースの画像符号化によって生成された顔画像がどの程度の類似度で真偽判定されるかを検討した。また、プロンプトベースの画像符号化によって生成された顔画像を適切に判別するための顔検出器と認識モデルの組み合わせを検討した。

顔認識システムにおいてエッジの情報は重要であると言え、敵対的な攻撃に対して脆弱であると考えられる。さらに今回の実験から、認識モデルによって判定にはばらつきがあるため、実用化の際には適切にモデルを選択する必要があると推察される。

参考文献

- [1] H. Watanabe, L. Jin, T. Hayami, T. Chujoh, T. Aono, Y. Yasugi, S. Hong, Z. Fan, and T. Ikai, “Prompt-based Image Coding with Edge Information,” 2023 Picture Coding Symposium, 画像符号化シンポジウム (PCSJ/IMPS2023), P1-12, Nov. 2023.
- [2] H. Watanabe, L. Jin, T. Hayami, T. Chujoh, Y. Yasugi, S. Hong, Z. Fan, and T. Ikai, “Prompt-based Image Coding with Edge and Color Information,” 電子情報通信学会総合大会, D-11A-27, Mar. 2024.
- [3] S. Serengil, A. Özpınar, “LightFace: A Hybrid DeepFace Recognition Framework,” IEEE Innovations in Intelligent Systems and Application Conference (ASYU) 2020, pp.1-5, Oct 2020.
- [4] Ashwin Gupta, Male and female faces dataset, <https://www.kaggle.com/datasets/ashwingupta3012/male-and-female-faces-dataset>
- [5] Lisa DeBruine, Benedict Jones, Face Research Lab London, https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666
- [6] Yurika Fujinami, Hiroshi Watanabe: “Adversarial Level of Face Images Generated by Prompt-based Image Coding in Face Recognition System,” 2024 IEEE 13th Global Conference on Consumer Electronics (GCCE 2024), P2-05, Oct. 2024.

2024 年度 卒業論文

プロンプトベースの画像符号化による符号化顔画像の
認識精度評価

Evaluation of Recognition Accuracy of Coded Face Images Using
Prompt-Based Image Coding

指導教員 渡辺裕 教授

提出日：2025 年 2 月 1 日

早稲田大学 基幹理工学部 情報通信学科

1W212339-4

藤浪優里佳

目次

第1章 序論.....	1
1.1 研究背景.....	1
1.2 研究目的.....	1
1.3 本論文の構成.....	1
第2章 関連研究.....	3
2.1 まえがき.....	3
2.2 Stable Diffusion.....	3
2.3 プロンプトベースの画像符号化.....	3
2.4 DeepFace.....	3
2.5 CLIP.....	4
2.6 むすび.....	4
第3章 実験結果と考察.....	5
3.1 まえがき.....	5
3.2 データセット.....	5
3.3 実験.....	5
3.4 実験結果.....	6
3.5 考察.....	8
3.6 むすび.....	8
第4章 実験結果と考察.....	10
4.1 まえがき.....	10
4.2 データセット.....	10
4.3 実験.....	10
4.4 実験結果.....	10
4.5 考察.....	11
4.6 むすび.....	12
第5章 結論と今後の課題.....	13
5.1 結論.....	13
5.2 課題.....	13
謝辞.....	14
参考文献.....	15
表一覧.....	17
図一覧.....	18
研究業績.....	19

第 1 章 序論

1.1 研究背景

近年、拡散モデルに基づく画像生成手法の研究開発が急速に進んでいる。その手法の主な処理は、テキストからプロンプト、あるいはプロンプトから画像への変換である。特に顔画像の生成においては、多くのモデルが研究され、多様で高品質な顔画像が得られている。一方、画像、プロンプト変換の結果を利用して、低ビットレートでの画像符号化を実現する手法も確立されつつある。特に、画像からプロンプト、エッジ、色情報を抽出するプロンプトベースの画像符号化方式は、顔画像の再現性に優れている。

また、CNN を用いた手法は、顔画像認識システムの中で高い認識精度を達成しており、社会インフラとして様々な応用が提案されている[1][2]。

1.2 研究目的

顔認識技術は急速に進化し、効率的で精度が向上している一方、外部からの操作に対して脆弱である。顔認証技術を用いたシステムを攻撃する方法の一つとして、敵対的な画像を利用するものがある。認識モデルを欺くために意図的な操作が加えられた画像は、機械学習モデルによって誤分類される可能性がある。

そこで、拡散モデルに基づく画像生成手法によって生成された顔画像が、顔認識システムにおいてどのような性質を持つかが重要な検討課題となっている。本研究では、プロンプトに基づく画像符号化によって得られた顔画像が、顔画像認識システムに入力されたときに、どの程度の類似度で真偽判定されるかを検討する。特に、顔画像のエッジの情報量を制御することが、分類にどのような影響を与えるかを調査する。また、Stable Diffusion によって生成された顔画像を判定する場合の、DeepFace の顔検出器と認識モデルの適切な組み合わせも検討する。

1.3 本論文の構成

本論文の構成を以下に示す。

第 1 章では本研究の研究背景、研究目的について述べる。

第 2 章では本研究で用いる関連研究について述べる。

第 3 章では本研究の提案手法について述べる。

第 4 章では実験の結果及び考察について述べる

第 5 章では本論文の結論及び今後の課題について述べる.

第2章 関連研究

2.1 まえがき

本章では、画像生成技術である Stable Diffusion、入力顔画像から擬似顔生成の応用を提供するプロンプトベースの画像符号化、顔認識システムである DeepFace、マルチモーダル学習モデルである CLIP について説明する。

2.2 Stable Diffusion

Stable Diffusion は、拡散モデルに基づく画像生成技術の一つであり、特に高解像度な画像生成において優れた性能を発揮する。ノイズを含んだ画像から、潜在空間でノイズを除去していくため、計算コストが大幅に削減されている。また、入力条件に基づいた画像を生成することができる。入力条件としてプロンプトやエッジ情報、色情報などを使用することで、多様な画像の生成が可能になる。

2.3 プロンプトベースの画像符号化

プロンプトベースの画像符号化は拡散モデルに基づく手法である[3][4]。これは、プロンプト抽出とエッジ検出、色検出を組み合わせることで、画像圧縮のために拡散モデルに特定の埋め込み最適化を行うものである。Stable Diffusion web UI では、ControlNet によってこれらが可能になっている。生成される顔の特徴は、拡散モデルに採用されている Stable Diffusion の学習済みモデルの影響を強く受ける。さらに、エッジ情報が十分でない場合には、顔パーツの形状が多様に生成される。

エッジの情報量は、Canny エッジ検出の二つの閾値によって制御することができる。Canny エッジ検出では、ノイズを除去した後、明るさの変化を計算して閾値によってエッジを決定する。二つの閾値のうち、高い閾値は確実にエッジである部分を選ぶ基準となる。低い閾値は信頼度の低いエッジ部分に対して用いられ、周囲のエッジ領域を参照しつつ、その閾値と的大小を比較することで、エッジか否かを識別する。

2.4 DeepFace

DeepFace は、最先端の顔認識フレームワークであり、顔検出器と顔認識モデルから構成

されている[5]. まず初めに検出器を用いて画像の顔領域以外の部分を破棄する. 次に, 目の位置に二つの角を持つ直角二等辺三角形を構成して, 特徴点の位置を基に, 顔の位置合わせを行う. そして特徴点から, それらの情報を含んだ特徴量ベクトルを返すことで, 元画像と比べたい画像の二つのベクトル間の距離を求め, 類似度が判定される. この特徴点には, 目や鼻, 口の視点と終点などが含まれ, 個人識別に利用されている. 数値で特徴を表すことで, DeepFace で扱えるようになる.

2.5 CLIP

CLIP[10]は, OpenAI によって提案されたマルチモーダル学習モデルであり, 画像とプロンプトの対応関係を学習するために設計されている. まず, 入力されたプロンプトと Diffusion モデルが生成する画像の双方を特徴量ベクトルに変換する. 二つの特徴量ベクトルを比較し, 一致度を算出することで, 画像がどれくらいプロンプトと類似しているかを評価する. この評価スコアを基に, プロンプトに合った画像を生成するように Diffusion モデルの調整を繰り返す. この過程を経て, 高精度な画像生成が実現されている.

2.6 むすび

本章では, 画像生成技術である Stable Diffusion と本研究に関連するプロンプトベースの画像符号化, 顔認識システムである DeepFace, マルチモーダル学習モデルである CLIP について説明した.

第3章 実験結果と考察

3.1 まえがき

本章では、実験の概要、結果及び考察について述べる。まず、本実験で使用するデータセット、実験方法について述べ、その実験結果を示す。

3.2 データセット

本実験では、データセットとして Male and Female faces dataset [6], DeepFace dataset [7], Face Research Lab London set[8] の三つを用いた。画像サイズは 512×512 で、枚数はそれぞれのデータセットから無作為に 20 枚ずつ顔画像を選び、男女 30 枚ずつ、計 60 枚とする。

3.3 実験

Stable Diffusion web UI を用いて、エッジの閾値を変化させることで、全 60 枚の画像からそれぞれ 5 枚の画像を生成する。元画像に近いものが生成されるように、CLIP でプロンプトを生成し、ControlNet で色と輪郭を指定する。エッジ抽出には Canny エッジ検出器を用いる。Canny エッジ検出器は、設定した第一の閾値以上の部分を主要エッジとして抽出し、次に主要エッジに接続された、第二の閾値以上のエッジを保持する。したがって、Canny エッジが Stable Diffusion の ControlNet で使用される場合、エッジが生成画像の境界を拘束し、その形状を保持することができる。一方で、テキストはプロンプトとハイパーパラメータによって指定された条件に従い、拡散モデルによって生成される。図 3.1 に閾値(100, 100), (100, 200), (100, 300)の場合の生成画像の例を示す。括弧内の数値はそれぞれ第一閾値、第二閾値とする。第二閾値を大きくすることで再現度が下がり、自然な表情から不自然な表情へ遷移していることが確認できる。

同一人物判定の処理過程を図 3.2 に示す。生成画像を元画像と共に、顔検出器として OpenCV、認識モデルとして VGG-Face を使用するデフォルトの設定で DeepFace に入力し、同一人物であるかどうかの真偽判定をする。生成画像は、エッジの情報量によって元画像からの再現度が変化する。エッジの情報量に変化する顔画像を DeepFace が判定し、顔認識結果を非類似度として算出し、閾値以下であれば False と判定される。非類似度は顔画像の処理によって変化する。

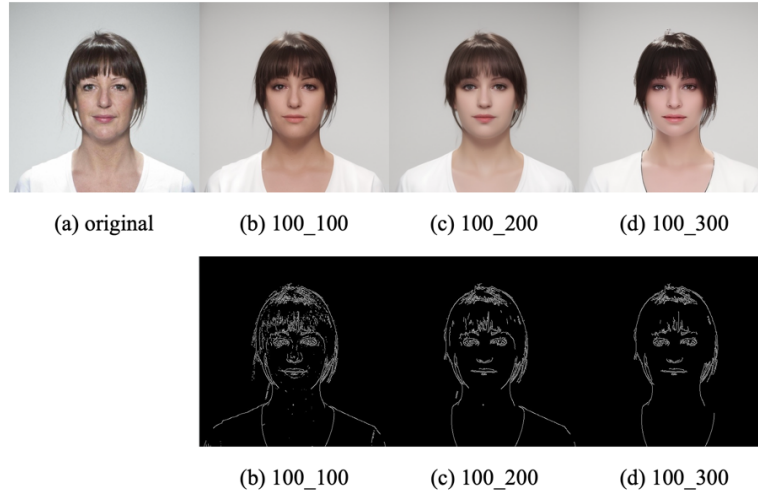


図 3.1 閾値を変化させた時のエッジ画像と生成画像の例 (既発表[27]より転載)

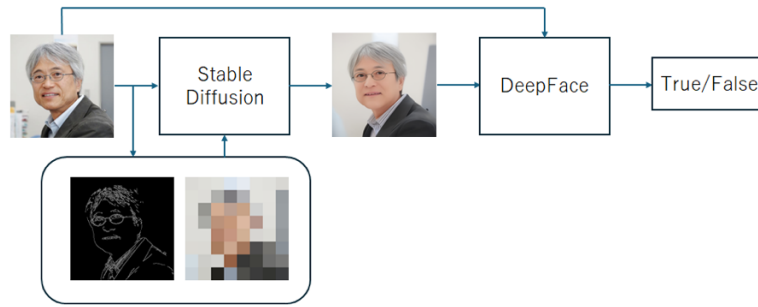


図 3.2 Stable Diffusion と DeepFace による同一人物判定の概要 (既発表[27]より転載.)

3.4 実験結果

生成された画像と元画像の類似度は DeepFace を用いて測定した．結果を図 3.3, 3.4, 3.5 に示す．顔検出器には OpenCV を，認証には VGG-Face を用いた．比較画像 x , y の非類似度 d は式(3.1)のように算出される．

$$d = 1 - \frac{\langle x, y \rangle}{\|x\| \|y\|} \quad (3.1)$$

値が 0 に近いほど，画像同士が似ているとされる．図 3.3, 3.4, 3.5 から，非類似度の値はどのデータセットにおいても，エッジの情報量が増えるにつれて小さくなる傾向にあることがわかる．

また，生成画像と元画像の人物が同一であると判定された割合を表 3.1 に示す．エッジの閾値が低い場合には True rate が高いが，エッジの情報量を減らすと大幅に低下していることがわかった．例えば，Face Research Lab Dataset の場合，閾値(100, 100)のときには True rate

が 85%だったのに対し、閾値(100, 300)の場合には 35%まで低下している。つまり、今回の実験における顔認識精度は最高で 65%であった。

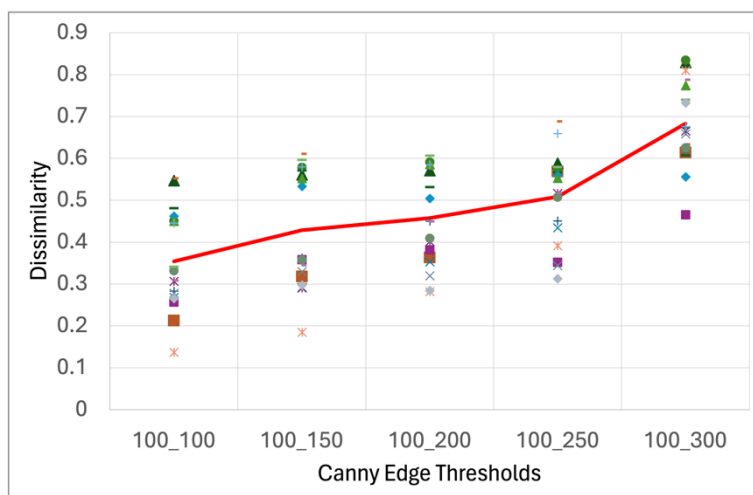


図 3. 3 Male and Female dataset の判定結果 (既発表[27]より転載.)

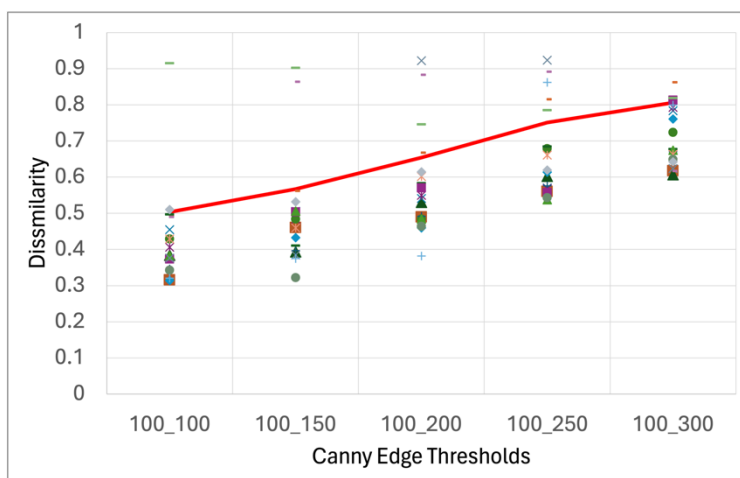


図 3. 4 DeepFace dataset の判定結果 (既発表[27]より転載.)

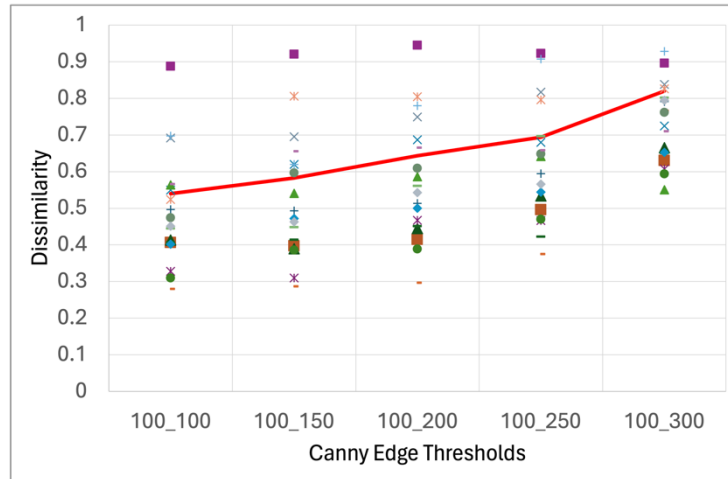


図 3.5 Face Research Lab London set の判定結果 (既発表[27]より転載.)

表 3.1 エッジ情報の異なる画像に対する DeepFace の True rate (既発表[27]より転載.)

Dataset	True rate [%]				
	100_100	100_150	100_200	100_250	100_300
Male and Female [6]	100	100	85	75	55
DeepFace [7]	95	90	80	60	50
Face Research Lab [8]	85	85	75	70	35

3.5 考察

表 3.1 より、エッジの情報量のわずかな変化が、認識精度に大きな影響を与えることが確認できた。これにより、顔認識システムにおいてエッジの情報は重要であるといえ、敵対的な攻撃に対して脆弱であると考えられる。また、DeepFace の顔認識精度は 97%を超えると記述もあるが[9]、表から読み取れるように、本実験ではそこまでの精度が認められなかった。大抵の画像が本人であると認識されてしまったからである。したがって、プロンプトベースの画像符号化を利用して生成された敵対的な画像を扱う場合には、類似性を評価する方法が適切でない可能性がある。顔認識モデルが適切に類似性を評価する方法は、画像の生成方法によって異なると考えられる。

3.6 むすび

本章では、プロンプトベースの画像符号化によって生成された顔の敵対的レベルを示す。実験結果は、エッジの数が非常に削られた場合を除き、DeepFace が実際の顔画像として顔

を認識することを示している。したがって、**Stable Diffusion** で生成された画像を拒否する場合、**DeepFace** をデフォルトの設定で使用するべきではないことがわかる。

第4章 実験結果と考察

4.1 まえがき

第3章では、DeepFaceでの同一人物判定の際に、顔検出器としてOpenCV、認識モデルとしてVGG-Faceを使用した。これは、DeepFaceのデフォルトの設定である。しかし表4.1にあるように、真偽判定の精度は低かった。そこで、本章では顔画像認識システムのモデルと検出器の組み合わせを変え、プロンプトベースの画像符号化により得られた顔画像が、どの程度の類似度で真偽判定されるかを検討する。

4.2 データセット

本実験では、データセットとしてFace Research Lab London set[8]を用いる。画像サイズは512×512で、無作為に男女それぞれ30枚ずつ顔画像を選び、計60枚とする。

4.3 実験

Stable Diffusion web UI を用いて、60枚の画像からそれぞれ生成画像を得る。この時、3章と同様の方法で、Canny エッジの閾値を(100, 200)に固定して生成する。そして、生成画像と元の画像の同一人物判定をDeepFaceによって行う。DeepFaceに対して2通りの設定を試行する。第一に、顔検出器としてOpenCVを固定し、顔認識モデルを変更する。第二に、顔認識モデルをVGG-Faceに固定し、顔検出器を変更する。各モデル設定における類似度評価を比較し、変更が同一人物判定にどのような影響を与えるかを調査する。

4.4 実験結果

非類似度の平均値とFARスコアの実験結果を表4.1, 4.2に示す。ここでThresholdは、DeepFaceの認識モデルが二つの画像が同一人物か否かを判定するための基準値である。この基準値はモデルによって異なる。ここで、FARスコアは生成画像を本人であると誤認識してしまう割合のことである。顔認識モデルを変えると同じ画像でも、真偽判定にばらつきが生じた。表4.1に示すように、今回の方法で生成した画像はDlib[10]で判定した場合に最も誤った判定が多かった。最も正しい判定が多かったGhostFaceNet[13]とは2倍以上の差

があることが読み取れる。また、表 4.2 より、検出器による精度の違いはあまり見られなかった。

表 4.1 顔認識モデルを変化させた際の非類似度の平均値と FAR スコア

Model	Threshold	Dissimilarity	FAR
VGG-Face [7]	0.68	0.677	0.51
FaceNet [8]	0.40	0.516	0.58
FaceNet512 [9]	0.30	0.548	0.40
Dlib [10]	0.07	0.073	0.83
ArcFace [11]	0.68	0.681	0.55
SFace [12]	0.59	0.654	0.47
GhostFaceNet [13]	0.65	0.716	0.35
DeepID [14]	0.015	0.034	0.70
OpenFace [15]	0.10	0.263	0.57

表 4.2 顔検出器を変化させた際の非類似度の平均値と FAR スコア(Threshold=0.68)

Detector	Dissimilarity	FAR
OpenCV[16]	0.677	0.51
MtCnn[17]	0.655	0.60
FastMtCnn[18]	0.651	0.61
RetinaFace[19]	0.650	0.60
YuNet[20]	0.651	0.53
CenterFace[21]	0.678	0.61
Yolov8[22]	0.650	0.70
Mediapipe[23]	0.623	0.61
Dlib[24]	0.652	0.53

4.5 考察

表 4.1 より、顔認識モデルによって、判定結果にばらつきが出ることが確認できた。一方で表 4.2 より、顔検出器を変化させても判定結果に大きな変化はなかった。顔検出器は、画像から顔の部分のみを切り抜く役割があるが、認証に直接は関係していないため、このような結果になったと言える。つまり、生成画像の同一人物判定において、顔検出器の選択は特に重要ではないと考えられる。

認証に直接関係する顔認識モデルについては、モデルごとに非類似度の算出方法や学習

方法が異なるため，入力して判定したい画像の特徴によって向き不向きがあると推察される．

4.6 むすび

本章では，顔画像認識システムのモデルと検出器の組み合わせを変え，プロンプトベースの画像符号化により得られた顔画像が，どの程度の類似度で真偽判定されるかを検討した．生成された画像と元画像の非類似度を見ると，認識モデルによって判定結果にはばらつきが生じることがわかった．したがって，生成画像の特性や生成方法によって顔認識モデルを適切に選択することが有効である可能性が示唆された．

第5章 結論と今後の課題

5.1 結論

本論文では、プロンプトベースの画像符号化によって生成された顔画像がどの程度の類似度で真偽判定されるかを検討した。また、プロンプトベースの画像符号化によって生成された顔画像を適切に判別するための顔検出器と認識モデルの組み合わせを検討した。

実験の結果、DeepFace はエッジの数が非常に削られた場合を除いて、生成画像の顔を本物であると認識することがわかった。顔認識システムにおいてエッジの情報は重要であると言え、敵対的な攻撃に対して脆弱であると考えられる。したがって、生成された画像を拒否する場合には、DeepFace をデフォルトの設定で使用するべきではない。さらに今回の実験から、認識モデルによって判定にはばらつきがあるため、実用化の際には適切にモデルを選択する必要があると推察される。

5.2 課題

本研究では、プロンプトベースの画像符号化を利用して生成された画像に関して課題が残されている。まず、エッジ以外の情報を変更または条件付けした生成画像に関して十分な検討がなされていない。色調や照明条件など、エッジ情報以外の変化が画像全体に与える影響についての詳細な評価が必要である。また、現実環境での応用において、敵対的攻撃や異常検出に対するモデルの耐性を検証する必要がある。これらの課題に対して、生成画像の特性をより包括的に評価し、適切な認識モデルの選定や対策手法の開発を行うことで、より実用性の高いシステムへの応用が期待される。

謝辞

本論文の執筆にあたり，丁寧で適切なお指導と研究環境を整えてくださった渡辺裕教授に心より感謝いたします。

また，日頃から相談に応じて助言やご指摘をくださった研究室の皆様にもお礼申し上げます。

最後に，精神面と経済面ともに多くの力添えをしていただいた両親に深く感謝いたします。

参考文献

- [1] F. Vakhshiteh, A. Nickabadi, and R. Ramchandra, "Adversarial Attacks against Face Recognition: A Comprehensive Study," arXiv:2007.11709v3, Feb. 2021.
- [2] Y. Xu, K. Raja, R. Ramchandra, and C. Busch, "Adversarial Attacks on Face Recognition Systems," Springer, Handbook of Digital Face Manipulation and Detection, pp. 139-161, Jan. 2022.
- [3] H. Watanabe, L. Jin, T. Hayami, T. Chujoh, T. Aono, Y. Yasugi, S. Hong, Z. Fan, and T. Ikai, "Prompt-based Image Coding with Edge Information," 2024 画像符号化シンポジウム(PCSJ) / 映像メディア処理シンポジウム(IMPS), P1-12, Nov.2023.
- [4] H. Watanabe, L. Jin, T. Hayami, T. Chujoh, Y. Yasugi, S. Hong, Z. Fan, and T. Ikai, "Prompt-based Image Coding with Edge and Color Information," 電子情報通信学会総合大会, D-11A-27, Mar.2024.
- [5] S. Serengil, A. Özpınar, "A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules," Journal of Information Technologies, Vol.17, No.2, pp.95-107, Mar.2024.
- [6] A. Gupta, Male and female faces dataset, <https://www.kaggle.com/datasets/ashwingupta3012/male-and-female-faces-dataset>
- [7] S. Serengil, A. Özpınar, "LightFace: A Hybrid DeepFace Recognition Framework," IEEE Innovations in Intelligent Systems and Application Conference (ASYU) 2020, pp.1-5, Oct 2020.
- [8] L. DeBruine, B. Jones, Face Research Lab London set, https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666
- [9] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," Conference on Computer Vision and Pattern Recognition, Jun 2014.
- [10] A. Radford, J. W. Kim, C. Hallacy, A. Ramesh, G. Goh, S. Agarwal, G. Sastry, A. Askell, P. Mishkin, J. Clark, G. Krueger, and I. Sutskever, "Learning Transferable Visual Models From Natural Language Supervision," arXiv preprint arXiv:2103.00020, 2021.Y
- [11] K. Balamurali, S. Chandru, M. S. Razvi, and V. Sathiesh Kumar, "Face Spoof Detection Using VGG-Face Architecture," J. Phys.: Conf. Ser., 1917, 012010, Apr. 2021.
- [12] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," arXiv preprint rXiv:1503.03832, 2015.
- [13] D. E. King, "Dlib-ml: A Machine Learning Toolkit," Journal of Machine Learning Research, Vol. 10, pp. 1755-1758, Jul 2009.
- [14] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," Conference on Computer Vision and Pattern Recognition, pp. 4690-4699, Jun 2019.

- [15] Y. Zhong, W. Deng, J. Hu, D. Zhao, X. Li and D. Wen, "SFace: Sigmoid-Constrained Hypersphere Loss for Robust Face Recognition," in *IEEE Transactions on Image Processing*, vol. 30, pp. 2587-2598, 2021
- [16] M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri and N. Werghi, "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations," in *IEEE Access*, vol. 11, pp. 35429-35446, 2023.
- [17] W. Ouyang, P. Luo, X. Zeng, S. Qiu, Y. Tian, H. Li, S. Yang, Z. Wang, Y. Xiong, C. Qian, Z. Zhu, R. Wang, C. Loy, X. Wang, X. Tang, "DeepID-Net: Multi-stage and Deformable Deep Convolutional Neural Networks for Object Detection," *arXiv preprint arXiv:1409.3505*, 2014.
- [18] T. Baltrušaitis, P. Robinson and L. -P. Morency, "OpenFace: An Open Source Facial Behavior Analysis Toolkit," *2016 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1-10, 2016.
- [19] I. Culjak, D. Abram, T. Pribanic, H. Dzapo and M. Cifrek, "A Brief Introduction to OpenCV," *2012 Proceedings of the 35th International Convention*, pp. 1725-1730, 2012.
- [20] N. Zhang, J. Luo, and W. Gao, "Research on Face Detection Technology Based on MTCNN," *2020 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, pp. 154-158, 2020.
- [21] J. Deng, J. Guo, Y. Zhou, J. Yu, I. Kotsia, and S. Zafeiriou, "RetinaFace: Single-stage Dense Face Localisation in the Wild," *arXiv preprint arXiv:1905.00641*, 2019.
- [22] W. Wu, H. Peng, and S. Yu, "YuNet: A Tiny Millisecond-level Face Detector," 2023, <https://doi.org/10.1007/s11633-023-1423-y>
- [23] Y. Xu, W. Yan, H. Sun, G. Yang, and J. Luo, "CenterFace: Joint Face Detection and Alignment Using Face as Point," *arXiv preprint arXiv:1911.03599*, 2019.
- [24] D. Reis, J. Kupec, J. Hong, and A. Daoudi, "Real-Time Flying Object Detection with YOLOv8," *arXiv preprint arXiv:2305.09972*, 2023.
- [25] C. Lugaresi, J. Tang, H. Nash, C. McClanahan, E. Uboweja, M. Hays, F. Zhang, C. Chang, M. G. Yong, J. Lee, W. Chang, W. Hua, M. Georg, and M. Grundmann, "MediaPipe: A Framework for Building Perception Pipelines," *arXiv preprint arXiv:1906.08172*, 2019.
- [26] S. Sharma, K. Shanmugasundaram, and S. K. Ramasamy, "FAREC — CNN based efficient face recognition technique using Dlib," *2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, pp. 192-195, 2016.
- [27] Yurika Fujinami, Hiroshi Watanabe: "Adversarial Level of Face Images Generated by Prompt-based Image Coding in Face Recognition System, " *2024 IEEE 13th Global Conference on Consumer Electronics (GCCE 2024)*, P2-05, Oct.2024.

表一覧

表 3.1	エッジ情報の異なる画像に対する DeepFace の True rate.....	8
表 4.1	認識モデルを変化させた際の非類似度の平均値と FAR スコア	11
表 4.2	検出器を変化させた際の非類似度の平均値と FAR スコア	11

図一覧

図 3.1 閾値を変化させた時のエッジ画像と生成画像の例	6
図 3.2 Stable Diffusion と DeepFace による同一人物判定の概要	6
図 3.3 Male and Female dataset の判定結果	7
図 3.4 DeepFace dataset の判定結果	7
図 3.5 Face Research Lab London set の判定結果	8

研究業績

- [1] Yurika Fujinami, Hiroshi Watanabe: “Adversarial Level of Face Images Generated by Prompt-based Image Coding in Face Recognition System”, 2024 IEEE 13th Global Conference on Consumer Electronics (GCCE 2024), P2-05, Oct.2024.

- [2] 藤浪優里佳, 渡辺裕: “顔認識システムにおけるプロンプトベース画像符号化と検出器の組み合わせによる精度評価”, 画像符号化シンポジウム／映像メディア処理シンポジウム(PCSJ/IMPS2024), P3-08, Nov.2024.