engineering proceedings

MDPI

Proceeding Paper

An Asymmetric Optical Cryptosystem Using Physically Unclonable Functions in the Fresnel Domain †

Vinny Cris Mandapati [1,*], Shashi Prabhakar [2], Harsh Vardhan [1], Ravi Kumar [1], Salla Gangi Reddy [1], Sakshi [3] and Ravindra P. Singh [2]

[1] Department of Physics, SRM University—AP, Amaravati 522502, India; harshvardhan_r@srmap.edu.in (H.V.); ravi.k@srmap.edu.in (R.K.); gangireddy.s@srmap.edu.in (S.G.R.)
[2] Physical Research Laboratory, Navrang Pura, Ahmedabad 380009, India; shaship@prl.res.in (S.P.); rpsingh@prl.res.in (R.P.S.)
[3] Department of Chemical Engineering, Ben-Gurion University of the Negev, P.O. Box 653, Beer-Sheva 8410501, Israel; sakshich289@gmail.com
* Correspondence: vinnycris_m@srmap.edu.in
† Presented at the International Conference on "Holography Meets Advanced Manufacturing", Online, 20–22 February 2023.

Abstract: In this paper, we propose a new asymmetric cryptosystem for phase image encryption, using the physically unclonable functions (PUFs) as security keys. For encryption, the original amplitude image is first converted into a phase image and modulated with a PUF to obtain a complex image. This complex image is then illuminated with a plane wave, and the complex wavefront at a distance d is recorded. The real part of the complex wavefront is further processed to obtain the encrypted image and the imaginary part is kept as the private key. The polar decomposition approach is utilized to generate two more private security keys and to enable the multi-user capability in the cryptosystem. Numerical simulations confirm the feasibility of the proposed method.

Keywords: asymmetric cryptosystems; physically unclonable functions; polar decomposition method

Citation: Cris Mandapati, V.; Prabhakar, S.; Vardhan, H.; Kumar, R.; Reddy, S.G.; Sakshi; Singh, R.P. An Asymmetric Optical Cryptosystem Using Physically Unclonable Functions in the Fresnel Domain. *Eng. Proc.* **2023**, *34*, 8. https://doi.org/10.3390/HMAM2-14124

Academic Editor: Vijayakumar Anand

Published: 6 March 2023

1. Introduction

The advancements in data transfer and storage technology have prompted new challenges in guaranteeing its secure transmission. A huge amount of data (images, passwords, bank details, etc.) is transmitted daily through open channels, making it vulnerable to intruders. To ensure safe transmission, several optical and digital encryption techniques have been explored. The first optical cryptosystem, i.e., the double-random phase-encoding (DRPE) technique, was demonstrated back in 1995. This employs a simple 4-f setup to encode a two-dimensional image into a white noise-like distribution [1]. With time, many variants of DRPE in other transform domains, such as fractional Fourier, gyrator, Mellin, Hartley, wavelet, and cosine transforms, have been explored to improve data transmission security [2,3]. Various other optical approaches like diffractive imaging and interference methods, as well as polarization encoding, were also explored to design new and sophisticated optical cryptosystems [2]. Most of these methods are symmetric in nature and vulnerable to different kinds of attacks [3,4]. To resist these attacks, several attempts were made to develop asymmetric cryptosystems that offer nonlinearity and serve as secure options against well-known attacks, such as known plaintext attacks, chosen plaintext attacks and cipher text-only attacks [3]. Although several cryptosystems have been developed in recent years, the search continues for newer advanced methods which can provide better security with less practical complexity and are computationally efficient.

In this paper, we present a new asymmetric cryptosystem using physically unclonable functions as security keys. Mostly, the security keys used in the existing image encryption methods are computer-generated noise-like distributions with uniformly distributed

histograms. On the other hand, the PUFs used in this paper are relatively unbreakable non-algorithmic functions which are difficult to reproduce. PUFs carry unique signatures due to the random and stochastic processes involved in their generation [5]. The PUFs employed here are obtained as random speckles from the coherence light source when passed through a ground glass diffuser. Statistically, an attacker may retrieve the computer-generated keys if they have partial/full knowledge of the cryptosystem; however, since PUFs are generated physically, it is difficult to retrieve them through iterative algorithms.

2. Proposed Technique and Results

The proposed technique is designed in the Fresnel transform domain to make it lensless. Polar decomposition (PD) process aids in making the system asymmetric and enables multiuser capabilities [4]. PUFs are generated experimentally, as discussed in Ref. [5]. PD essentially factorizes the input matrix into a set of linearly independent matrices, i.e., one rotational matrix and two symmetric matrices. To reconstruct the input matrix or image, only the rotational matrix and one of the symmetric matrices is required [4].

For encryption, the first input image, $f(x,y)$, is phase-encoded as $\exp(i\pi f(x,y))$ and modulated with the first PUF phase function as $A(x,y) = \exp(i\pi f(x,y)) \times PUF1$. The complex image $A(x,y)$ is then Fresnel-propagated with distance d_1, to obtain the complex wavefront $A'(u,v)$. Next, the real and imaginary parts of $A'(u,v)$ are separated; the real part undergoes the polar decomposition process; and the imaginary part is retained as the first private key. The PD will result in three images, i.e., R: the rotational image; and U and V: the positive symmetric matrix images. U and V are stored as the private keys and can be distributed to two different users for individual decryption. The rotational matrix part $R(u,v)$ is further Fresnel-propagated to a distance d_2, which results in the complex wavefront $B(u',v')$. This complex amplitude image is then modulated with the second PUF2 to obtain the final encrypted image $E(u',v')$. The original image can be recovered through the reverse process using all the correct keys. The flowchart of the encryption and decryption process is illustrated in Figure 1a,b, respectively.

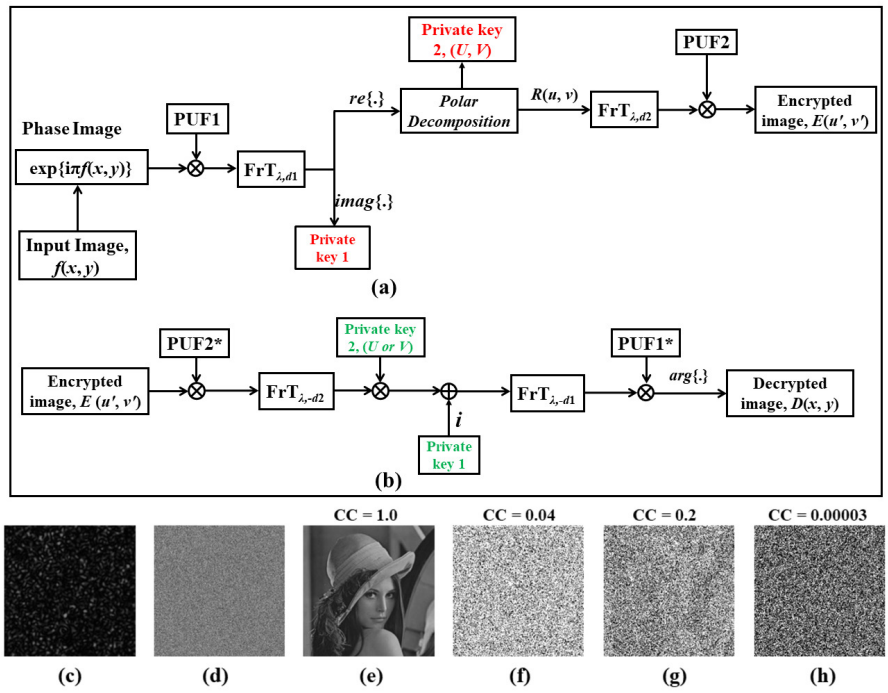

Figure 1. Flowchart for (**a**) encryption process; (**b**) decryption process; (**c**) PUF used (order of optical vortex = 2); (**d**) encrypted image. Decrypted image with (**e**) all correct keys (**f**) deviation in d_1 = 2 mm (**g**) deviation in d_2 = 2 mm (**h**) using wrong PUF (order of optical vortex = 3). The red colored details denotes private keys 1 and 2 in encryption process and green colored details denotes the keys in decryption process; '*' represents the complex conjugate of the function.

The validity of the proposed technique was verified by performing numerical simulations on MATLAB^{TM} (Mathworks, Natick, MA, USA, version 2022(b)) on an AMD Ryzen 5-5500 U laptop, with 16 GB RAM. The 'Lena' image of 256 × 256 pixels is used as the input image. Figure 1c shows one of the PUFs used for encryption and the final encrypted image is shown in Figure 1d, whereas the decrypted image with all correct keys is shown in Figure 1e. The sensitivity of security keys is also checked by performing decryption with a small deviation in Fresnel parameters or by using wrong keys. The corresponding results are shown in Figure 1f–h. The results confirm that the proposed method is feasible and sensitive to the keys.

3. Concluding Remarks

In conclusion, a new asymmetric optical cryptosystem with multiuser capabilities is proposed using polar decomposition in the Fresnel domain. The method has a large set of keys which include the Fresnel propagation parameters, two variable PUFs, and three private keys generated during the encryption process. The PUFs used as security keys are difficult to replicate, a fact which improves the robustness against various attacks. The sensitivity of all the keys is also verified. The work is a subject of our ongoing research and will be presented in detail in the near future.

Author Contributions: Conceptualization, S.P., R.K., S.G.R. and R.P.S.; methodology, V.C.M., H.V., S.P., S.G.R., S. and R.K.; software, V.C.M., H.V., S. and R.K.; validation, V.C.M. and H.V.; formal analysis, V.C.M. and S.; investigation, V.C.M., H.V. and S.; resources, S.G.R., S.P. and R.P.S.; data curation, V.C.M. and H.V.; writing—original draft preparation, V.C.M., H.V., R.K. and S.G.R.; writing—review and editing, R.K., S.G.R. and R.P.S.; visualization, V.C.M. and H.V.; supervision, R.K. and S.G.R.; project administration, R.K. and S.G.R. All authors have read and agreed to the published version of the manuscript.

Funding: The research was granted by the Science and Engineering Research Board (SERB), the Government of India, under the start-up research grant (Grant No. SERB/SRG/2019/000857), and SRM University—AP for seed research grants under SRMAP/URG/CG/2022-23/006 and SRMAP/URG/E&PP/2022-23/003 to S.G.R.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data related to the paper are available from the corresponding authors upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Refregier, P.; Javidi, B. Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
2. Nischal, K.N. *Optical Cryptosystems*; IOP Publishing Ltd.: Bristol, UK, 2020; pp. 2-1–2-18.
3. Javidi, B.; Carnicer, A.; Yamaguchi, M.; Nomura, T.; Pérez-Cabré, E.; Millán, M.S.; Markman, A. Roadmap on Optical Security. *J. Opt.* **2016**, *18*, 083001. [CrossRef]
4. Kumar, R.; Quan, C. Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform. *Opt. Lasers Eng.* **2022**, *120*, 118–126. [CrossRef]
5. Vantiha, P.; Manupati, B.; Muniraj, I.; Anamalamudi, S.; Reddy, S.G.; Singh, R.P. Augmenting Data Security: Physical Unclonable Functions for linear canonical transform based cryptography. *Appl. Phys B* **2022**, *128*, 183. [CrossRef]