Plasmonics Based Keys for Image Encryption That Uses Exclusive OR Logic Operation

N.K. Nishchal[1], A. Fatima[1], I. Mehra[1], D. Kumar[1]

[1]Indian Institute of Technology Patna, Patna, Bihar, India

Abstract

Optical encryption has become a significant research field due to its remarkable advantages [1-5]. The unique features of plasmonics have drawn researchers' attention towards the role which it can play in information security [3 & 4]. The electric field is greatly enhanced when a metallic nanoparticle is illuminated by an appropriate electromagnetic field. The distribution and enhancement of this electric field is highly sensitive to the dimensions of the nanoparticle. This particular sensitivity is used to generate keys for image encryption. The dimension of the nano-object and the illuminating wavelength offer greater degrees of freedom for the security keys. In this paper, an optical encryption scheme is proposed which uses exclusive OR (XOR) operation. The first step consists of constructing the encryption keys. This process is carried out using COMSOL Multiphysics® software. The Wave Optics Module (frequency domain) is employed for this purpose, wherein a gold nanosphere of radius 10 nm is constructed under the geometry node. A PML of thickness half the wavelength surrounds the geometry to restrict the domain under calculation. The nanosphere is illuminated with a plane wave with electric field along the z-axis. The direction of propagation is along the x-axis. The scattered field is evaluated by solving the Maxwell's equations. The values of the scattered electric field are evaluated at specific spatial points using the Cut Point 3D function. These values are then used to construct the keys. These keys provide increased security to the cryptosystem because of the fact that electric field values are sensitive to the shape, dimension of the nano-object, the illuminating wavelength, and the selected spatial points.
The second step consists in encrypting a binary input image using the generated keys.

The numerical study has been carried out using COMSOL Multiphysics®. Initially, a gold nanosphere of radius 10 nm, as shown in Fig. 1 is impinged with electric wave of wavelength 550 nm (on COMSOL®). The electric field at specific points is evaluated to construct the amplitude key. Figure 2 shows the input image of size 32 × 32 pixels. This input image is encrypted using XOR operation scheme as shown in Fig. 3. Figure 4 shows the decrypted image obtained after using the correct key. The benefits of the proposed scheme are as follows:
(1) The keys generated through plasmonics offer higher security as they cannot be replicated without the knowledge of the shape and dimensions of the nano-object and other physical parameters.
(2) The spatial points chosen for the evaluation of electric field enhance the security of this cryptosystem.
(3) The plasmonics based keys have been applied using XOR operation. This scheme is non-

iterative and does not require recording of the keys in the form of holograms and thus offers flexibility in the design of cryptosystem.

Reference

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, 767-769 (1995).

[2] S. K. Rajput and N. K. Nishchal, “Known- plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform,” Appl. Opt.52, 871-878 (2013).

[3] T. Grosges and D. Barchiesi, “Towards nanoworld-based secure encryption for enduring data storage,” Opt. Lett. 35, 2421-2423 (2010).

[4] M. Francois, T. Grosges, D. Barchiesi, and R. Erra, “Generation of encryption keys from plasmonics,” PIERS Online 7, 296-300 (2011).

[5] H. Y. Tu, C. J. Cheng, and M. L. Chen, “Optical image encryption based on polarization encoding by liquid crystal spatial light modulator,” J. Opt. 6, 524-528 (2004).

Figures used in the abstract

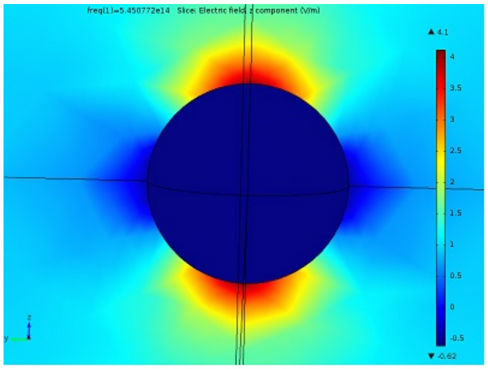

Figure 1: Nanosphere generated through COMSOL Multiphysics software.

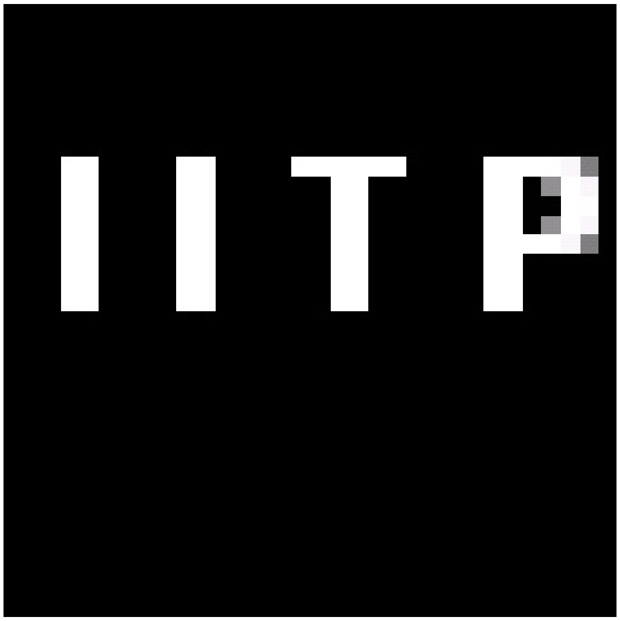

Figure 2: Input image to be used for encryption.

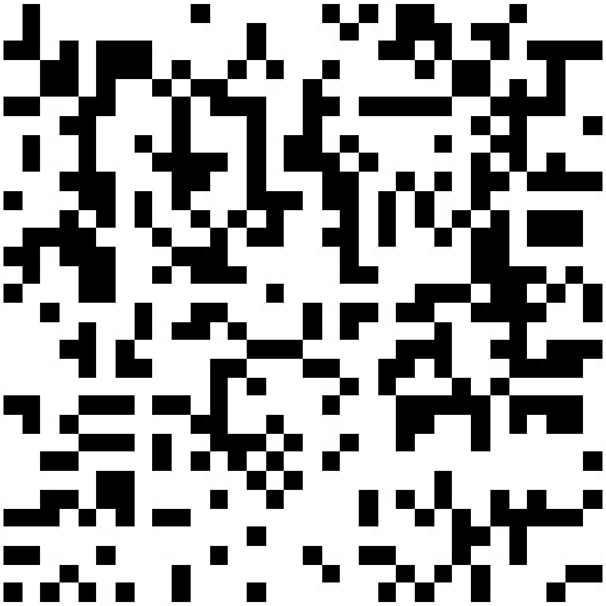

Figure 3: Encrypted image.

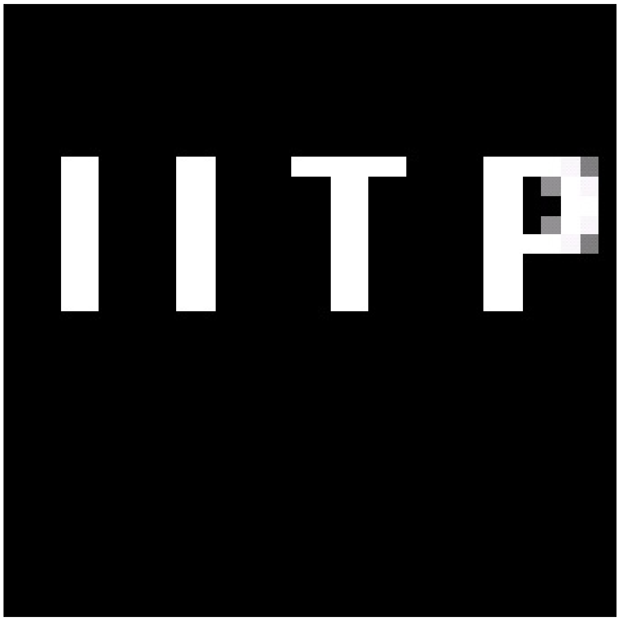

Figure 4: Decrypted image obtained after using the correct keys.