The University of Osaka
Institutional Knowledge Archive

Title	真正歩容動画の匿名化となりすまし偽歩容動画に対する防御
Author(s)	廣瀬, 雄基
Citation	大阪大学, 2023, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/91939
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

様式３

論　文　内　容　の　要　旨

氏　名　（　　廣瀬雄基　　）	
論文題名	真正歩容動画の匿名化となりすまし偽歩容動画に対する防御

論文内容の要旨

本論文では，真正な歩容情報の流通に伴うプライバシー情報流出，および，偽歩容情報の流出がもたらす「なりすまし」，という二つのリスクに対処する方法について論じた．

第1章では，歩容認証の発達により顕在化した真正歩容動画からのプライバシー情報流出問題，および，マルチメディアデータ生成技術の進展に伴って今後の深刻化が危惧される偽歩容動画を用いたなりすまし攻撃の危険性について述べ，本研究の目的を明らかにした．

第2章では，歩容およびその他の生体情報である顔や声などについて，生体認証や匿名化，なりすまし攻撃とその防御法に関する関連研究とそれらの課題を挙げ，本研究の位置づけを明らかにした．

第3章では，真正歩容を含む動画が非意図的に Web上で公開されることによるプライバシー情報流出問題について検討し，それ対する防御手法として，シルエットベース歩容認証手法を想定した歩容動画の匿名化について述べた．匿名化の従来手法である黒塗りやモザイク処理では動画の見た目が不自然になる問題に対し，歩容シルエットの形状の変形および姿勢変化パターンの変更とそれに合わせた色の再配置による匿名化手法を提案した．提案手法の匿名化後歩容動画を匿名性と見た目の自然さの観点からそれぞれ実験的に評価し，見た目の自然さを保ったまま匿名化が実現可能であることを示した．

第4章では，特定個人の一枚の歩容画像からその人物のなりすまし偽歩容動画を生成する手法を検討し，それによるなりすまし攻撃がどの程度現実的であるかを検証した．このなりすまし攻撃が対象とする歩容認証器では，歩容シルエット情報のみを用いて認証を行うと想定される．従って，第4章では偽歩容シルエット動画の生成手法について議論した．この偽歩容シルエット動画の生成は歩容画像から姿勢に非依存の特徴を抽出するエンコーダと，その特徴量から歩容シルエット動画を生成するデコーダの構築により実現した．さらに，デコーダにより生成される歩容動画は個人性の情報が一部欠落しているため，それらを補完する手法についても提案した．提案手法の偽歩容シルエット動画に対し，歩容認証器の精度の観点から評価を行い，なりすまし攻撃のリスクが無視できない程度に存在することを明らかにした．

第5章では，第4章で述べたなりすまし攻撃に対する防御法として，真正歩容動画と偽歩容動画を識別する手法について論じた．偽歩容動画がなりすまし攻撃に用いられる際には，一度シルエット化されたのちに歩容認証器に入力されることが想定されるため，本手法の識別対象は歩容シルエット動画とした．真／偽以外の人物，服装，姿勢，視点の4つの要素が統制された歩容シルエット動画対からなる学習データセットを自己符号化器により構築し，真正歩容動画と偽歩容動画を識別する識別器を作成した．複数のテストデータセットを対象に評価実験を行ったところ，高い精度で真正歩容動画と偽歩容動画を識別できること示した．

最後に，第6章で，Web動画中に存在する歩容情報に纏わる問題とその対処法に関する検証によって得られた結論をもとに今後の展望について述べた．

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　廣瀬　雄基　）			
論文審査担当者		（職）	氏　名
	主 査	教授	田中　雄一
	副 査	教授	丸田　章博
	副 査	教授	駒谷　和範
	副 査	教授	滝根　哲哉
	副 査	教授	三瓶　政一
	副 査	教授	宮地　充子
	副 査	教授	井上　恭
	副 査	教授	鷲尾　隆
	副 査	准教授	中村　和晃（東京理科大学 工学部 情報工学科）

論文審査の結果の要旨

歩容は生体情報の一種であり、人間の歩行の様子を指す。典型的には、歩行者の体型・歩行姿勢・歩行リズムとその組合わせが歩容と呼ばれる。歩容は個人ごとに異なっているため、指紋等と同様に個人を特定し得る生体情報である。ソーシャルネットワーキングサービスの発展やスマートフォンをはじめとしたカメラ付き携帯端末の普及により、大量の動画像がインターネット上に流通している。その中には歩容が含まれる動画像も多く含まれる。すなわち、撮影されている本人が意図しない形で歩容から個人を特定されるおそれが発生している。また、深層学習をはじめとした人工知能技術により、偽の歩容動画像が敵対する個人・団体により生成され、流通する可能性も否定できない。上に述べたような 1）真正歩容動画像から個人を特定し、プライバシー情報を取得する行為、2）偽歩容動画像を生成し、流通させることで個人の行動に対し偽の情報を拡散させる行為、に対する検討は、他の生体情報と同様に重要であるにも関わらず、今までほとんど行われていなかった。

本論文は、歩容動画像の流通に係るプライバシー情報を保護することを目的とし、真正歩容動画像の匿名化と偽歩容動画像の生成による攻撃可能性の実証、さらに真正歩容動画像と偽歩容動画像を識別するための手法に対する考察をまとめたものである。主たる研究成果を要約すると以下のようになる。

(1) 真正歩容を含む動画像の非意図的な公開によるプライバシー情報流出問題について検討している。歩容を匿名化しながら動画像を自然なものとするため、歩容シルエットの形状の変形および姿勢変化パターンの変更とそれに合わせた色の再配置による匿名化手法を提案している。また、提案手法により得られた歩容動画像を匿名性と見た目の自然さの観点から実験的に検証している。

(2) 1 枚の歩容画像からその人物の偽歩容動画像を生成する深層学習手法を検討している。また、生成した偽歩容動画像によるなりすまし攻撃がどの程度現実的であるかを検証している。提案手法の偽歩容シルエット動画像に対し、なりすまし攻撃のリスクが無視できない程度に存在することを明らかにしている。

(3) 偽歩容動画像を用いたなりすまし攻撃に対する防御法として、真正歩容動画像と偽歩容動画像を識別する手法について検討している。具体的には、シルエットを入力とする識別器を構築し、その学習に適した動画像データセットを自己符号化器により作成する枠組みを提案している。複数のテストデータセットを対象に評価実験を行い、高い精度で真正歩容動画像と偽歩容動画像を識別できることを明らかにしている。

以上のように、本論文は歩容動画像の流通におけるプライバシーに関する数多くの有用な知見を与えており、情報通信工学、特にメディア情報工学の発展に寄与するところが大きい。よって、本論文は博士論文として価値あるものと認める。