審査の結果の要旨

論文提出者氏名　　金　美羅

本論文は「Copyright Protection System Using The Fingerprinting Scheme (フィンガープリンティング方式を用いる著作権保護システム)」と題し，デジタルコンテンツの不正配布を抑止する著作権保護システムを構成する上で有効なフィンガープリンティング方式に関して，①フィンガープリンティング方式の性能向上，②フィンガープリント付きのコンテンツの配信方式，③ソフトウェア電子透かし，の三つの観点から検討している．デジタルコンテンツの不正配布を抑止する著作権保護システムを構成する上でフィンガープリンティング方式は有効であるが，これを実際に用いる場合，フィンガープリントのサイズをどう抑え，フィンガープリント付きのコンテンツをどのように配信するかが鍵となってくる．また，フィンガープリンティング方式は安全な電子透かしの存在が前提となるが，コンテンツがプログラムなどのソフトウェアである場合，電子透かしの基礎検討が不十分であり，その安全性が不明である．本論文は，これらの問題に対し，解決策を検討したものであり，「Introduction」を含め5章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第2章は「Construction of Secure Fingerprinting Schemes Against Collusion Attacks（結託攻撃に対して安全なフィンガープリンティング方式の構成）」と題し，結託攻撃が行われた後も，デジタルコンテンツの不正流出元の追跡を可能にする手法を示している．結託攻撃はフィンガープリンティング方式に対する強力な攻撃手法である．これに対して耐性があるフィンガープリントを構成する方式が研究されているが，従来方式では，フィンガープリントのサイズが極めて大きかった．本章では，結託攻撃に対して耐性があり，フィンガープリントのサイズを小さくする手法を示している．

第3章は「Broadcast Encryption Against Contents Illegal Redistribution（コンテンツの不正配布抑止のための放送暗号）」と題し，放送暗号を用いてフィンガープリント付きコンテンツを配信する手法を示している．放送暗号は暗号化された放送用コンテンツに対して，復号鍵を持つユーザだけにアクセスを許可する手法である．しかし，ユーザごとに異なるコンテンツが割り当てられるフィンガープリンティング方式と放送暗号と組み合わせることは困難であった．本章では，放送暗号とフィンガープリンティング方式を組み合わせるための新しいモデルを示すとともに，提案モデルに適した新しい放送暗号を示している．この放送暗号は，従来方式に比べ，メモリ量，通信量ともに削減できる．

第4章は「Differing-Inputs Software Watermarking Scheme（入力差分を持つソフトウェア電子透かし）」と題し，同形変換攻撃に対して安全なソフトウェア電子透かしに関して，計算量的な観点からの新しい考え方を示したものである．従来の研究では，同形変換攻撃に対して安全なソフトウェア電子透かしは存在しないことが示されている．これに対し本章では，ソフトウェア電子透かしの定義をやや緩めることにより，安全なソフトウェア電子透かしの存在の可能性を示している．

最後に第5章は「Conclusion（結言）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，デジタルコンテンツの不正配布の抑止に有効なフィンガープリンティング方式に関する基礎検討を行うとともに，フィンガープリンティング方式を用いる著作権保護システムに必要な具体的手法を明示したものであり，電子情報学，特に情報セキュリティ工学上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．