Plasmon Based Keys for Image Encryption that uses Exclusive OR Logic Operation

Areeba Fatima, Isha Mehra, Dhirendra Kumar, and Naveen K. Nishchal
Department of Physics, Indian Institute of Tehnology Patna, Patliputra, Patna 800013
E-mail id: nkn@iitp.ac.in, areeba@iitp.ac.in

ABSTRACT

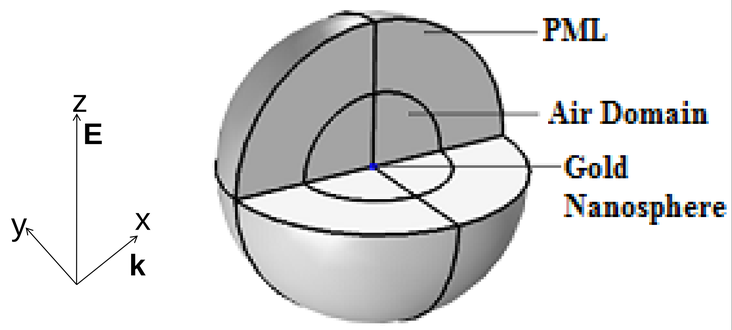
We present a study of plasmon based encryption scheme. Generation of plasmons is a resonance phenomenon and is thus sensitive to the shape, size and the illuminating wavelength. The electric field distribution changes when any one of these parameters is changed. This feature is exploited to develop an encryption key that has higher degrees of freedom. The values of the electric field at various spatial points are evaluated using finite element method (FEM) of COMSOL and these values are used to construct the desired key.

NUMERICAL MODEL & COMPUTATIONAL METHOD

We aim to evaluate the electric field distribution developed due to scattering of the electromagnetic field by the metallic nanosphere (gold nanosphere). Thus, we solve the Maxwell's Eq., which is

$$\nabla \times \mu_r^{-1}(\nabla \times \mathbf{E}) - k_0^2(\varepsilon_r - \frac{j\sigma}{\omega\varepsilon_0})\mathbf{E} = 0$$

The computational model consists of a gold nanosphere centered at the origin. There are two layers above the sphere. The immediate layer above the nanosphere (275 nm) consists of the near field zone. The second layer is perfectly matched layer (PML), imposed to reduce the backscatter in the computational domain.

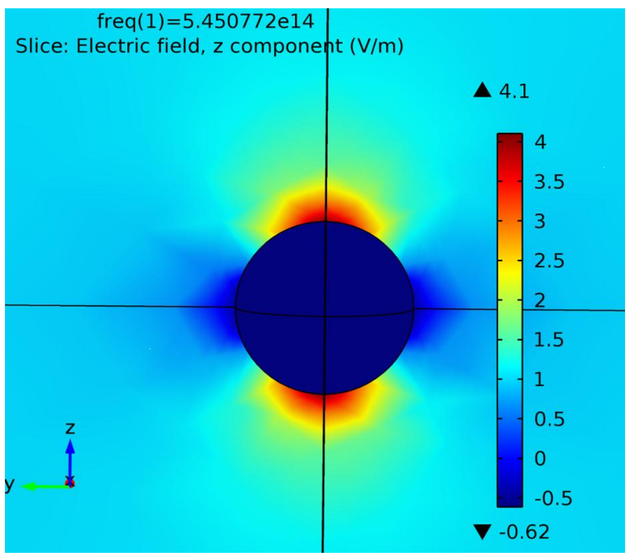


Gold nanosphere with the computational domain

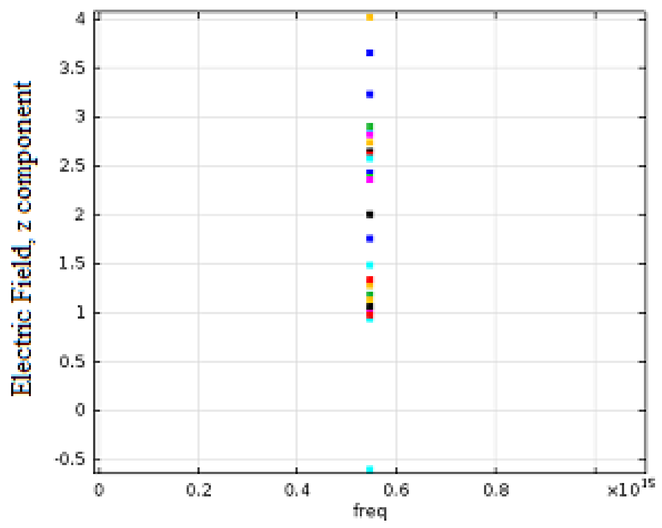
The scatterer is set to be non-magnetic through a separate wave Equation, electric sub-node under the Physics node. The permittivity of the gold nano particle is set through interpolation of the real and imaginary parts of the permittivity provided with the COMSOL software. We illuminate the nanosphere with a plane wave of electric field magnitude of 1.0 V/m, travelling in the *x*-direction and polarized along the *z*-direction.

SIMULATION RESULTS

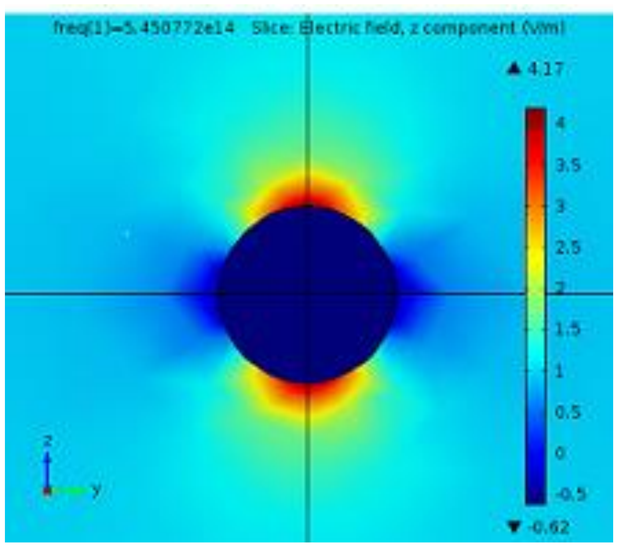
Initially, a plane wave of wavelength 550 nm impinges the nanosphere. The electric field values at 32 spatial points obtained from this simulation is used to make the encryption key. Next, we follow the same procedure with a sphere of radius 12.5 nm. For comparative study, electric field values in this case are evaluated at same points and are used to make decryption keys that would serve to check the robustness of plasmonic encryption keys. The input image used for study is a binary text 'IITP' of size 32 × 32 pixels.



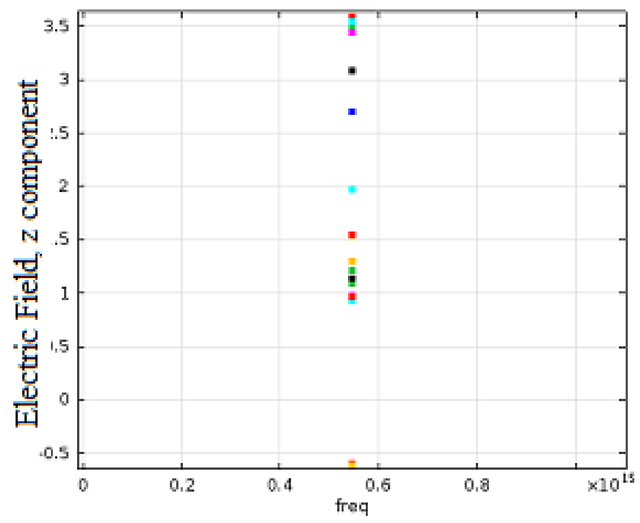
***z* component of the electric field around the nanosphere of radius = 10.0 nm.**



Plot of electric field, *z* component at different spatial points (for radius = 10.0 nm).

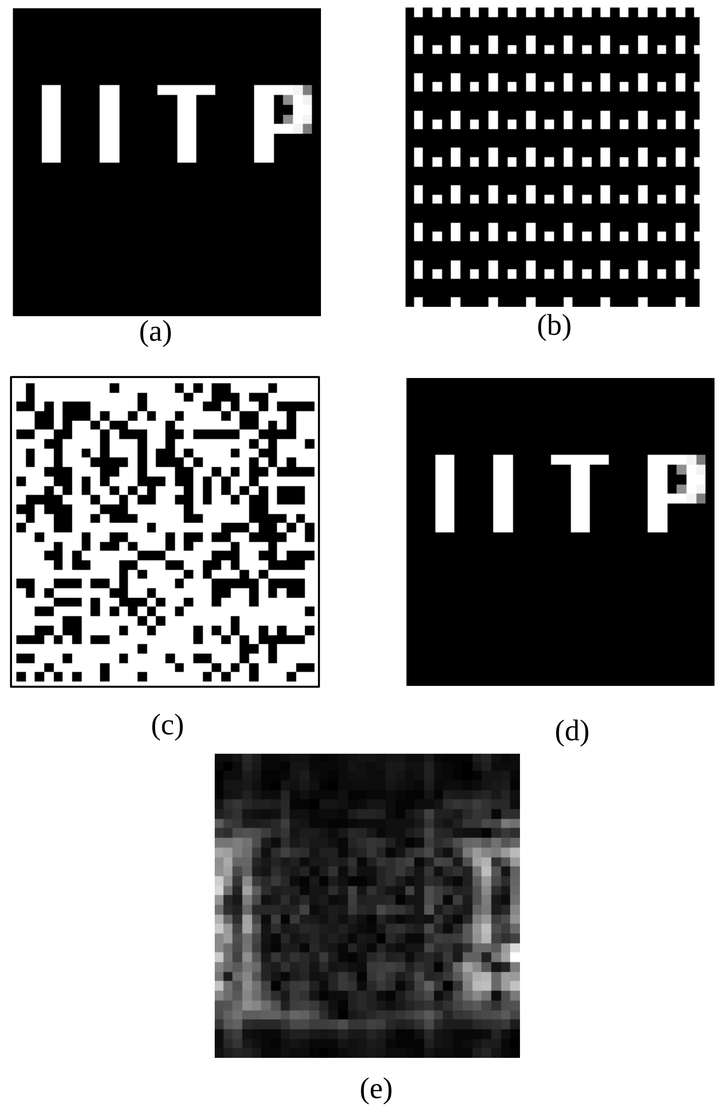


***z* component of the electric field around the nanosphere of radius = 12.5 nm.**



Plot of Electric Field, *z* component at different spatial points (for radius = 12.5 nm).

ENCRYPTION PROCEDURE



Simulation results for image encryption: (a) input image, (b) plasmonic encryption key, (c) encrypted image, (d) decrypted image obtained after using the correct keys, and (e) decrypted image obtained with wrong key.

CONCLUSION

Plasmonic based encryption is in its nascent stage and shows promising growth. Plasmonic keys offer additional degrees of freedom to the encryption keys and thus facilitate robust encryption schemes. COMSOL Wave Optics Module has been used as a platform to optimize the parameters that can be included in the construction of encryption keys.

REFERENCES

[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] M. Gu, X.Li, T. H. Lan, and C. H. Tien, "Plasmonic keys for ultra-secure information encryption", SPIE-Newsroom (2012).

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

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

[6] S. A. Maier, Plasmonics: *Fundamentals and Applications*, 65-73, Springer, New York (2007).