氏　　名	安井　達哉
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　６９２８　　号
学位授与の日付	２０２３年　９月　２５日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study of Digital Watermarking for Protecting the Multimedia Content （マルチメディアコンテンツを保護するための電子透かしに関する研究）
論文審査委員	准教授　栗林　稔　　教授　舩曳　信生　　教授　野上　保之

学位論文内容の要旨

This thesis is organized with five chapters as follows.

Chapter 1 introduces the objectives of protecting the multimedia content with reference to multimedia security techniques and related research.

In Chapter 2, the watermarking and fingerprinting techniques and algorithm are reviewed.

Chapter 3 proposes the DNN watermarking robust against pruning attacks. Our contribution is the introduction of encoding technique into the DNN watermark to make it robust against pruning attacks. While previous studies have proposed DNN watermarks that are robust against a certain level of pruning rate, our method can assure the robustness with a pre-defined level of pruning rate by carefully setting the encoding parameters. The common scenario in which DNN watermarks are used in DNN model is the buying and selling of DNN models. In this scenario, our method can prevent illegal redistribution and illegal copying by users who have purchased the DNN model. As a white-box watermarking is assumed in our method, it suffers from the direct modification of weight parameters, which is the common threat in white-box setting. If the weight parameters are replaced with random values and trained from the scratch with enough dataset, the watermark can be removed completely without compromising the performance of DNN model. Hence, it is assumed in our method that the attacker cannot train the target DNN model from scratch in terms of computational resources and amount of training dataset.

Chapter 4 proposes the near-optimal detection for near-optimal detection for binary Tardos code by estimating collusion strategy. Our contribution is the realization of detector for optimal detector by estimating requirement parameters which are number of colluders and collusion strategy by colluders. In other words, we have developed an estimator that estimates the parameters required for an optimal detector. The collusion strategy estimator focuses on the number of symbols in the binary code. Symbols are distributed differently depending on the number of colluders and collusion strategies. It achieved better performance than any of the previous studies. Similar performance was also achieved when the evaluation was conducted under realistic noise-added scenarios.

Finally, Chapter 5 concludes the thesis by briefly reviewing the entirety.

論文審査結果の要旨

安井達哉氏はコンテンツの保護技術に関して、マルチメディアコンテンツと深層学習モデルを対象にして研究を行った。人間の知覚の特性を利用して人間が知覚できないコンテンツの領域に情報を埋め込むことで複製や改ざんを抑制する電子透かし技術において、コンテンツへの電子透かしの埋め込みを通信路モデルとしてみなして、送受信するデータを透かし情報、コンテンツを通信路にモデル化して研究を行っている。対象とするコンテンツは、従来から研究されている音声、音響、画像、映像などのマルチメディアコンテンツだけでなく、深層学習技術によって生成されたDNNモデルを扱っている。まず、DNN電子透かし技術においては、透かし情報を取り除くために想定されるプルーニング攻撃に対して堅牢性を担保するため、攻撃による影響を消失通信路にモデル化し、重み一定符号による符号化の手段を考案している。マルチメディアコンテンツの不正コピーから不正者を特定するための電子指紋技術においては、最も脅威となっている複数の利用者による結託攻撃を対象に、電子指紋符号の研究に着目している。従来研究で示された最適な検出器には、結託者数と結託戦略が不可欠であり、通常はこれらの情報は検出側において未知であった。これらの情報を高精度で推定するために、コンテンツから抽出した符号語の系列の偏りを解析する手法を考案しており、最適な検出器を実現するための手法を提案している。

このように安井達哉氏は従来とは全く異なるアプローチを手掛けており、それら手法の新規性および有効性は数量的に示され、従来法と比べても優位性が十分示されている。その成果は、工学的・学術的価値が極めて高く、外部発表においても学術研究賞を4件受賞するなど学術的にその成果が認められてことから、本論文は博士(工学)の学位授与に値するものと認められる。