A Study on Security Analysis of Image Encryption Algorithms

趙, 亮
九州大学システム情報科学府

https://doi.org/10.15017/25136

出版情報：九州大学, 2012, 博士（工学）, 課程博士
バージョン：
権利関係：

氏　　名　：　趙　　亮

論文題名　：　A Study on Security Analysis of Image Encryption Algorithms
（画像向け暗号方式の安全性解析に関する研究）

区　　分　：　甲

論　文　内　容　の　要　旨

近年､デジタルメディア情報に対応するセキュリティ上の問題はますます重要となりつつある。デジタルメディア情報に関する安全な通信のための方法として3種類が存在する｡伝統的な方法では、デジタルメディア情報が最初に圧縮され、次に暗号化される。第二の方法では、暗号化に続いて圧縮を行う。第三の方法は、デジタルメディア情報の暗号化と圧縮を同時に達成することである。上記の分析から、第二の方法と第三の方法は、デジタルメディアのセキュリティ関する二つの重要なトピックである｡これら2つの方法については多くの暗号化アルゴリズムが存在している。そのため実世界で実際に利用する前にこれらのアルゴリズムに関するセキュリティ分析を行うことは重要である。本論文では、デジタルメディア関する暗号化アルゴリズムのセキュリティを調査する。特に、本セキュリティ分析ではデジタル画像に関する暗号化アルゴリズムに焦点を当てる。

最初に、我々は画像の空間スクランブル暗号化アルゴリズムに関するスクランブリングの分析方法を示す。画像スクランブリングアルゴリズムは広くデジタル画像を暗号化するために使用されるため、対応する暗号文画像のスクランブリング度を測定する必要がある。本研究では、ビットプレーンに基づく評価方法を提案する。実験結果に基づき、本評価方法は画像スクランブリングアルゴリズムのスクランブリング度を測定するための候補として考えることができる。

次に、我々は画像暗号化アルゴリズムのセキュリティを分析する。ピクセルビットの配置換えによるカオスシステムを活用した画像暗号化アルゴリズムが(Pattern Recognition Lett., 31, pp: 347-354, 2010) において提案された。本研究では、この画像暗号化手法のセキュリティ上の欠点を分析するために, ある特定の選択平文攻撃を適用する。LiとLoによって提案された従来の攻撃(Signal Process., 91,pp:949-954, 2011) と比較し、我々の攻撃はより低い計算複雑性を実現している。更に 攻撃に対する改善対策手法も提示している。

最後に、我々はマルコフモデルに基づいたランダム化算術コードのセキュリティ分析を示す。算術コードの改善手法(ACMM)が論文 (Commun.Nonlinear Sci. Numer. Simulat., 16, pp: 2554-2562, 2011) において提案されている。本研究ではまず、異なる鍵が異なるメッセージの暗号化のために使用されるという条件の下での暗号文攻撃を示す。またメッセージの暗号化において異なる乱数シーケンスが使用されてもACMM は安全ではないことを示す。更にACMM がランダム化算術コード(RAC)(IEEE Trans. Multimedia, 8, pp: 905-917, 2006) と組み合わされて使用される場合の安全性の問題についても調査し, この複合暗号化方式(ACMM+RAC) も安全ではないことを示す。

〔作成要領〕

１．用紙はＡ４判上質紙を使用すること。

２．本文の文字サイズは１０．５ポイント（「論文内容の要旨」の文字は１２ポイント）
　１行の字数４４字，行数４２行、余白（左右２０mm，上下２５mm程度）をあけ，頁数は記入しない。

３．要旨は１頁に２，０００字程度（最大２頁以内を目安）にまとめる。

４．図表・図式等は随意に使用のこと。

５．氏名は外国人の場合，カタカナ表記（漢字圏の学生は漢字）で記入する。

６．論文題名は論文目録と合わせる。（外国語の場合は和訳をカッコ書きで付記する。）

７．区分には甲または乙を明示すること。

この原稿は，「九州大学博士学位論文内容の要旨及び審査結果の要旨」の原稿としてオフセット印刷するので，鮮明な原稿をクリップ止めで提出すること。