データの真正性を保証する電子透かしに関する研究

【代表者】黄　緒平　島根大学　総合理工学部　准教授

【研究の目的と内容】

デジタルメディア技術の急速な発展とともに、画像、音声、映像、文書等の多様なコンテンツがネットワークを通じて容易に生成・流通・共有されるようになった。こうした利便性の向上に伴い、デジタルデータの改ざん、偽造、不正流通といったセキュリティ上の脅威も深刻化しており、データの**真正性（authenticity）および完全性（integrity）**を担保する技術の確立が強く求められている。これに対して、電子透かし技術は有効なアプローチの一つとして注目されている。電子透かしとは、デジタルデータに対して人間の知覚では判別困難な透かし情報を埋め込み、それを後から検出・抽出することで、著作権保護、データの改ざん検出、認証などを実現する技術である。特に真正性の保証においては、原本データに対応する電子透かしを埋め込むことで、改ざんの有無やデータの出所の検証が可能となる。真正性を保証するための電子透かし技術には、以下のような課題が残されている。真正性の保証を目的とする電子透かし（fragile watermarking）は、データの微小な改ざんに対しても高精度に検出する必要があるが、その一方で自然な通信・保存過程における信号圧縮等の劣化にも脆弱であるという脆弱性と耐改ざん性のトレードオフがある。また、透かし情報を機能するため、ダイジェスト情報を埋め込む容量を確保しつつ、原本のデータ品質を維持する必要がある。特に証拠性の高い医療カルテや軍事用衛星データ等に適用する際に、埋め込み容量と可逆性の両立を確保する必要がある。更に、改ざん検出機能を備えた電子透かしが攻撃者により無効化され、偽の透かしが埋め込まれるリプレイ攻撃への耐性が不十分であると、真正性保証の根幹が揺らぐ。このため、暗号技術との併用や、鍵に依存するセキュアな埋め込み・抽出方式のメカニズムにおいて、攻撃耐性とセキュリティ性の確保が重要な研究課題である。

【研究の成果（本研究によって得られた知見、成果、論文、学会発表、外部資金への応募見込み等）】

本研究は、証拠性を有する音響データに対して、改ざんの検出およびデータの真正性を保証するための、可逆かつ不可聴な音響電子透かし手法を提案するものである。提案手法は、改良型整数離散コサイン変換（modified integer discrete cosine transform; intDCT）係数拡張に基づき、音声信号をフレーム単位で処理し、各フレームに透かし情報を埋め込む。具体的には、主に高周波帯域の DCT 係数に対して情報を埋め込むことで、聴覚上の違和感を最小限に抑えつつ、十分な埋め込み容量を確保している。埋め込みおよび抽出は完全に可逆であり、原信号を損なうことなく復元可能である。さらに、原信号を用いずに改ざん検出が可能なブラインド検出方式を実現している点においても実用的な有用性を有することを明らかにした。提案手法の性能評価として、ITU-T 標準の 112 種の音声信号を用いて客観的音質指標に基づく実験を行った。その結果、音声品質指標 MOS-LQO において平均 4.41、セグメンタル S/N 比（segSNR）において平均 23.31 dB を記録し、埋め込み容量 8000 bps の条件下でも高い不可聴性と埋め込み容量の両立が確認された。また、処理時間に関しても、10 秒の音声クリップに対して平均 4.88 秒で処理が完了し、リアルタイム応用への適用可能性を示した。更に、既存の LPC（Linear Predictive Coding）に基づく手法と比較し、提案手法は時間領域における歪みの低減、およびオーバーフロー発生の低減において優れた性能を示した。これらの結果は、提案手法が真正性検証を必要とする音声データに対する有効かつ実用的な情報隠蔽技術であることを示した。

本研究の推進は概ね順調で、研究期間中、以下の査読付きジャーナル 1 報、査読付き国際会議プロシーディング1報、国内会議研究論文1報の計 3 件の国内外における研究成果の発表があった。今後も本研究を引き続き研鑽を積み、外部資金の採択につながるよう励んでいきたい。