システム情報工学研究科修士論文概要

年 度	平成　24 年度	学位名	修士(工学)
専 攻	知能機能システム　専攻	著者氏名	児矢野 和也

指導教員氏名　古賀 弘樹

論文題目

確率的な電子指紋符号の容量に関する研究

論文概要

近年ではインターネットを介して動画や音楽等のデジタルコンテンツの不正配信が問題となっている. 不正配信により正規のユーザ以外がコンテンツを入手できるため著作権保護の観点から対策が必要である.

不正配信を防止するための手法としてコンテンツに配信するユーザの ID 情報をあらかじめ埋め込む電子指紋符号が有効である. 電子指紋符号はユーザにはわからないようにコンテンツに ID 情報となる符号を埋め込む技術であり, 不正配信されたコンテンツからID情報を読み取ることで不正配信を行ったユーザを特定することができる.

しかし, 電子指紋符号は結託攻撃に弱いという問題がある. 結託攻撃とは複数のコンテンツから読み取った符号を比べることによって, 新しい符号を作りコンテンツに埋め込む攻撃のことである. 結託攻撃が行われた場合には不正配信されたコンテンツに埋め込まれている符号は, 元の符号とは異なるため正しく ID 情報を取り出して不正者を特定することができない. このような不正者の結託攻撃に対して耐性のある結託耐性符号の研究が盛んに行われている. 結託耐性符号には不正者を正しく検出し, 無実のユーザを誤って検出しないことが求められる. 電子指紋符号の研究において不正者の攻撃に制約を与えるマーキング仮定というものがある. マーキング仮定とは, 不正者が複数の符号語を比べた場合にビット値の等しいビットを検出することができず, ビット値を変更できないという仮定である.

本研究では符号語を確率的に生成し, マーキング仮定下で不正者 2 人の結託攻撃を条件付き確率分布でモデル化する. 各ユーザの符号語と不正符号語によって定まるタイプによる相互情報量を用いることで, 不正者を検出するアルゴリズムを提案する. そして, 不正者が k 人の場合への攻撃モデルと検出アルゴリズムの一般化を行う. ユーザ数と相互情報量がある条件を満たす場合に, 十分大きいすべての n に対して不正者の誤検出確率が十分小さくなることを示す. また, 不正者が 2 人の場合に十分大きいすべての n に対して不正者の誤検出確率が十分小さいならば, $C > m$ となることを示す. 不正者が k 人の場合に検出アルゴリズムで用いる相互情報量を容量について考察し公式を導出する.

審査日　　平成　25 年　1 月　30 日

審査員	（大学名 職名）	（学位）	（氏名）
主査	筑波大学 准教授	博士(工学)	古賀 弘樹
副査	筑波大学 准教授	博士(工学)	掛谷 英紀
副査	筑波大学 講師	博士(工学)	延原 肇