博士論文審査結果の要旨

博士論文審査委員会

主　　査	大関　和夫	審査委員	杉本　徹
審査委員	平川　豊	審査委員	木村　昌臣
審査委員	佐藤　清次		

氏　　名	魏　遠玉
論文題目	電子透かしによる画像の保護特性に関する研究

〔論文審査の要旨〕

「電子透かしによる画像の保護特性に関する研究」という題で、２月１９日（水）論文発表と審査会を開催した。申請者から60分の発表が有り、その後約60分の質疑応答があった。

研究発表内容は、まず電子透かしを公開領域で検出するために、検出ソフトウェアも公開していく必要性があるため、検出ソフトウェアを機能を保ったまま難読化し、公開しても解読を防ぐことが重要となっている。本研究では、公開領域においても解読されない難読化方式を提案し、その計算量的困難性を評価している。また、この方式は企業の行うソフトウェア公開においても、有効な方式であるため、実用化の共同研究と実用化のサポートを行ってきた。その結果、ある企業で、具体的に本方式の開発を行い、実用化を行う所までの成果を上げることができた。

次に、電子透かしそのものの特性向上のため、３次元直交変換による埋込み方式の研究を行い、また同一基準で１次元から３次元までの比較を行い、次元の増加に伴う、特性の向上の度合いを定量的に求めることを行っている。変換の方式は、従来からある離散コサイン変換（ＤＣＴ）に加え、新たに電子透かしに適した独自チャープ変換を開発し、埋込み範囲の拡大を図るなどの特性向上を達成している。１次元から３次元までの特性評価を詳細に行い、多数の結果を得てきたが、変換にＤＣＴを用いる場合は、十分な特性向上が図れているが、独自チャープ変換を用いた場合、３次元変換を行うと、特性が悪くなるという問題が出た。この劣化が計算ミスか特性自体が悪いかの調査や検証を進め、最終的には、チャープ変換は１次元変換では良好な性能を有すが、２、３次元変換では、特性が悪いことがわかった。これは、最初の設計において１次元のモデルしか存在しないたためで、２、３次元のモデルの構成が難しいことがわかった。そこで、２次元のＤＣＴと１次元のチャープ変換を組み合わせ、合計３次元の構成をとったら、高性能が得られると共に、チャープ変換の好特性である埋込み範囲の拡大が図れることが分かった。このような試行錯誤と多くの検証実験を行うことにより、ＤＣＴとチャープ変換を組み合わせる方式が最も良いという、意外な結果がえられ、これを最終的な提案方式として、まとめることになった。

質疑では、難読化に使用した公開鍵暗号方式の数値例について、チャープ変換の変換行列の基底ベクトルについて、チャープ変換の場合の埋込み位置について、量子化手法について、プログラム構成図について、動画から１次元データや２次元データの取り出す図について、耐性評価のグラフについて、耐性や圧縮率の対応関係について、MPEG圧縮を行った場合の耐性について、動画の画像サイズや原情報量について、チャープ変換で画像の平坦部に埋込んだ時の特性について、など多数の質疑を行い、それぞれほぼ問題なく回答した。

審査の結果、留学生であり、日本語の厳密な表現はやや問題はあるが、研究のレベルや実験量、得られた成果など、どれも課程博士として十分な内容であるとの見解が得られ、全員一致で、合格との判定となった。

（様式第６号）

論　文　要　旨

年　月　日

※報告番号	甲　第 156 号	氏　名	魏　遠玉

主論文題名：電子透かしによる画像の保護特性に関する研究

内容の要旨：電子透かしは人の目に見えないマークをコンテンツに情報として埋め込み、必要に応じて検出することによって、コンテンツの著作権保護や真偽判定に役立つ情報セキュリティ技術である。情報を埋め込み、著作権の所在を主張しようと企画したものである。また、利用者の情報を埋め込む事によって、不正行為が行われた際に、埋め込まれている情報を検出する事で、不正行為の防止に役立ち、著作権侵害に対する検証方法として利用されている。

米国の Digimark 社は電子透かしをビジネスとしており、大きく成功をしている。埋込サービスや、クーポン券などに電子透かしを埋込みバーコードなどよりも親みやすい応用を普及させている。又、埋込んだ画像のネット上での検索サービスなども行っている。

電子透かしの検出器を難読化する意義は、難読化により、著作権情報等を検出するときに事実上公開される検出器の動作が隠蔽され、埋込み検出の一連の動作も隠蔽され続けることにある。隠蔽されることによって、検出器の動作を解析することによる解明は直接的にはできなくなる。これにより、パラメータの変更でユーザーごとに異なる電子透かし(Fingerprinting)を埋込んだまま、埋込みシステムの基本構成を長期に変更すること無く運用できることになる。この効果は、プライベートな電子透かしにおいても、耐性向上の一つとして有効である。画像流通に際してセキュリティや履歴による立証のため電子透かしを使用することが検討されている.

本研究では、検出器を公開領域に出し、その領域で、プログラムを難読化により保護しようとすることと、埋め込み手法の高能率化を図ることを目標とした。検出器ソフトは難読化を施し、鍵に相当する情報の「場合の数」が膨大にできるため、探索するには計算量が多くなることにより、途中結果の数値に基づいて対応させた素数を復号鍵とし、次の処理に必須の定数値を復号鍵に対応する公開鍵で暗号化して、難読化の要素として、計算量を増大させ、解析時間もかかる構成となっている。又、電子透かしは，攻撃がある状況では，確定的な認証性は得られていないが，他のデジタル認証手段と比較して確率的には，同等レベルの証拠的価値があると考えられる.

計算量を見積もる難読化方式に加え、計算アルゴリズムを隠蔽する ROM 方式の難読化方式を検討し、実際に実現構成を行い、モノクロ画像での電子透かし埋込み実験を行った。埋込み領域が小さいため、周囲の切取りにも耐性があることが特徴である。一方、埋込みを拡大するには、ROM 容量の限界が有り、難読性の強さを減らして、階層的な形式にしていくことが考えられる。

次に、3 次元線形変換を行う電子透かし方式を検討した。1 次元、2 次元変換の電子透かし方式の研究は多いが、3 次元変換を行う方式はまだ少ない。本論文では、1 次元 2 次元 3

次元の性能比較を極力公平な形で行った。埋め込み方式に対し、埋込み手法の高能率化を図るために、DCT（離散コサイン変換）に変えてChirp変換とDCT変換を組み合わせる手法を開発した。電子透かし方式としての総合的な特性の評価を行った。多数の実験を行い、検証した。これにより検出器を公開でき、又、耐性の高い電子透かし方式を構成できた。

変換にDCTを用いて、１、２、３次元変換後に量子化による埋込みを行う電子透かし方式を比較した。従来単独の結果しか得られていなかったが、埋込みビット数を揃え比較し、定量的な特性比較を行うことができた。離散コサイン変換（DCT）を用いる方式においては、１次元よりも２次元の耐性が高く、更に２次元よりも３次元が高い耐性を持つことが示された。また、Chirp変換を用いる方式はDCTと同類の直交変換であることから、耐性に関する性能はほぼ同程度であった。しかし、Chirp 変換は非対称で有るため、平坦な画像部分にも有効な埋込みがなされ、DCTでは埋め込んでも埋め込まなくても検出ができ識別性が劣るのに比べ、平坦部にも埋込むことができることによる埋込み範囲の拡大という特徴を持つ。Chirp変換を用いる方式においては、１次元、２次元、３次元の比較を行ったが、特に３次元共にChirp変換を用いる3D-chirp変換方式は埋込み特性が悪いことが分かった。これは、提案したChirp 変換が１次元のモデルで設計したためと考えられた。これに関し、多数の検証実験を繰り返した結果、DCTとChirp変換を組み合わせる方式は特性がよくなることが分かった。最終的に、２D-DCTと1D-Chirp変換を組み合わせた合計で３次元の変換を用いると耐性が最も高く、埋込み範囲も最も広くなるという貴重な結果が得られた。

※印欄記入不要