

学位論文審査結果の概要

氏名	佐々木 隆幸
学位論文審査委員氏名	主査 長瀬 智行
	副査 小野口 一則
	副査 今井 雅
	副査 別宮 耕一
	副査 水田 智史
論文題目	二重情報ハイディング画像に関する研究 (A Study on Double Information Hiding Images)
審査結果の概要（2,000字以内）	
<p>本論文は、個人情報秘匿に、大量に、安全に、伝達することを目的とした研究論文である。ここに想定している個人情報とは画像と文書の2種類である。具体例には、病院患者の診察画像とカルテ文書を想定している。本論文の独創的な着眼点は3つである。1つ目は画像を暗号化するための正規直交関数系を擬似乱数系列で構築した点である。数多くの文献で採用される正規直交関数系は、超越関数グループに属する三角関数やハール関数などである。しかし、ここでは秘匿性を高めるために擬似乱数系列で構築した正規直交関数系を採用している。2点目は1枚の画像の中に大量の個人情報を埋め込むために1枚の画像と1枚の文書の埋め込みを可能にした点である。1枚の画像に二重に埋め込むことによって、種類の異なる個人情報を大量に伝達することができる。3点目は伝達途中における改ざんや傍受に対する安全対策強化のため、画像のビットプレーンを転置した点である。このビットプレーン転置には改ざん領域の集約化が可能となる利点、しかも伝達する画像の高画質化が可能となる利点がある。したがって、伝達途中の安全性向上が期待できることである。</p> <p>本論文は、3つの独創的な着眼点を中心にアルゴリズムの制作、実験、そして評価を多くの画像とイラストを用いて具体的に記述し、まとめたものであり、8章からなる。</p> <p>第1章は論文の目的と意義を詳細に述べている。</p> <p>第2章では、情報ハイディングの現状を述べている。6つの情報ハイディングの原理、模擬実験、長所、短所を紹介し、どの情報ハイディング技術にも長所と短所があることを示している。</p> <p>第3章では、「秘匿のために」に特化して述べている。5つの正規直交関数系を紹介し、秘匿にするために必要な条件を、秘匿化、平坦化、量子化の3つの観点から整理している。そして、本論文は独創的な着眼点である擬似乱数系列に基づく正規直交関数系を提案している。</p> <p>第4章では「多重化のために」に特化して述べている。5つの多重化を紹介している。すなわち、偶関数と奇関数による二重化、画素平面を2分割する二重化、画素空間を2分割する二重化、カラー別の三重化、ステガノグラフィと電子透かしを組み合わせた二重化である。多重化に最適な方法を探り、独創的な着眼点としてステガノグラフィと電子透かしによる画素空間の2層構造を提案している。</p> <p>第5章では、第三者による傍受や改ざんに対応する「安全性」について述べている。傍受や改ざん</p>	

による被害を軽減するためにどのような方法があるか、第三者が傍受や改ざんを起こさせないためにはどのような方法があるかについて述べている。すなわち、伝達する二重情報ハイディング画像の画質を高めることができ、しかも同時に改ざんに強い耐性をもつ安全対策として、本論文の独創的な点であるビットプレーン転置を提案している。

第6章では、前述してきた3つの提案を取り入れたアルゴリズムを制作し実験を行っている。伝達したい秘匿画像は秘匿画像 A 、伝達したい秘匿文書は秘匿文書 M である。それぞれを暗号化し画像 Q 、画像 C とする。これらを合成した画像が画像 G である。この画像 G をカギ画像 K に埋め込んだ画像が二重情報ハイディング画像 H である。これを受信者に伝達する。受信者は画像を再生するために次のことを行う。画像 H からカギ画像 K を引き算して画像 G を得る。その画像 G を画像 Q と画像 C に分離する。最後に、画像 Q から再生画像 A' を再生し、画像 C から再生文書 M' を再生する。

第7章では、再生した秘匿画像と秘匿文書の精度を測定し改ざんに対する評価を行っている。測定方法はピーク信号対雑音比と相関係数の2種類である。二重情報ハイディング画像 H とカギ画像 K および秘匿画像 A と再生画像 A' の類似性が高いこと、秘匿文書 M と再生文書 M' が一致することを確認している。

第8章は、本研究による成果が個人情報や秘匿に大量に安全に伝達することに役立つことを論じ、本論文をまとめている。

第1回審査会において予備審査における指摘事項を含めた論文審査および専門分野における口述試験を行った。さらに博士論文公聴会およびオンラインによる視聴配信を行い、論文内容の説明の後、質疑応答を行った。以上、本研究は情報セキュリティ分野において有用であり、総合的に判断した結果、論文審査および口述試験において合格と判定する。

学位論文の基礎となる参考論文

- (1) 佐々木 隆幸, 長瀬 智行, “擬似乱数系列でつくる二重情報ハイディング”, 情報処理学会論文誌 デジタルコンテンツ, Vol. 8, No. 1, pp. 11-19, 2020.
- (2) 佐々木 隆幸, 川守田 聡, “三重電子透かし画像づくり”, 職業能力開発報文誌, Vol. 31, No. 1, pp. 1-8, 2019.
- (3) T. Sasaki, T. Nagase “Constructing Digital Watermark Based on Orthogonal Functions”, 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), pp.140-143, 2018.
- (4) 佐々木 隆幸, 川守田 聡, “直交関数系でつくる電子透かし”, 職業能力開発報文誌, Vol. 30, No. 1, pp. 1-12, 2018.