修士学位論文要約（令和 4 年 3 月）

ステガノグラフィを用いたキャンセラブル顔認証に関する研究

神津 岳志
指導教員：青木 孝文

Cancelable Face Recognition Using Steganography

Takashi KOZU
Supervisor: Takafumi AOKI

The secure transfer and storage of biometric traits are important for protecting the privacy of users. In this paper, we propose a cancelable face recognition method based on Deep Steganography. We embed a face image or face feature into an arbitrary image, called a cover image, to generate a stego image with the same appearance as the cover image. By using a feature extractor dedicated to stego images, face recognition can be performed without restoring the original face image or face feature from the stego image. The use of stego images generated by the proposed method makes it possible to transfer face images or face features without being noticed by the attackers. Through a set of experiments using public face image datasets, we demonstrate that the proposed method exhibits efficient performance on stego image generation and face recognition.

1.　はじめに

信頼性と利便性が高い個人認証技術としてバイオメトリクス認証が注目されている．バイオメトリクス認証の 1 つである顔認証は，非接触で生体情報を取得するため，利便性が高く，衛生的である．一方で，認証に用いる顔画像または顔特徴量（以下，まとめて顔情報と呼ぶ）が第三者に漏洩するとユーザのプライバシが侵害される恐れがある．そのため，顔情報を保護するためにキャンセラブルバイオメトリクス（CB）[1] が用いられる．CB では，生体情報を別の情報に変換し，それをテンプレートとして認証に用いる．変換パラメータを変えることで異なるテンプレートを生成できるため，テンプレートを容易に破棄・更新することができる．ユーザ固有の変換パラメータをユーザ自身が管理する必要があるため，本論文では，パラメータの管理を必要としないステガノグラフィを用いた手法に着目する．ステガノグラフィとは，ある情報を別の情報に埋め込んで秘匿する技術であり，情報を安全に転送したり，保管したりすることができる．ステガノグラフィを用いた顔認証が提案されているが，顔画像を埋め込んだ画像の品質が低く，認証精度の劣化が大きい問題がある．本論文では，Deep Steganography（DS）[2] を用いたキャンセラブル顔認証を提案する [3]．DS は，Convolutional Neural Network を用いた画像の埋め込み・抽出手法である．DS を用いることで，任意の画像（カバー画像）に顔情報を埋め込みつつ，その見た目が同じであるステゴ画像を生成する．認証時には，ステゴ画像から特徴量を抽出してマッチングすることで，顔情報を秘匿したまま顔認証を行う．大規模公開データセットを用いた性能評価実験を通して提案手法の有効性を示す．

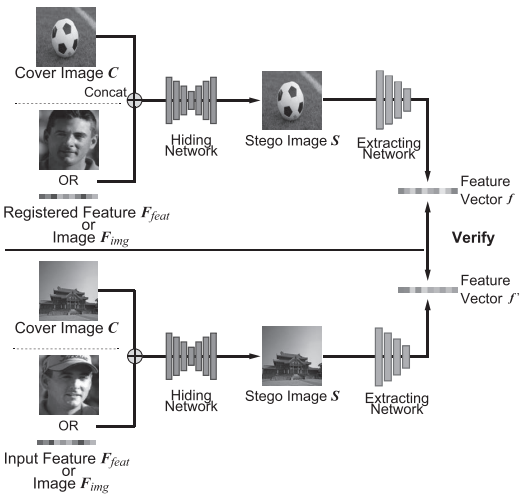

図 1　ステガノグラフィを用いたキャンセラブル顔認証

2.　ステガノグラフィを用いたキャンセラブル顔認証

ステガノグラフィを用いたキャンセラブル顔認証の概要を図 1 に示す．提案手法では，Hiding Network

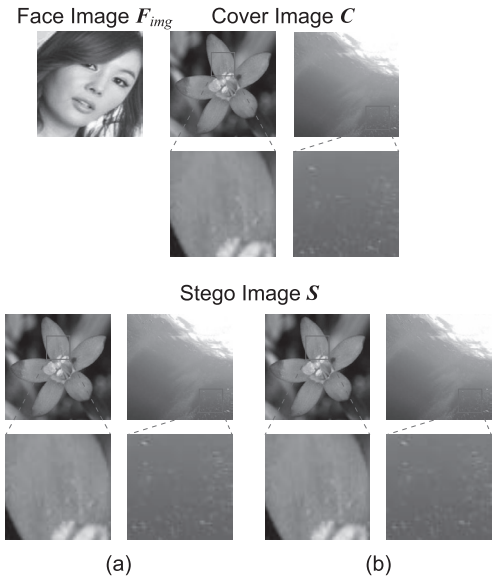

図 2　ステゴ画像例: (a) 顔画像を埋め込んだ場合, (b) 顔特徴量を埋め込んだ場合

(HN) を用いてステゴ画像を生成し，Extracting Network (EN) を用いてステゴ画像から特徴量を抽出する．まず，顔画像あるいは顔特徴量をカバー画像と結合し，HN に入力する．顔特徴量を用いる場合は，顔画像から抽出された顔特徴量をカバー画像と同じサイズになるまで複製する．HN では，カバー画像と見た目が同じであるステゴ画像を生成する．次に，HN から出力されたステゴ画像を EN に入力し，特徴量を抽出する．抽出された特徴量同士をマッチングすることで，個人認証を行う．ここで，EN が出力する特徴量は，顔特徴量に対して擬似乱数行列を乗算した特徴量とする．埋め込まれた顔情報の復元を困難にすることで，提案手法の安全性を向上させる．疑似乱数行列を変更することで異なる特徴量を生成できる．

3.　公開データセットを用いた性能評価実験

ネットワークの学習には CelebFaces Attributes dataset [4] を用いる．提案手法で生成したステゴ画像の例を図 2 に示す．図 2 より，埋め込む顔情報に関わらずカバー画像と見分けのつかないステゴ画像が生成されていることが確認できる．次に，提案手法における顔認証精度を評価する．顔認証精度の評価指標として，データセットに含まれる全ての画像ペアのうち正しく本人ペアあるいは他人ペアを推定できた割合を示す Accuracy，および他人受入率と本人拒否率の値が一致するときのエラー率を示す Equal Error Rate (EER) を用いる．ステガノグラフィによる認証精度への影響を評価するため，HN と EN を用いずに顔特徴量をそのまま認証に用いた場合をベースラインとして認証精度を比較する．表 1 に，評価用データセットとして Labeled Faces in the Wild (LFW) dataset [5] を用いたときの認証精度を示す．提案手法において顔特徴量を埋め込んだ場合の認証精度と，ベースラインの認証精度は同程度であった．一方で，Jiabao ら [6] の手法と同様に顔画像を埋め込んだ場合は，ベースラインより精度が低下した．顔画像を埋め込む場合は，特徴量を抽出しつつ埋め込む必要があるため，認証精度が低下したと考えられる．顔特徴量を埋め込むことで，認証精度を低下させることなくプライバシを保護できる．

表 1　LFW の顔認証精度

Verification method	Accuracy [%]	EER [%]
Baseline	99.70	0.3000
Proposed (Face image)	97.78	2.400
Proposed (Face feature)	99.50	0.6667

4.　まとめ

本論文では，任意の画像に顔情報を埋め込み，顔情報を保護するキャンセラブル顔認証を提案した．ステゴ画像の定性的評価，および公開データセットを用いた顔認証精度評価実験を通して，提案手法の有効性を実証した．今後の展望として，指紋や虹彩等の顔以外の生体情報を用いた生体認証への応用が挙げられる．

文献

1) M. Rawat and N. Kumar, “Cancelable biometrics: A comprehensive survey,” Artificial Intelligence Review, vol.53, pp.3403–3446, June 2020.
2) S. Baluja, “Hiding images in plain sight: Deep steganography,” Proc. Advances in Neural Information Processing Systems, vol.30, pp.2069–2079, Dec. 2017.
3) 神津岳志，河合洋弥，伊藤康一，青木孝文，“ステガノグラフィを用いたプライバシ保護顔認証とその安全性評価,” 第 24 回画像の認識・理解シンポジウム，pp.1–4, July 2021.
4) Z. Liu, P. Luo, X. Wang, and X. Tang, “Deep learning face attributes in the wild,” Proc. Int’l Conf. Computer Vision, pp.3730–3738, Dec. 2015.
5) G.B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled faces in the wild: A database for studying face recognition in unconstrained environments,” Technical Report 07–49, University of Massachusetts, Amherst, Oct. 2007.
6) J. Cui, P. Zhang, S. Li, L. Zheng, C. Bao, J. Xia, and X. Li, “Multitask identity-aware image steganography via minimax optimization,” IEEE Trans. Image Processing, vol.30, pp.8567–8579, Sept. 2021.