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] , RP 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

Objectives

- To design a new asymmetric optical cryptosystem using PUFs
- To enable multiuser capability using polar decomposition method..
- To study the key sensitivity and robustness of the proposed method.

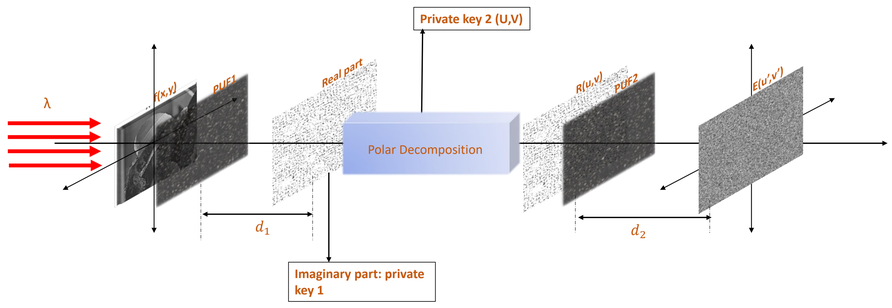


Fig.1. encryption process

Proposed Technique

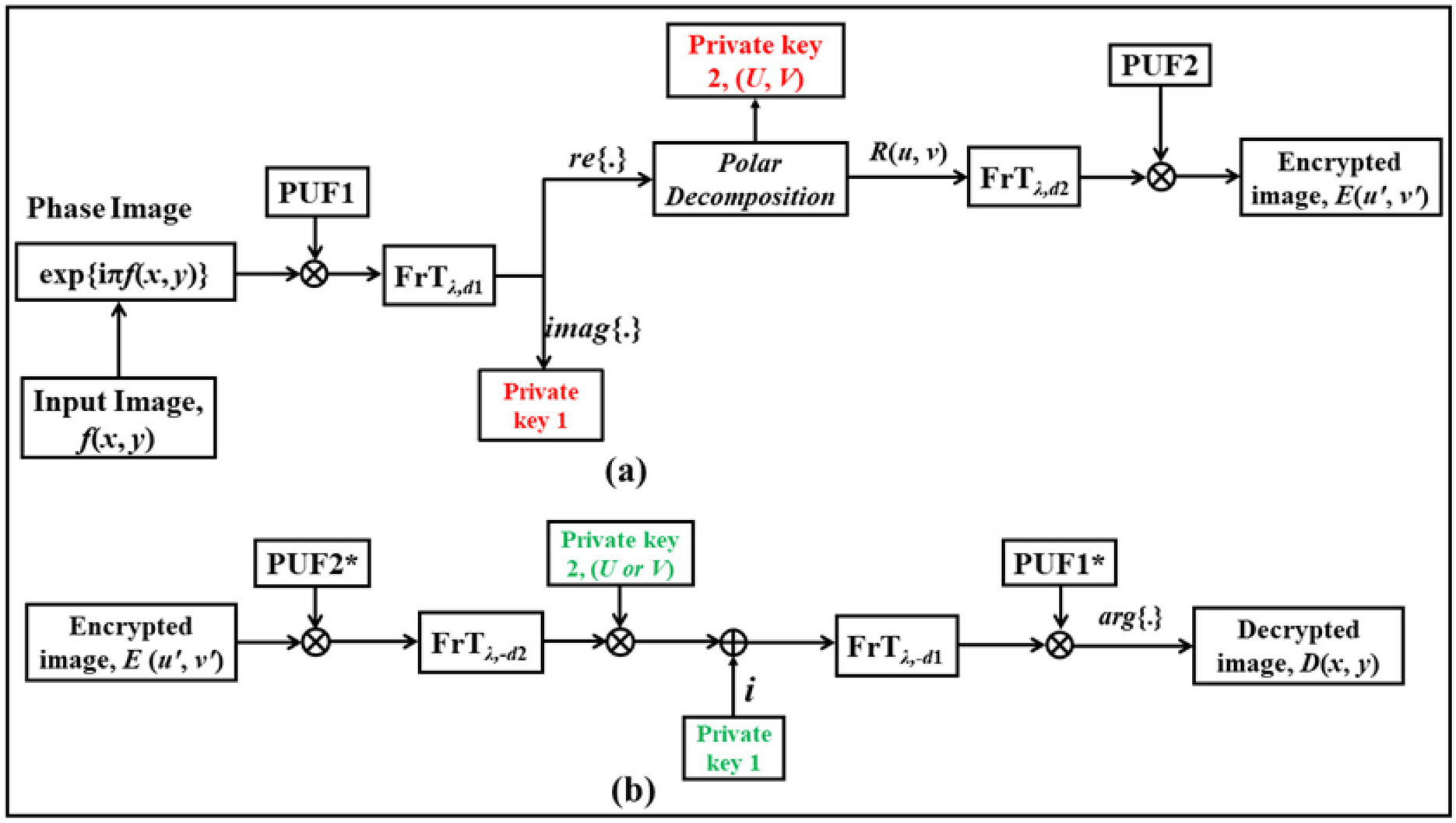
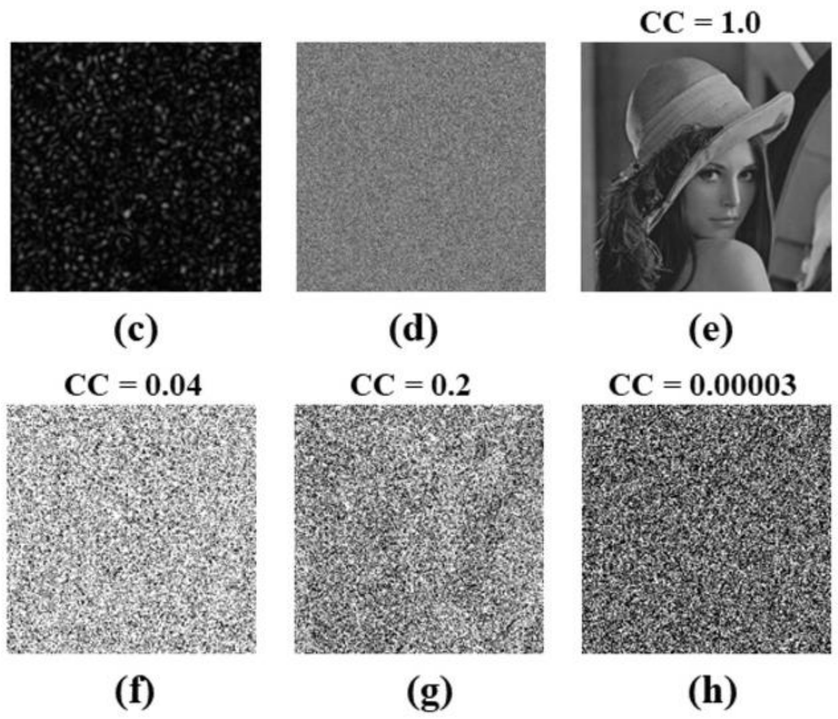
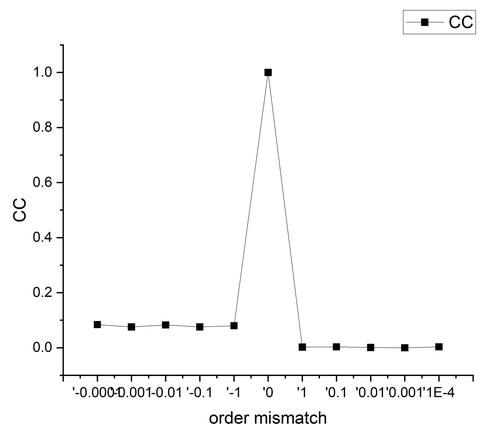


Fig.3. Flowchart explaining the (a) encryption and (b) decryption process.

Results





(i)

Fig.3. (c) PUF of OV(m=2) (d) encrypted image (e) decrypted image with all the correct parameters (f) decrypted image with deviation in Fresnel distance d1=2 mm (g) deviation in Fresnel distance d2 = 2mm (h) using wrong PUF of OV(m =3) with corresponding CC values. (i) CC plot for deviation in fractional order OV- PUF

Theory

$$A(x,y) = (\exp(i\pi f(x,y)) * PUF1)$$

$$A'(x,y) = \Im_{\lambda}^{d_1}[A(x,y)]$$

$$PD\{real\{A'(x,y)\}\} = [R \quad U \quad V]$$

$$B(x'',y'') = \Im_{\lambda}^{d_1}[R(x',y')]$$

$$E(x",y") = (B(x',y') * PUF2)$$

Conclusions

- 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