成蹊大学理工学研究報告
J. Fac. Sci.Tech., Seikei Univ.
Vol.59 No.1･2 (2022)pp.17-20

光による画像暗号及び符号化について

中野　和也*1

Image Encryption and Encoding based on Optical Systems

Kazuya NAKANO*1

ABSTRACT：Optical encryption and encoding techniques are attractive to researchers, because they can optically encrypt an image at high speed. Especially, double random phase encoding (DRPE) is known as a typical optical encryption and encoding method. DRPE encrypts images by random phase modulations in the spatial and Fourier plane. Many researchers have reported the security analysis of DRPE. It is important to investigate the security strength against some attacks, such as known-plaintext attack (KPA). In this paper, we introduce the known-plaintext attack-based analysis of DRPE. DRPE is easy to expand because the optical system of DRPE is simple. Therefore, there are various types of DRPE, such as DRPE based on fractional Fourier transform and Fresnel transform. However, the optical systems are based on coherent light. Therefore, we introduce the proposed incoherent optical system of DRPE. In the future, we expect new applications based on DRPE algorithm for a camera and sensor.

Keywords：optical encryption, Fourier optics, image processing

(Received December 1, 2022)

1．はじめに

光による暗号及び符号化に関する技術を紹介すると共に筆者が取り組んできた研究内容の一部について述べる。光の性質を利用した画像の暗号･符号化について様々な手法[1]が提案されているが、代表的な光暗号・符号化手法として二重ランダム位相暗号化(DRPE: Double Random Phase Encoding)[2]がある。これは実面とフーリエ面に配置されたランダム位相マスクを用いてコヒーレント光のランダム位相変調を行うことで実現される．DRPEは2つのレンズと2つのランダム位相マスクを配置した光学系から成り，暗号時と復号時の鍵はフーリエ面に置いたランダム位相マスクとなる。DRPEはRefregier博士とJavidi博士によって1995年に提案されてから現在に至るまで多くの研究者によりそのセキュリティ評価や拡張手法の提案が報告されている。ここでは、筆者が取り組んできたDRPEのセキュリティ評価や拡張手法について紹介する。

*1：理工学部理工学科准教授（kazuya-nakano@st.seikei.ac.jp）

2．セキュリティ評価

DRPEは光による暗号と考えられているため、離散数学に基づく暗号技術と同様に、各種攻撃に対する耐性評価が重要である。その攻撃としては、暗号文単独攻撃（COA: ciphertext-only attack）、選択暗号文攻撃（CCA: Chosen-ciphertext attack）、選択平文攻撃（CPA: Chosen-plaintext attack）、既知平文攻撃（KPA: known-plaintext attack）などがある。ここではKPAについて述べる。KPAとは、攻撃者が何らかの方法で平文とそれに対する暗号文を入手した際に、その平文暗号文の組から鍵となる情報を解読する攻撃である。DRPEのKPAについては1組の既知ペアを用いた研究[3]や複数の既知ペアを用いた研究[4][5]がある。特に複数の既知ペアを用いる手法は、2値画像のように画素値がゼロの画素が多く含まれる平文画像に対しては非常に強力な攻撃手法であることが知られている。しかし、実際に光によりDRPEを実装した場合、得られる暗号画像の振幅及び位相情報にはノイズが存在する。そこで、Fig.1に示すようにノイズを段階的に付加し、その時のKPAの結果を分析した[6]。暗号画像の

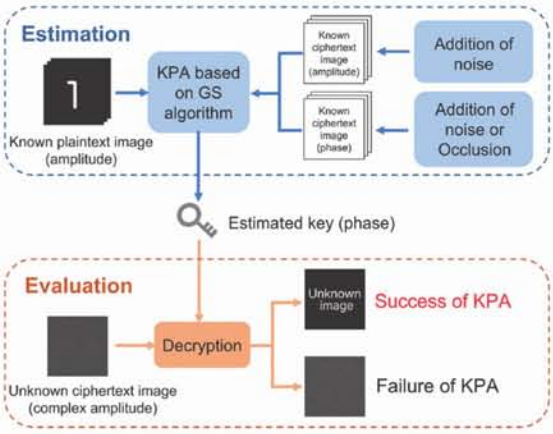

Fig.1　Analysis of DRPE based on KPA. [Reprinted/Adapted] with permission from [ref 6] © The Optical Society.

フーリ振幅に段階的に変えたノイズを付加し、その暗号画像を用いてKPAの成否について調査した結果をFig.2に示す。横軸は付加したガウシアンノイズの標準偏差、縦軸は未知の平文画像とKPAで推定した鍵で復号した未知暗号画像との間で算出した相関係数である。相関係数が 1 に近いほどKPAによる鍵解読は成功、0 に近いほど失敗を意味する。暗号画像のフーリエ振幅にノイズがない場合、複数組の既知ペアを用いたKPAによる鍵の解読は成功する。次に暗号画像のフーリエ振幅にノイズを加えた場合、1 組の既知ペアを用いたKPAでは鍵の完全な解読までは至らないが、複数組の既知ペアのKPAではノイズ量に関係なく鍵解読が成功することがわかる。このことから、暗号画像のフーリエ振幅にノイズが生じたとしても、複数組のKPAには影響しないといえる。次に、暗号画像のフーリ位相に段階的に変えたノイズ付加し、その暗号画像を用いてKPAの成否について調査した結

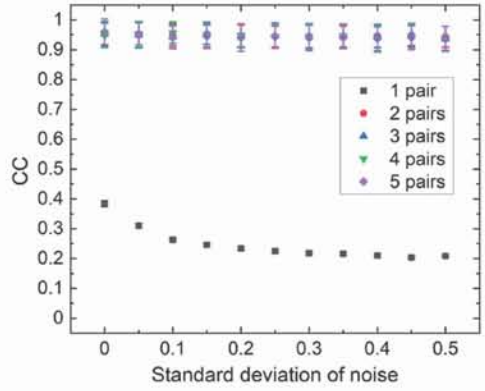

Fig.2　Results of KPA when noise was added to Fourier amplitude. [Reprinted/Adapted] with permission from [ref 6] © The Optical Society.

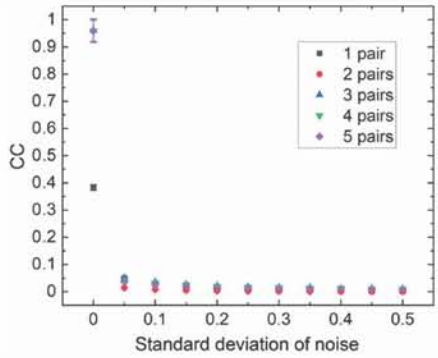

Fig.3　Results of KPA when noise was added to Fourier phase. [Reprinted/Adapted] with permission from [ref 6] © The Optical Society.

果をFig.3 に示す。横軸が付加したガウシアンノイズの標準偏差、縦軸は未知の平文画像とKPAで推定した鍵で復号した未知暗号画像との間で算出した相関係数である。暗号画像のフーリエ位相にノイズを加えると、既知のペア数によらずKPAによる鍵の解読が困難になる。

3．拡張手法

DRPEの拡張について述べる。セキュリティ評価と並び、DRPEは多くの拡張が提案されている。例えば、DRPEが用いる変換に非整数次フーリエ変換 [7]やフレネル変換 [8]を利用する手法などが挙げられる。非常に多くの手法が現在も提案されており、今後も盛んに研究されると予想される。また、従来のDRPEではコヒーレント光での実装が必須であり、光源としてレーザーを使用しなければならなかった。しかし、インコヒーレント光で実装できるようになると、LEDといった光源を使用することができるため、暗号カメラやセンサーといったアプリケーションにもつながり、今後の応用への幅が広がると考える。そこで、インコヒーレント光で実装可能なDRPE拡張 [9]について説明する。

提案したDRPEのインコヒーレント光学系をFig.4 に示す。この光学系ではレンズアレイを用いて光によるベクトル行列演算を行う。このとき、２つのンズアレイに挟まれた位置に配置されたマスクを鍵とする。マスクにはDRPEの鍵情報に相当する画素ごとの透過率が設定されている。そして、レンズアレイで集光された光の強度情報を数値計算により後処理をしたものが暗号画像となる。Fig.5 にマスク乗算までを光実装、後処理や復号を数値計算で行った結果を示す。このとき、平文となる画像として 4 画素の市松模様を使用した。Fig.5 (a)に正しい鍵で復号した結果、Fig.5 (b)に誤った鍵で復号した結

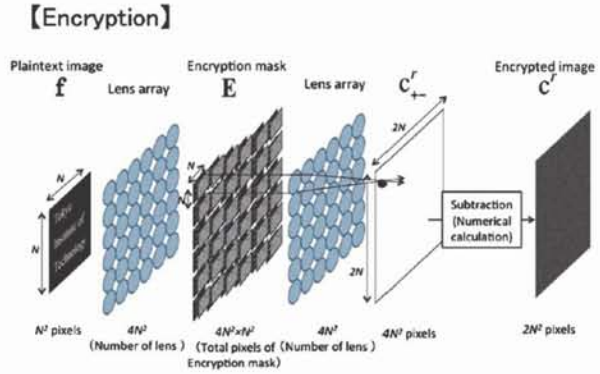

Fig.4 Optical system of incoherent DRPE. [Reprinted/Adapted] with permission from [ref 9] © The Optical Society.

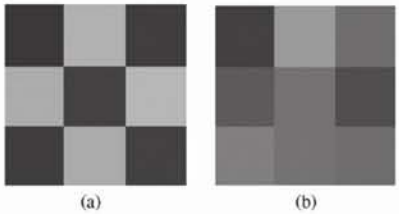

Fig.5 Decrypted images. [Reprinted/Adapted] with permission from [ref 9] © The Optical Society.

果を示す。このように、正しい鍵を用いれば平文画像を得ることができるが、間違った情報で復号した場合、平文画像を得ることができないことを確認している。

4．最後に

光によって物理的に暗号・符号化を行う手法について述べた。DRPEを始めとする光学的手法は数値計算、光学実装どちらも可能で拡張のしやすさから、セキュリティに限らず画像を用いた様々なアプリケーションの提案につながると期待し今後も進めていく。

参考文献

1) B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S Millán, N. K Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A Alfalou, C Brosseau, C. Guo, J. T Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W H Pinkse, A. P Mosk and A. Markman. "Roadmap on optical security", J. Opt. 2016;18(8):083001.

2) P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, pp. 767–769 (1995).

3) X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. 31, pp. 1044–1046 (2006).

4) G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," Appl. Opt. 46, pp. 5257–5262 (2007).

5) K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs," Appl. Opt. 53, pp. 6435–6443 (2014).

6) K. Nakano and H. Suzuki, "Known-plaintext attack-based analysis of double random phase encoding using multiple known plaintext–ciphertext pairs," Appl. Opt. 61, pp. 9010–9019 (2022).

7) G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. 25, pp. 887–889 (2000).

8) G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. 29, pp. 1584–1586 (2004).

9) K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Encrypted imaging based on algebraic implementation of double random phase encoding," Appl. Opt. 53, pp. 2956–2963 (2014).