Samenvatting

Dit proefschrift richt zich op twee belangrijke toepassingen: identificatie van de broncamera en verbeterde robuustheid van ConvNets met gebruikmaking van beeldruis. De focus van het eerste deel van het proefschrift ligt op de forensische analyse van digitale afbeeldingen en video's. Dit helpt LEAs om extra informatie te verzamelen die gebruikt kan worden bij het identificeren van de persoon achter dergelijke inhoud. Dit werk heeft een belangrijke maatschappelijke toepassing in de strijd tegen seksueel misbruik van kinderen. Het tweede deel richt zich op het robuust maken van ConvNets voor ongeziene beeldcorrupties, waarvan de technieken voor verschillende toepassingen kunnen worden gebruikt. Beide delen betreffen de ruis in het invoerbeeld, waarbij in het eerste geval de aanwezigheid van ruis cruciaal is en in het tweede geval de ruis wordt onderdrukt.

Het eerste deel van het proefschrift richt zich op broncamera-identificatie, waarbij de ruis in het invoerbeeld in ons voordeel wordt gebruikt voor de identificatie van de broncamera uit afbeeldingen of videoframes. In vergelijking met traditionele benaderingen (Goljan, 2008), hebben recente methoden gebaseerd op ConvNets (Cozzolino and Verdoliva, 2019) aanzienlijke vooruitgang geboekt. Daarom beperkt dit proefschrift zich tot de studie van ConvNets voor broncamera-identificatie. Bovendien is dit werk beperkt tot de identificatie van de broncamera op basis van alleen de pixelgegevens (zonder rekening te houden met de begeleidende beeldmetadata). Dit is gedaan om te voorkomen dat het systeem vertrouwt op meta-gegevens waarvan manipulatie onopgemerkt kan blijven.

Hoofdstukken 2 en 3 gaan over broncamera-identificatie uit afbeeldingen. Forensische onderzoekers kunnen geconfronteerd worden met de vraag of twee afbeeldingen afkomstig zijn van hetzelfde cameratoestel. Om deze vraag te beantwoorden is een systeemontwerp voorgesteld (hoofdstuk 2) en gevalideerd met experimenten voor apparaat-gebaseerde beeldvergelijking. Dit bestaat uit een

tweedelig netwerk: het eerste netwerk onttrekt haalt forensische handtekeningen uit een ingevoerd beeld en het tweede netwerk neemt een paar handtekeningen om de gelijkwaardigheidsscore ertussen te berekenen. De experimenten op de *jpeg* subset van de dataset van Dresden hebben het potentieel van deze benadering aangetoond en bieden ruimte voor interessant toekomstig werk. Hoofdstuk 3 stelt de vraag: "Is er in sommige gebieden van een afbeelding meer cameraruis aanwezig dan in andere gebieden?" Op basis van de waarnemingen dat de sensorruis kan worden geëxtraheerd wanneer deze wordt blootgesteld aan een uniform belichte scène en de scène-inhoud de sensorruis vervormt, werd de hypothese gesteld dat homogene regio's in een afbeelding de voorkeur verdienen voor forensische analyse. Aangetoond werd dat wanneer er op een hiërarchische manier op deze homogene region's getraind wordt, dit resulteert in een classificator die rekenkundig efficiënt, modulair en effectiever is dan een vlakke (enkele classificator) benadering. Door middel van grondige experimenten op de *natural* subset van de dataset van Dresden bereiken we de beste classificatienauwkeurigheid ooit van 99,01% voor de identificatie van cameramodellen.

Hoofdstukken 4 en 5 betreffen broncamera-identificatie van video's. Analoog aan camera-identificatie van beelden werden videoframes gebruikt voor de bronclassificatie van een video. Van de drie typen videoframes bleken I-frames meer forensische sporen te bevatten (omdat ze niet beïnvloed worden door videostabilisatie). Een uitgebreide geconcentreerde convolutielaag werd voorgesteld voor scène-inhoudsonderdrukking van RGB-beelden (zie Hoofdstuk 4) voor ondiepe ConvNets. Er werd vastgesteld dat een dergelijk schema voor scène-onderdrukking contraproductief is voor geavanceerde ConvNets. Het effect van videocompressie op forensische sporen werd ook bestudeerd. De prestaties van het systeem blijven consistent, zelfs wanneer de eigen video's worden onderworpen aan YouTube- en WhatsApp-compressie. Er werden uitgebreide experimenten uitgevoerd met verschillende geavanceerde ConvNets op de VISION- en de QUFVD-datasets om de doeltreffendheid van de methoden aan te tonen.

Hoewel systemen voor machinaal leren traditioneel werden geëvalueerd door de verdeling van de testset gelijk te houden aan die van de trainingsset, ondervinden de gebruikte systemen in de praktijk distributieverschuivingen als gevolg van verschillende ongecontroleerde factoren. Daarom wordt in het tweede deel van het proefschrift ruisonderdrukking voor robuuste ConvNets onderzocht. In het bijzonder werden twee onafhankelijke richtingen verkend. In de eerste richting wordt een voorbewerkingsstap voorgesteld om de robuustheid van het model te verbeteren. De tweede richting bestaat uit het aanbrengen van

architecturale veranderingen om de robuustheid van het model voor beeldcorrupties te verbeteren.

Hoofdstuk 6 richt zich op beeldvoorbewerking voor robuuste beeldclassificatie. Er is een transformatiestap voorgesteld om het generalisatievermogen van het ConvNet te verbeteren. Concreet worden de afbakeningskaarten van gegeven beelden bepaald met behulp van de CORF push-pull inhibitie operator. Een dergelijke operatie transformeert een ingevoerd beeld in een ruimte die robuuster is voor ruis, voordat het wordt verwerkt door een Convolutional Neural Network (ConvNet). Onze experimenten op de Fashion MNIST-dataset met AlexNet toonden aan dat de voorgestelde CORF-ondersteunde pijplijn een aanzienlijk hoger generalisatievermogen vertoont voor additieve Gaussiaanse en uniforme ruis dan een conventioneel AlexNet zonder de CORF-transformatiestap. Vergelijkbare resultaten worden bereikt op ruisvrije beelden.

Hoofdstuk 7 onderzoekt de out-of-distribution robuustheid voor ConvNets door architecturale veranderingen door te voeren. Een rekenlaag, PushPull-Conv, wordt voorgesteld ter vervanging van de traditionele convolutionaire laag in de eerste laag van het Convolutional Neural Network (ConvNet). Het ontwerp van PushPull-Conv is geïnspireerd op de hersenen en bestaat uit excitatoire en inhibitoire (of push en pull) berekeningspaden. Deze methodologie helpt robuustheid te bereiken tegen hoogfrequente corrupties met een klein compromis voor schone testgegevens. We hebben uitgebreide analyses en experimenten uitgevoerd op CIFAR10-C en ImageNet-C datasets om onze hypothese te valideren.

Kortom, dit werk maakt gebruik van beeldruis en draagt betere oplossingen aan voor twee cruciale toepassingen, namelijk identificatie van de broncamera en verbeterde robuustheid van convolutionaire neurale netwerken. De voorgestelde methoden bevorderen de state-of-the-art in de respectievelijke onderzoeksproblemen en helpen belangrijke maatschappelijke problemen aan te pakken.