AJP

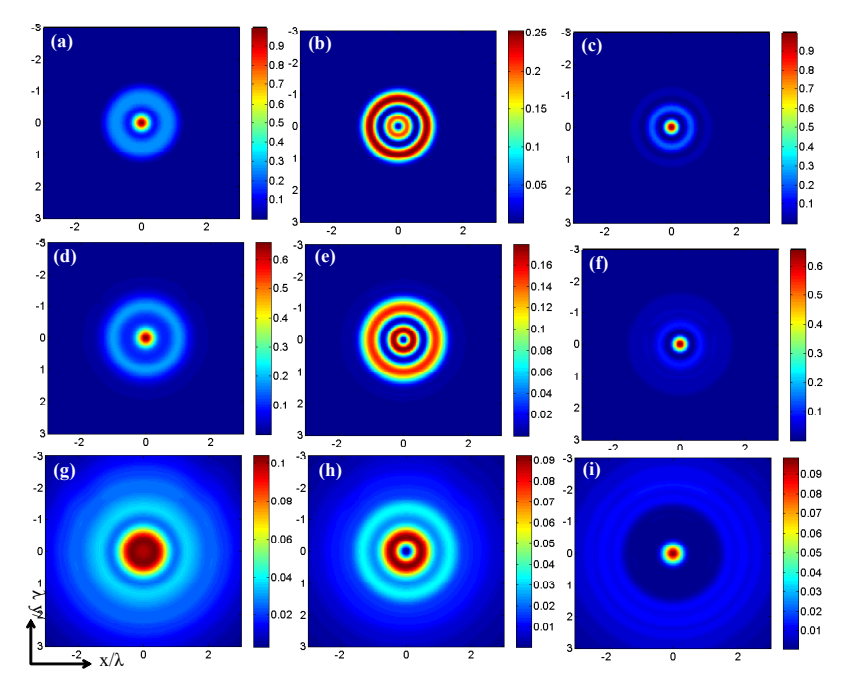
ISSN : 0971 - 3093

Vol 25, No 1, January, 2016

ASIAN JOURNAL OF PHYSICS

25th anniversary year
since 1992

An International Research Journal



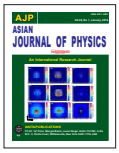
ANITA PUBLICATIONS

FF-43, 1st Floor, Mangal Bazar, Laxmi Nagar, Delhi-110 092, India

B O : 2, Pasha Court, Williamsville, New York-14221-1776, USA

ap

Asian Journal of Physics
Vol. 25, No 1 (2016) 59-64
Available on: www.asianjournalofphysics.in



Plasmonics: A new paradigm for information security

Areeba Fatima and Naveen K Nishchal
Department of Physics
Indian Institute of Technology Patna, Patna-801 118, India

(Celebrating 25th anniversary)

Due to electromagnetic interaction at the metal-dielectric interface, propagating surface waves are formed which are known as surface plasmons. Certain non-propagating excitations too are formed by appropriately illuminated metal nanoparticles which are known as localized surface plasmon resonance. These excitations exhibit special features and have thus, found their use in information security, its authentication and validation. This paper reviews the recent advancements made in the field of information security using plasmonics.

Keywords: Plasmonics; Encryption; Localized surface plasmon resonance; Surface plasmon polaritons.

1 Introduction

With the rapid development of the communication techniques, information security is becoming important day-by-day. Protection of the synthesized data from unauthorized use and counterfeiting has become an important subject for research [1-6]. In the present scenario, there is an increased interest to develop information security techniques based on optical technologies. Refregier and Javidi [2], in their seminal paper, proposed a double random phase encoding (DRPE) scheme that paved the way for other variant methods based on optical information processing techniques. Encryption using optical technology proves to be an efficient procedure because it offers parallel processing of large storage memories at great speed along with large degrees of freedom. However, with several proposed attack mechanisms, there is a continuous urge to develop strategies that should have higher degrees of freedom and robustness [7-10]. In this regard, employing the complexity of physical world to generate encryption keys that fulfill the necessary cryptographic properties has become relevant. Randomness with determinism makes these systems useful for encryption. One such system, which complies with the above mentioned criteria, is the plasmonic system which is discussed in the following sections.

The electromagnetic properties of metal-dielectric interfaces show unique features and have thus attracted the researcher's community to this fascinating area of research. The work of Ritchie [11] generated further interest in the study of these properties, which soon led to the field of plasmonics. Plasmonics is the subfield of modern optics which studies the phenomenon wherein metal-dielectric interfaces are able to sustain coherent electron oscillations known as surface-plasmon polaritons (SPPs) leading to electromagnetic fields confined to the metallic surface [12-13]. This confinement of light in dimensions smaller than the wavelength of photons in free space makes it possible to match different length scales associated with photonics and electronics in a single nano-scale device. Thus, plasmonics is rapidly finding its applications in many fields [12-16].

Corresponding author :
e-mail: nkn@iitp.ac.in (Naveen K Nishchal)

2 Information security using plasmonics

2.1 Localised surface plasmon resonance **(***LSPR***)** *for security applications*

LSPR is non-propagating excitation that arises when the oscillation of conduction electrons of any metal nanoparticle is coupled with the electromagnetic field impinged on it [14,15]. The electromagnetic field causes the polarization of charges in the nanoparticle. The polarization inducing field is an electromagnetic wave, and hence, the direction of the external electric field would change its direction with a frequency equal to that of the wave. This results in oscillating electrons as well as an oscillating dipole which generates enhanced radiation. For the case where diameter of the nanoparticle is much smaller than the wavelength of light in the surrounding medium, the quasi-static approximation can be applied. In such case, the phase of the harmonically oscillating electromagnetic field is approximated to be constant over the volume of the particle. For metal nanospheres, this method approximates the potential outside the metal nanosphere to contain dipole radiation terms [16]. The polarizability associated with the dipole moment generated at the centre of the nanosphere is found to be [14]

$$\alpha = 4\pi a^3 \frac{\varepsilon - \varepsilon_m}{\varepsilon + 2\varepsilon_m} \tag{1}$$

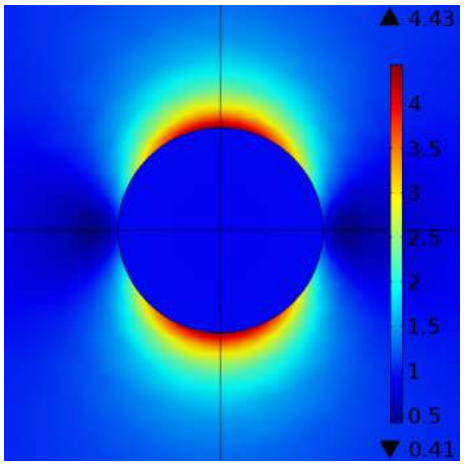
Here, α and a are the polarizability of the metal nanosphere and its radius, respectively. ε and ε_m represent the dielectric constants of the metal and the medium, respectively. The maximum gain for the enhancement of the electric field is achieved when the denominator of Eq (1) is minimum. This in turn introduces a dependence on the frequency of applied electromagnetic field because the dielectric constant of the metal (ε) is a function of the frequency.

The quantitative analysis of the resonance phenomenon can be done by measuring the absorption or scattering cross-section for electromagnetic waves, which too would be enhanced. The polarization of the impinging beam becomes a crucial factor for LSPR generation where there is anisotropy of the nanoparticle. Apart from this, the radius and the shape of the metal nanoparticle too are important parameters to affect the spectrum as shown in Fig 1.

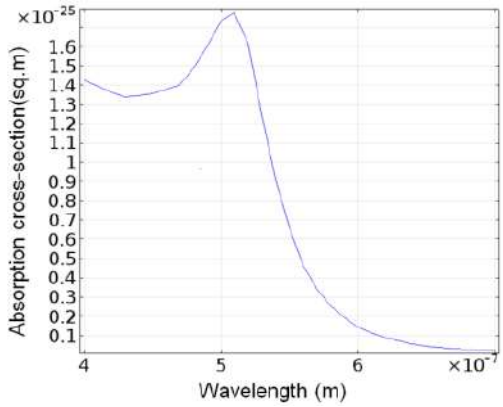
This spectral response of the resonance phenomena and its sensitivity towards different parameters has found its use in various kinds of authentication, validation and other security schemes [17-24]. For robust encryption, a lengthy key (larger key space) with random quality is essential. These features can be accomplished by plasmonic keys [17-18]. The tomography measurements enable the mapping of the intensity of the electric field around a metal nanosphere. This map is the origin of the encryption key and is further numerically processed to increase the entropy [17] making it difficult to intercept it without prior knowledge of the parameters.

In another scheme, surface-enhanced Raman scattering (SERS) has been used to construct anti-counterfeiting labels for authentication [21]. The highly localized light field generated due to the LSPR has been found to increase the power of the scattered beam in the Raman scattering process. The SERS signal depends on the polarization and the wavelength of the electromagnetic wave incident on the plasmonic nanoparticle. Consequently, metal nanorods fabricated on a medium allow for selective read-out of enhanced Raman-signals depending on the polarization of the used electromagnetic wave. Thus, alignment of metal nanowires in the form of alphabet or graphics has been proposed to be used as security labels [21].

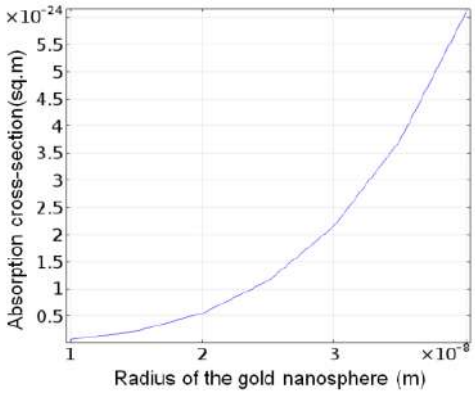
The polarization orientation based ‘key’ technique has been used to store and encrypt larger information content [22-24]. The three-dimensional orientations of the gold nanorods are aligned such that five different patterns are fabricated in single volume. With an electromagnetic beam that can have unlimited three-dimensional polarization orientation, the five patterns can be read out separately through two photon fluorescence (TPF) imaging [24]. The information is read out as noise if the polarization orientation, which serves here as the key, is incorrect.



(a)



(b)



(c)

Fig 1. (a) Dipole radiation due to LSPR in gold nanosphere of radius 10 nm, (b) variation of the absorption cross-section with respect to the wavelength showing resonance above 500 nm, and (c) variation of the absorption cross-section with respect to the radius of the nanosphere

Near-field processes such as LSPR generation are different from the far-field processes, showing hierarchical properties which allow the co-existence of optical features in the propagating-light domain and the sub-wavelength domain [25-27]. Different information content can be retrieved at different scales. Using this fact for security applications, nanometric structural changes (< 100 nm) are applied to the surface of conventional hologram (> 100 nm) so that information corresponding to the nanostructure can be obtained through near field detection while maintaining the far field view of the original hologram [26].

2.2 SPP for security applications

When two materials at an interface have opposite signs of the real part of their dielectric constants (as in metal-dielectric interface), then there exists transverse mode (TM) surface wave solution to the Maxwell's equations. These propagating and dispersive electromagnetic waves are called surface plasmon polaritons (SPP). They arise due to coupling of the impinged electromagnetic field to the oscillations of the conductor's electron plasma [16]. SPPs are marked by energy confinement to nano-scale dimensions which makes them a good prospect for interconnect in photonic circuits. Another remarkable feature of the surface plasmons is their dispersion relation, which is given by

$$k_{sp} = k_0 \sqrt{\frac{\varepsilon_d \varepsilon_m}{\varepsilon_d + \varepsilon_m}} \tag{2}$$

Here, ε_d and ε_m are the permittivity of the dielectric and the metal respectively; k_0 and k_{sp} are the wave vector of the free-space wave and the wave vector of the surface plasmon. It can be easily interpreted from Eq (2) that the wavelength of the generated SPP is larger than that of free-space wave. The unmatched wave vectors make it impossible to generate the SPP by simply illuminating the metal-dielectric interface. One of the methods to bridge this mis-match is through grating coupling [14]. The phase of the plasmon mode and the illuminating beam is matched when the following vector equality holds

$$k_p = k_i + N \times K_g \tag{3}$$

where k_p is the plasmon wave vector, k_i the incident beam wave vector, and K_g the grating vector.

Sauvage-Vincent *et al* [28] used the principle of grating coupling to propose an optical security device. Suppose the grating lies along the *y*-axis, the *z*-axis is perpendicular to the grating in its plane and the incident light makes an angle θ with the out-of-plane *x*-axis, ϕ being the angle of azimuth, then, the vector equality of Eq (1) can be written as [28]

$$k_p = [(k_0 \times n_s \times \sin\theta \cdot \sin\phi)^2 + (k_0 \times n_s \times \sin\theta \cdot \cos\phi) + N \times K_g)^2]^{1/2} \tag{4}$$

Here, n_p and n_s are the effective refractive index of the surface plasmon mode and the index of the dielectric, respectively and k_0 is the free space wave vector of the impinging electromagnetic wave. As the azimuth angle changes, different transmission behavior is observed.

In Ref [28], the transmission for two angles, i.e. $\phi = 0^\circ$ and $\phi = 90^\circ$ has been studied. A letter *D* of the English alphabet has been fabricated using gratings such that the letter and the background have same grating parameters but are perpendicular to each other. This structure shows different transmission effects at various combinations of the angle. This feature can help in authentication and verification of any document.

Besides this, there are many properties of plasmonic systems which have the potential to contribute towards information security. The enhanced transmission through periodic arrays of sub-wavelength holes in metallic films occurs due to the generation of surface plasmons [29]. The spectra can be tuned by changing the shape and size of the aperture and this forms the basis of the anti-counterfeiting scheme as proposed in Ref [30]. An aperture in the form of nano-ellipse shows different enhanced transmission spectra at different

wavelengths and polarization. This sensitivity in the visible range or the near-infra red range can be used to label any high end packaging to counter fake copies.

3 Conclusion

This paper gives a restricted but representative overview of the use of two major excitations in plasmonics, the LSPR and the SPP, in information security. With the advent of technology, there is a constant effort to reduce the size of the optical devices and photonic circuits. Optical near field interactions can be used to achieve this as these interactions lie in nanometer dimensions. With that, the existing security schemes would have to shift their bases to the nanodomain too. This is because the existing optical security schemes work on the principles of optical far fields or propagating light that suffers from diffraction-limit. The field of plasmonics can prove to be helpful in achieving these goals.

References

1. Javidi B, Optical and Digital Techniques for Information Security, (Springer-Verlag, New York), 2005.
2. Refregier P, Javidi B, Optical image encryption based on input plane encoding and Fourier plane random encoding, *Opt Lett*, 20(1995)767-769.
3. Nishchal N K, Naughton T J, Flexible optical encryption with multiple users and multiple security levels, *Opt Commun*, 284(2011)735-739.
4. Rajput S K, Nishchal N K, An optical encryption and authentication scheme using asymmetric keys, *J Opt Soc Am A*, 31(2014)1233-1238.
5. Rajput S K, Nishchal N K, Fresnel domain nonlinear image encryption scheme based on Gerchberg-Saxton phase retrieval algorithm, *Appl Opt*, 53(2014)418-425.
6. Mehra I, Nishchal N K, Wavelet-based image fusion for securing multiple images through asymmetric keys, *Opt Commun*, 335(2015)153-160.
7. Carnicer A, Usategui M M, Arcos S, Juvells I, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys, *Opt Lett*, 30(2005)1644-1646.
8. Gopinathan U, Monaghan D S, Naughton T J, Sheridan J T, A known-plaintext heuristic attack on the Fourier plane encryption algorithm, *Opt Exp*, 14(2006) 3181-3186.
9. Peng X, Zhang P, Wei H, Yu B, Known-plaintext attack on optical encryption based on double random phase keys, *Opt Lett*, 31(2006)1044-1046.
10. Frauel Y, Castro A, Naughton T J, Javidi B, Resistance of the double random phase encryption against various attacks, *Opt Exp*, 15(2007)10253-10264.
11. Ritchie R H, Plasma losses by fast electrons in thin films, *Phys Rev*, 106(1957)874-881.
12. Prasad P N, Nanophotonics, (John Wiley & Sons Inc., Hoboken, NJ, USA), 2004.
13. Gaponenko S V, *Introduction to Nanophotonics*, (Cambridge University Press, USA), 2010.
14. Maier A, *Plasmonics: Fundamentals and Applications*, (Springer, New York), 2007.
15. Atwater H A, The promise of plasmonics, *Scientific American*, 56(2007)38-45.
16. Maier S A, Atwater H A, Plasmonics: Localization and guiding of electromagnetic energy in metal/dielectric structures, *J Appl Phys*, 98(2005)011101-10
17. Grosges T, Barchiesi D, Towards nano world based secure encryption for enduring data storage, *Opt Lett*, 35(2010)2421-2423.
18. Francois M, Grosges T, Barchiesi D, Erra R, Generation of encryption keys from plasmonics, *PIERS*, 7(2011),296-300.
19. Fatima A, Mehra I, Nishchal N K, Plasmonics based keys for optical image encryption, Int'l Conf on Fibre Optics and Photonics (PHOTONICS-2014 Kolkata, India, December 13-14, 2014).
20. Fatima A, Mehra I, Kumar D, Nishchal N K, Plasmonics based keys that uses Exclusive OR logic operation, Comsol Conference Bangalore, (November 13-14, 2014).

21. Cui Y, Hegde R S, Phang Y I, Lee H K, Ling X Y, Encoding molecular information in plasmonic nanostructures for anti-counterfeiting applications, *Nanoscale*, 6(2014)282-288.
22. Zijlstra P, Chon J W M, Gu M, Five-dimensional optical recording mediated by surface plasmons in gold nanorods, Nature, 459(2009)410-413
23. Gu M, Li X, Lan T H, Tien C H, Plasmonics keys for ultra-secure information encryption, SPIE-Newsroom, (19 November 2012) doi:10.1117/2.1201211.004538.
24. Li X, Lan T H, Tien C H, Gu M, Three-dimensional orientation-unlimited polarization encryption by a single optically configured vectorial beam, *Nat Commun*, 3(2012)1-6.
25. Naruse M, Tate N, Ohtsu M, Optical security based on near-field process at the nanoscale, *J Opt*, 14(2012)094002, 1-13.
26. Tate N, Nomura W, Yatsui T, Naruse M, Ohtsu M, Hierarchical hologram based on optical near-and far-field responses, *Opt Exp*, 16(2008)607-12.
27. Tate N, Naruse M, Yatsui T, Kawazoe T, Hoga M, Ohyagi Y, Fukuyama T, Kitamura M, Ohtsu M, Nanophotonic code embedded in embossed hologram for hierarchical information retrieval, *Opt Exp*, 18(2010)7497-7505.
28. Sauvage-Vincent J, Tonchev S, Veillas C, Reynaud S, Jourlin Y, Optical security device for document protection using plasmon resonant transmission through a thin corrugated metallic film embedded in a plastic foil, *J Europ Opt Soc Rap Public*, 8(2013)13015-13021.
29. Ebbesen T W, Lezec H J, Ghaemi H F, Thio T, Wolff P A, Extraordinary optical transmission through sub-wavelength hole arrays, *Nature*, 391(1998)667-669.
30. Lovera P, Jones D, Corbett B, O'Riordon A, Polarization tunable transmission through arrays of elliptical nanopores, *Opt Exp*, 20(2012)25325-25332.

[*Received*: 25.11.2015; *accepted*: 3.12.2015]

Areeba Fatima is currently pursuing Ph D under the supervision of Dr. Naveen K. Nishchal at IIT Patna. She received the degree of Masters in Science from the Patna University in the year 2011. Her research is focused on optical information security systems. She is a student member of OSA - the Optical Society.