博　士（情報科学）　田　森　秀　明

学 位 論 文 題 名

数論変換の電子透かしへの応用に関する研究

学位論文内容の要旨

著作権保護のための耐性型電子透かしで代表的な手法に直交変換を用いた手法が数多く紹介されている. これは空間領域に直接署名情報を埋め込むのではなく, 直交変換領域に埋め込むことにより, ロバスト性や安全性, あるいは秘匿性の向上が期待できるからである.

一方で, 電子透かしの用途は, 著作権保護のみならず様々な方面への応用が研究されている. 改ざん検出のための脆弱型電子透かしもその一つである. これは, 保護対象とするディジタル画像に, 特定の画像処理に意図的に壊れやすくした脆弱型の電子透かしを, 小さなブロック単位で画像全体に繰り返し埋め込む. 改ざん検出の段階では, 破壊された電子透かしを視認により同定し, 改ざん位置の特定を行うものである.

脆弱型電子透かしにおいては, 実用的な運用の面からも方式の検討がされている. 非対称型電子透かしと呼ばれる手法は, 電子透かしを埋め込む鍵と, 抽出する鍵が異なる, 公開鍵暗号方式の考え方を取り入れたものである. 埋め込み鍵と抽出鍵が同じ, いわゆる秘密鍵による電子透かし手法は, 鍵が流出すると, 保護すべきコンテンツに攻撃者が新たに電子透かしを上書きできる. よって, 実際の運用では鍵を公開できず, ユーザー側で抽出処理ができない. 一方, 非対称型電子透かしは, 公開する抽出鍵では電子透かしを埋め込めないため, この抽出鍵を公開できる. これにより, ユーザー側で透かし情報を抽出・検証できるため, 実際の運用を簡素に構築できる.

さらには近年, ロスレス型の電子透かしが検討されている. これは, 埋め込み処理において復元用の情報を作成し, 署名情報とともに対象となる原画像に埋め込む. 埋め込み処理をされた画像は劣化したものであるが, 抽出処理の段階では, その抽出された情報で埋め込み画像から原画像を復元するものである. この手法は, 芸術性が追求される画像データや劣化が許されない医用画像などの保護に応用されることが考えられている.

従来の耐性型電子透かしに用いられる代表的な直交変換として, 離散コサイン変換や離散フーリエ変換などが検討されてきた. これらの変換は空間領域における変化がわずかなら, 変換領域にはほとんど影響しないロバストな性質があり, 一方で浮動小数点演算による計算誤差が発生する. このような直交変換を脆弱型電子透かしやロスレス型電子透かしに応用する場合, 脆弱型電子透かしにおいてはロバストな性質は逆に改ざん検出の妨げになる. また, 誤差の発生により, 抽出された透かし情報に破壊が見受けられた場合, それが計算誤差によるものか, 改ざんによるものかの判断がつかなくなる. 例えば, 変換領域を利用した脆弱型電子透かしは SHIH らにおいて検討されている. これは DCT 領域に署名情報を埋める手法であるが,DCT の計算で丸め誤差が発生する. そこで SHIH らの手法では, 遺伝的アルゴリズムを用いて計算誤差を考慮し, この問題を解決しなければならなかった. また, ロスレス型電子透かしでは, 誤差によって抽出情報に符号誤りが発生した場合はその機能

を果たさないことがある. これらの理由から, 脆弱型電子透かしやロスレス型電子透かしの従来手法は耐性型電子透かしとは異なり, 空間領域, すなわち画素値を直接利用して実現されることが多かった. しかし, 画素値を直接操作する電子透かし手法は, 埋め込み済み画像の画素値を解析することで, 様々な攻撃方法が発見できる危険性があるとされる. そこで, これらが直交変換領域を用いた手法で実現できれば, 耐性型電子透かしが変換領域を利用することで得られるような, 安全性や秘匿性の向上が期待できる.

以上の背景を鑑み, 直交変換に基づくこれらの電子透かしとして, これまでに私は数論変換による手法を提案してきた. 数論変換は計算誤差が発生せず, また空間領域のわずかな変化もその変換領域に大きな影響を与える脆弱な性質を持つ. これらの性質は脆弱型電子透かしおよびロバスト型電子透かしへの応用に適していると考えられる. 数論変換を利用することで, 計算誤差による署名情報の破壊に関する考慮を不要にし, さらには安全性を向上することを検討してきた.

本論文では数論変換を利用した脆弱型電子透かしとロスレス型電子透かしを提案する. 脆弱型電子透かしにおいては,JPEG 画像への応用や, 非対称型電子透かしについても検討する. 実験では, それぞれの提案手法を静止画像に適用し, その有効性について検討する.

学位論文審査の要旨

主　査　教　授　山　本　　強
副　査　教　授　荒　木　健　治
副　査　教　授　長谷山　美　紀

学位論文題名

数論変換の電子透かしへの応用に関する研究

著作権保護のための耐性型電子透かしで代表的な手法に直交変換を用いた手法が提案されている．これは空間領域に直接署名情報を埋め込むのではなく，直交変換領域に埋め込むことにより，ロバスト性や安全性，あるいは秘匿性の向上が期待できるからである．　一方で，電子透かしの用途は，著作権保護のみならず様々な方面への応用が研究されている．改ざん検出のための脆弱型電子透かしもその一つである．これは，保護対象とするディジタル画像に，特定の画像処理に意図的に壊れやすくした脆弱型の電子透かしを，小さなブロック単位で画像全体に繰り返し埋め込む．改ざん検出の段階では，破壊された電子透かしを視認により同定し，改ざん位置の特定を行うものである．

脆弱型電子透かしにおいては，実用的な運用の面からも方式の検討がされている．非対称型電子透かしと呼ばれる手法は，電子透かしを埋め込む鍵と，抽出する鍵が異なる，公開鍵暗号方式の考え方を取り入れたものである．埋め込み鍵と抽出鍵が同じ，いわゆる秘密鍵による電子透かし手法は，鍵が流出すると，保護すべきコンテンツに攻撃者が新たに電子透かしを上書きできる．よって，実際の運用では鍵を公開できず，ユーザー側で抽出処理ができない．一方，非対称型電子透かしは，公開する抽出鍵では電子透かしを埋め込めないため，この抽出鍵を公開できる．これにより，ユーザー側で透かし情報を抽出・検証できるため，実際の運用を簡素に構築できる．

さらに近年，ロスレス型の電子透かしが検討されている．これは，埋め込み処理において復元用の情報を作成し，署名情報とともに対象となる原画像に埋め込む．埋め込み処理をされた画像は劣化したものであるが，抽出処理の段階では，その抽出された情報で埋め込み画像から原画像を復元するものである．この手法は，芸術性が追求される画像データや劣化が許されない医用画像などの保護に応用されることが考えられている．

従来の耐性型電子透かしに用いられる代表的な直交変換として，離散コサイン変換や離散フーリエ変換などが検討されてきた．これらの変換は空間領域における変化がわずかなら，変換領域にはほとんど影響しないロバストな性質があり，一方で浮動小数点演算による計算誤差が発生する．このような直交変換を脆弱型電子透かしやロスレス型電子透かしに応用する場合，脆弱型電子透かしにおいてはロバストな性質は逆に改ざん検出の妨げになる．また，誤差の発生により，抽出された透かし情報に破壊が見受けられた場合，それが計算誤差によるものか，改ざんによるものかの判断がつかなくなる．例えば，変換領域を利用した脆弱型電子透かしは Shih らにおいて検討されている．これは DCT 領域に署名情報を埋める手法であるが，DCT の計算で丸め誤差が発生する．そこで Shih らの手法では，遺伝的アルゴリズムを用いて計算誤差を考慮し，この問題を解決しなければならな

かった.

また, ロスレス型電子透かしでは, 誤差によって抽出情報に符号誤りが発生した場合はその機能を果たさないことがある. これらの理由から, 脆弱型電子透かしやロスレス型電子透かしの従来手法は耐性型電子透かしとは異なり, 空間領域, すなわち画素値を直接利用して実現されることが多かった. しかし, 画素値を直接操作する電子透かし手法は, 埋め込み済み画像の画素値を解析することで, 様々な攻撃方法が発見できる危険性があるとされる. そこで, これらが直交変換領域を用いた手法で実現できれば, 耐性型電子透かしが変換領域を利用することで得られるような, 安全性や秘匿性の向上が期待できる.

数論変換は計算誤差が発生せず, また空間領域のわずかな変化もその変換領域に大きな影響を与える脆弱な性質を持つ. これらの性質は脆弱型電子透かしおよびロバスト型電子透かしへの応用に適している特性である. そして数論変換を利用することで, 計算誤差による署名情報の破壊に関する考慮を不要にし, さらには安全性を向上することを提案している.

本論文では数論変換を利用した脆弱型電子透かしとロスレス型電子透かしの具体的な手法を提案し、実装法について検討しており、 脆弱型電子透かしにおいては,JPEG 画像への応用や, 非対称型電子透かしについても検討するとともに, それぞれの提案手法を静止画像に適用し実験によってその有効性を示している.

以上要するに、本論文は数論変換を応用した脆弱型およびロスレス型の電子透かしの新しい方式を提案するとともに実装によって有効性を検証したものであり、情報メディア学の発展に大きく寄与するものである。よって著者は北海道大学博士 (情報科学) の学位を授与される値するものと認める。