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

With the development of the computer and network technology, digital media information is used in many fields more widely, e.g., the industry, medical treatment and academic research. As a result, the corresponding security problem of the digital media information becomes increasingly significant. Moreover, to reduce the volume of the information for the transmission, the digital media information, in general, does the compression as one procedure. Based on this background, there are three kinds of methods for the secure communication of the digital media information. The traditional way is that the digital media information is first compressed to reduce the redundancy, and then encrypted to mask its meaning. However, in some application scenarios, the sender of the digital media information hopes encrypting the original data firstly and the network provider may compress the encrypted information without knowing any knowledge on the original and the corresponding data. Therefore, the second method which does the encryption followed by the compression has been attracted as the considerable research interest recently. Specially, for the second method, the research of the corresponding encryption algorithms is one of the main research topics in the digital media security. The third method is that the compression of the digital media information and the corresponding encryption can be achieved simultaneously. This research always considers the revision of the traditional compression algorithm (e.g., the Huffman coding and arithmetic coding). The purpose of it focuses on the reduction of the time and computation of each operation (i.e., the compression and encryption), and this kind of research makes the system flexible for the advanced digital media processing.

According to the above analysis, it can be found that the second method and the third method are two interesting topics in the field of the digital media security. In fact, there have been many encryption algorithms belonging to these two methods which are proposed for protecting the secrecy of the digital media information. Correspondingly, the security analysis of the proposed algorithms also becomes important before they are employed in practice. In this thesis, we investigate the security of some encryption algorithms about the digital media. In particular, as the still image is one of the main vehicles of the digital media information which causes that there have been many proposed image encryption algorithms, our security analysis primarily focuses on the still image related encryption algorithms. In our analysis, we try to identify some properties in the different encryption algorithms which can be exploited to break the corresponding ciphers.

In this thesis, there are 6 chapters as follows:

Chapter 1 provides the general outline on this research. We present the motivation and main contributions of this thesis in this chapter. Moreover, the organization of this thesis is also described.

Chapter 2 includes the introduction of two main branches on our research. On one hand, the basic information about the digital media security is provided. We introduce the concept and the application of the digital media firstly. Then, the background, motivation and corresponding research progress about the digital media security are presented. On the other hand, a short review about the security analysis of the digital media encryption is given. We provide the categories of the security and the target of the adversary in this chapter. Moreover, the classification of the attack scenarios and the measurement of the attack are also introduced. Finally, some examples about the security analysis of image encryptions are presented.

Chapter 3 presents a scrambling analysis of image spatial scrambling encryption algorithms. As the image scrambling algorithms (e.g., the Arnold cat map and Fibonacci transformation) are widely used to encrypt the digital image, the scrambling degree of the corresponding ciphertext image should be measured. In this chapter, an evaluation method based on the bit-plane has been proposed. Specially, the bit-plane theory is the core of this evaluation method. In the evaluation step, the spatial distribution entropy and centroid difference for the bit-plane are used to measure the scrambling degree of each bit-plane. As the relationship between the original image and most significant bit-plane to least significant bit-plane reduces gradually, we set a level decreasing-based weight for each bit-plane when the final scrambling degree is computed. The experiment results show that this evaluation method can find the scrambling degree for the image scrambling algorithms.

Chapter 4 addresses a security analysis of an image encryption algorithm of pixel bits and provides the comparison with the previous state of the art. We use the chosen-plaintext attack for an image scrambling encryption algorithm of pixel bits which was provided by Ye published on *Pattern Recognition Letters* in 2010. Our attack reveals the encryption vectors which can substitute for the secret keys. Compared with the former analysis work achieved by Li and Lo which was published on *Signal Processing* in 2011, our attack has the lower complexity which implies that our attack is more efficient than Li and Lo's attack. Moreover, a suggested improvement against our attack is presented in details. In fact, we introduce the self-correlation which comes from the idea of the self-adaptive encryption, proposed by Chen et al. published on *Journal of Software* in 2005, into the original algorithm to enhance the security. The final simulations show that the suggested improvement may be better than the original algorithm.

Chapter 5 is concerned with a security analysis of the randomized arithmetic codes based on the Markov model and the further analysis on the corresponding improvement. The randomized arithmetic code is a kind of symmetric-key algorithm which can achieve the encryption and the compression for the digital media information simultaneously. In this chapter, we first put forward a formal definition of a randomized arithmetic code based on the Markov model (ACMM) which is proposed by Duan et al. published on *Communications in Nonlinear Science and Numerical Simulation* in 2011, and then explore the security of ACMM. Our analysis shows that ACMM is insecure under the ciphertext-only attack (COA) even if a new pseudorandom bit sequence is used for the encryption of each message. Moreover, an enhanced algorithm which combines ACMM with the randomized arithmetic coding (RAC), introduced by Grangetto et al. and published on *IEEE Transactions on Multimedia* in 2006, is presented. However, the security analysis also shows that ACMM+RAC is insecure under the COA. Finally, we present the simulation results to confirm the proposed attacks.

Chapter 6 summarizes the results of this thesis and describes some corresponding future works.

〔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。