1.

Record Nr.	UNINA9910872182803321
Autore	Wen Yunqian
Titolo	Face de-Identification
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	9783031582226 9783031582219
Edizione	[1st ed.]
Descrizione fisica	1 online resource (195 pages)
Altri autori (Persone)	LiuBo SongLi CaoJingyi XieRong
Disciplina	006.37
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Acknowledgments -- About the Book -- Contents -- Acronyms -- Part I Introduction -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Face Recognition and Face De-identification -- 1.2.1 Face Recognition -- 1.2.2 Face De-identification -- 1.3 Book Overview -- References -- 2 Facial Recognition Technology and the Privacy Risks -- 2.1 Face Recognition Technology -- 2.2 Threat Models and Privacy Risks -- 2.3 Regulations and Acts on Facial Data Privacy -- 2.4 Conclusion and Future Outlook -- References -- Part II Face De-identification Techniques -- 3 Overview of Face De-identification Techniques -- 3.1 Face Image De-identification -- 3.1.1 Obfuscation-Based Methods -- 3.1.2 k-Same Algorithm Based Methods -- 3.1.3 Adversarial Perturbation-Based Methods -- 3.1.4 Deep Generative Model-Based Methods -- 3.1.4.1 Attribute Manipulation-Based Methods -- 3.1.4.2 Conditional Inpainting-Based Methods -- 3.1.4.3 Identity Representation Manipulation-Based Methods -- 3.2 Face Video De-identification -- 3.2.1 Methods of Applying Image De-identification Methods to Videos -- 3.2.1.1 Methods of Applying Image Method Frame by Frame -- 3.2.1.2 Methods of Adding Smooth Transition Measures Between Frames -- 3.2.2 Methods Designed Specifically for

Videos -- 3.2.2.1 Methods Based on Manipulating Identity Representation -- 3.2.2.2 Methods Based on Obfuscation -- 3.3 Evaluation Metrics -- 3.3.1 Privacy Protection -- 3.3.2 Utility Preservation -- 3.3.2.1 General Utility -- 3.3.2.2 Customized Utility -- References -- 4 Face Image Privacy Protection with Differential Private k-Anonymity -- 4.1 Introduction -- 4.2 Related Works -- 4.2.1 Privacy-Preserving Machine Learning -- 4.2.2 GAN-Based Face Manipulation -- 4.3 Preliminaries -- 4.3.1 Differential Privacy -- 4.3.2 Privacy Amplification -- 4.4 Our Approach -- 4.4.1 Step 1: Attributes Prediction.

4.4.2 Step 2: Obfuscation -- 4.4.2.1 k-Anonymity Average Attributes -- 4.4.2.2 Differential Privacy -- 4.4.3 Step 3: Image Generation -- 4.5 Experiments -- 4.5.1 Dataset -- 4.5.2 Implementation Details -- 4.5.3 Performance Analysis -- 4.5.4 Quantitative Evaluation -- 4.6 Conclusion -- References -- 5 Differential Private Identification Protection for Face Images -- 5.1 Introduction -- 5.2 Related Work -- 5.2.1 Face De-identification Methods Guaranteed by k-Anonymity Theory -- 5.2.2 Face De-identification Methods Guaranteed by t-Closeness Theory -- 5.2.3 Face De-identification Method Guaranteed by Differential Privacy Theory -- 5.3 Preliminaries -- 5.3.1 Problem Formulation -- 5.3.2 Differential Privacy Theory -- 5.3.2.1 Differential Privacy -- 5.3.2.2 Local Differential Privacy -- 5.3.2.3 Two Important Properties -- 5.3.3 Face Verification and Our Assumptions -- 5.3.4 The Proposed IdentityDP Framework -- 5.3.5 Stage-I: Facial Representations Disentanglement -- 5.3.6 Stage-II: -IdentityDP Perturbation -- 5.3.7 Stage-III: Image Reconstruction -- 5.3.8 Training Process -- 5.3.9 Some Discussions About Our Research Topic -- 5.4 Experiments -- 5.4.1 Experimental Setup -- 5.4.2 Evaluation Metrics -- 5.4.3 Implementation Details -- 5.4.4 -IdentityDP Mechanism Analysis -- 5.4.5 Comparisons with Traditional Methods -- 5.4.6 Comparisons with SOTA Methods -- 5.4.7 Generalization Ability -- 5.4.8 Computational Overhead -- 5.5 Conclusion and Future Work -- References -- 6 Personalized and Invertible Face De-identification -- 6.1 Introduction -- 6.2 Problem Formulation -- 6.3 Our Approach -- 6.3.1 Network Architecture -- 6.3.1.1 Identity Encoder -- 6.3.1.2 Attribute Encoder -- 6.3.1.3 Identity Modification Module -- 6.3.1.4 Generator -- 6.3.2 Training Process -- 6.3.3 Protection Process -- 6.3.4 Recovery Process -- 6.4 Experiments -- 6.4.1 Implementation Details.

6.4.2 Evaluation Results -- 6.4.2.1 De-identification -- 6.4.2.2 Recovery -- 6.5 Conclusion -- References -- 7 High Quality Face De-identification with Model Explainability -- 7.1 Introduction -- 7.2 Related Work -- 7.2.1 3D Monocular Face Reconstruction -- 7.2.2 Blind Face Restoration -- 7.3 Methodology -- 7.3.1 Overview of IDeudemon -- 7.3.2 Step I: Parametric Identity Protection -- 7.3.3 Step II: Utility Preservation -- 7.3.4 Loss Function -- 7.4 Experiments -- 7.4.1 Experimental Setup -- 7.4.2 Protective Perturbation Analysis. -- 7.4.3 Comparison with SOTA Methods. -- 7.4.4 Model Analysis and Ablation Study -- 7.5 Discussion -- 7.6 Conclusion -- References -- 8 Deep Motion Flow Guided Reversible Face VideoDe-identification -- 8.1 Introduction -- 8.2 Related Work -- 8.2.1 Face Video De-identification -- 8.2.2 Surveillance Video De-identification -- 8.3 Preliminaries of Problem Formulation -- 8.4 Deep Motion Flow Guided Reversible Face VideoDe-identification -- 8.4.1 Protection Module -- 8.4.2 Recovery Module -- 8.4.3 Motion Flow Module -- 8.4.4 Affine Transformation Module -- 8.4.5 The Entire IdentityMask Pipeline -- 8.5 Implementation -- 8.5.1 Identity Disentanglement Network Configuration -- 8.5.2 Other Implementation Details -- 8.6

Experiments -- 8.6.1 Experimental Setup -- 8.6.2 Comparison in De-identification -- 8.6.3 Analysis in Identity Recovery -- 8.6.4 Model Analysis and Discussions -- 8.7 Conclusions -- References -- Part III Conclusion and Future Work -- 9 Future Prospects and Challenges -- 9.1 Future Prospects and Open Research Questions -- 9.2 Technical Challenges -- 9.2.1 Low-Complexity and Real-Time De-identificationMethods -- 9.2.2 Preventing Reverse Engineering Attacks of De-identified Faces -- 9.2.3 Moving Beyond Supervised Learningon Limited Datasets -- 9.2.4 Multimodal De-identification -- References -- 10 Conclusion.

Glossary.