An asymmetric optical cryptosystem using physically unclonable functions in the Fresnel domain

Vinny Cris M[a,*], Shashi Prabhakar[b], Harsh Vardhan[a], Ravi Kumar[a], Salla Gangi Reddy[a], Sakshi[c], Ravindra P Singh[b]

[a]Department of Physics, SRM University - AP, Andhra Pradesh - 522502, India
[b]Physical Research Laboratory, Navrang Pura, Ahmedabad-380009, India
[c]Ben-Gurion University of the Negev, P. O. Box 653, Beer-Sheva 8410501, Israel
*Email: vinnycris_m@srmap.edu.in

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 to a phase image and modulated with a PUF to get the 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 get the encrypted image and the imaginary part is kept as the private key. Polar decomposition approach is utilized for generating two more private security keys and to enable the multi-user capability in the cryptosystem. Numerical simulations confirm the feasibility of the proposed method.

1. Introduction

The advancements in data transfer and storage technology have prompted new challenges for its secure transmission. Everyday a huge amount of data (images, passwords, bank details etc.) is transmitted through open channels, making it vulnerable to intruders. To ensure the safe transmission, several optical and digital encryption techniques have been explored. The first optical cryptosystem, i.e., double random phase encoding (DRPE) technique was demonstrated back in 1995 which 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 the security [2, 3]. Various other optical approaches like diffractive imaging and interference methods, and polarization encoding were also explored to design new 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 are secure options against well-known attacks such as known plaintext attack, chosen plaintext attack 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 having uniformly distributed histogram. On the other hand, the PUFs used in this paper are relatively unbreakable non algorithmic functions which are difficult to be reproduced. PUFs carry unique signatures due to the random and stochastic process involved in their generation [5]. The PUFs employed here are obtained as random speckles from the coherence light source passed through a ground glass diffuser. Statistically, an attacker may retrieve the computer-generated keys if he/she will have partial/full knowledge of the cryptosystem, but since the PUFs are generated physically it would be 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 the multiuser capabilities [4]. PUFs are generated experimentally as discussed in [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, first the input image, $f(x,y)$ is phase encoded as $\exp(i\pi f(x,y))$ and modulated with the first PUF phase function as $A(x,y) = \exp(i\pi f(x,y)) * PUF1$. The complex image $A(x,y)$ is then Fresnel propagated with distance d_1, to get, 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 into three images, i.e., R: the rotational image; and U, V: positive symmetric matrix images. U, V will be 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 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 1 (a) and 1(b), respectively.

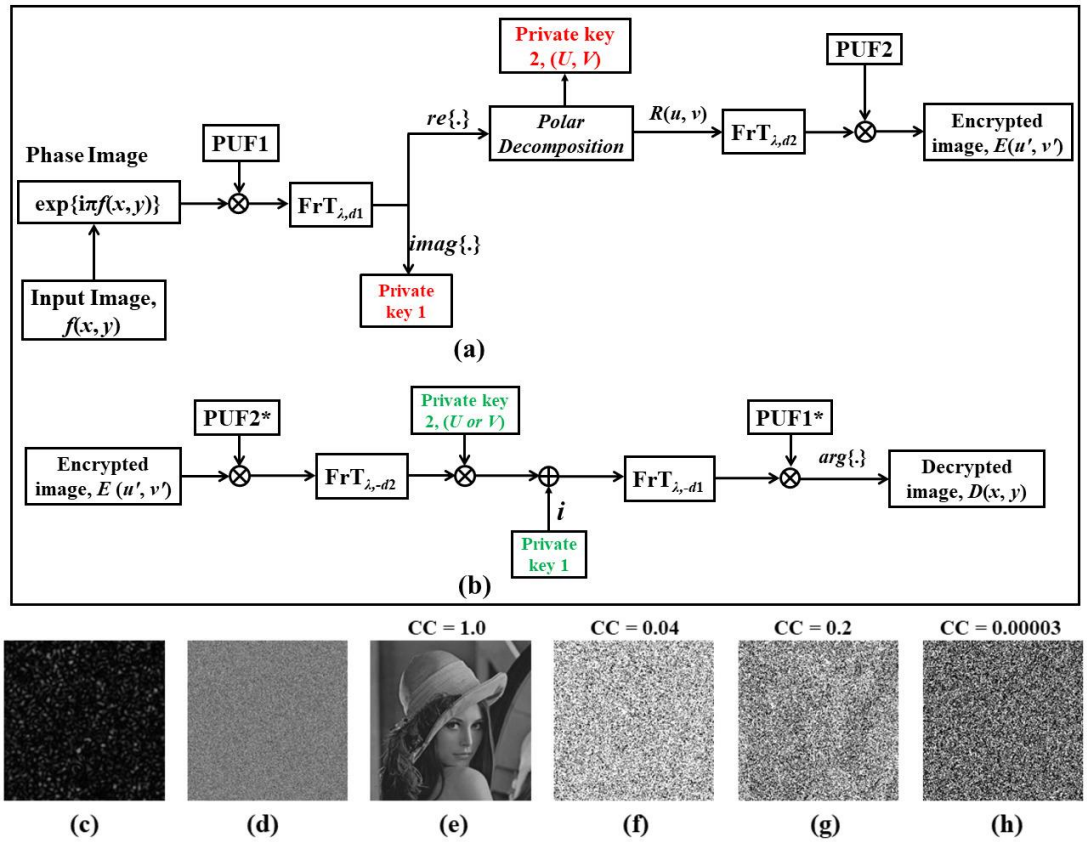

Figure. 1: Flowchart for (a) encryption process; (b) decryption process; (c) PUF used (order of optical vortex=2); (d) encrypted image; Decrypted image with (e) all correct keys (f) deviation in d_1 = 2mm (g) deviation in d_2 = 2 mm (h) using wrong PUF (order of optical vortex = 3).

The validity of the proposed technique was verified by performing numerical simulations on MATLAB™ (version 2022(b)) on an AMD Ryzen 5 5500U Laptop with 16GB RAM. The 'Lena' image having 256×256 pixels is used as the input image. Figure 1(c) shows one of the PUFs used for encryption and the final encrypted image is shown in 1(d), whereas the decrypted image with all correct keys is shown in Figure 1(e). The sensitivity of security keys is also checked by performing decryption with small deviation in Fresnel parameters or using wrong keys. The corresponding results are shown in Figures 1(f)-(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 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 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.

References

[1] Refregier, P.; Javidi, B. Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Optics Letters* 1995, 20, 767-769.

[2] Nischal, K.N. *Optical Cryptosystems*; IOP Publishing Ltd: Bristol, UK, 2020; pp 2-1-2-18.

[3] Javidi, B. et.al, Roadmap on Optical Security, *Journal of Optics* 2016, 18:083001.

[4] Kumar, R.; Quan, C. Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform, *Optics and Lasers in Engineering* 2022, 120, 118-126; https://doi.org/10.1016/j.optlaseng.2019.03.024

[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, *Applied Phys B* 2022, 183; https://doi.org/10.1007/s00340-022-07901-z