Progress In Electromagnetics Research C, Vol. 30, 225–239, 2012

NOVEL DESIGN OF SYMMETRIC PHOTONIC BANDGAP BASED IMAGE ENCRYPTION SYSTEM

N. F. F. Areed and S. S. A. Obayya*

Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Mansoura, Egypt

Abstract—A novel approach for the design of image encryption system based on one stage of 3D photonic bandgap structure is proposed. Using the Finite Integration Time Domain (FITD) method, the performance of the proposed design is optimized through the utilization of the reflection properties from 3D photonic bandgap structure while maintaining constant phase encoding. To demonstrate the robustness of the suggested encryption system, root mean square error is calculated between the original and decrypted images revealing the high accuracy in retrieving the images. In addition, as the proposed system renders itself as easy to fabricate, it has an excellent potential for being very useful in both microwaves and photonics imaging system applications.

1. INTRODUCTION

Encryption is one of the most important and most affordable defenses available to protect our information, and most notably in securing our on-line data transmission from attack. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Due to special characteristics of image data, such as large data volumes, and high redundancy, sometimes image encryption techniques have their own requirements such as compression, format compliance, mean square error tolerance, etc. [1–3].

Traditionally, several methods can be used to encrypt image data streams, some of which can be symmetric in which encryption and decryption keys are the same, or asymmetric in which encryption and decryption keys differ. Symmetric keys, however, usually encrypt more

Received 2 May 2012, Accepted 11 June 2012, Scheduled 22 June 2012

* Corresponding author: Salah S. A. Obayya (sobayya@yahoo.co.uk).

efficiently, so they lend themselves to encrypting large amounts of data and are likely to be even more secure than the asymmetric method [4].

Recently, optical security techniques have witnessed some advances due to characteristics of parallelism and fast processors. Optics provides many degrees of freedom with which the optical beam may be encoded, such as amplitude, phase, wavelength, and polarization. As a result, a number of schemes for optical encryption have been proposed such as amplitude-based encryption and full phase encryption and polarization encoding encryption according to the method of encoding input information [5–8]. Full phase encryption using phase encoded input information is lasting and more secure than amplitude-based encryption due to the presence of additive noise and nonlinear characteristics of phase function. In ideal case the phase information is not invisible and cannot be copied by an intensity detector.

Double random phase encoding (DRPE), proposed by Refregier and Javidi [1], is considered as one of the most widely used optical encryption techniques. Fractional Fourier transform (FRFT) [9] is proposed as a generalization of the conventional plane encodings. Optical Fourier Transform (OFT) plays an important role in optical image processing for encoding systems. In this regard, lenses are used to perform OFT of an object in the DRPE technique. But lenses suffer from aberration which produces errors in the calculated Fourier transform [10, 11].

Currently, there are many available developed approaches for optical encryption systems. In one of them, the concept of modes on DRPE-type encryption systems has been introduced to analyze the encryption system in the context of known attacks [12]. Cryptographic block ciphers partition messages into data blocks before transmission. These blocks are then processed, one at a time. The best way to do this is using the standard modes of operation along with the basic cryptographic algorithm. These modes of operation can be used to pad in a more secure way, control error propagation, and transform a block cipher into an arbitrary length stream cipher. The main contribution of [12] is to present several modes of operation with increased sophistication, that allow the sender some level of defense against the known attacks upon DRPE. Further radically different considerations for optical encryption based on the concepts of computational ghost imaging have been proposed [13]. Ghost imaging is an intriguing optical technique where the imaging information is obtained through photon coincidence detection. The idea is based on sharing a secret key, consisting of a vector of N components between the sender and the recipient, and a spatially coherent monochromatic

laser beam passes through an spatial light modulator, which introduces an arbitrary phase-only mask. The transmitted light is collected by a single-pixel detector. This operation is repeated N times for N different phase profiles, each of them corresponding to one secret key component. The encrypted version of the object image is not a complex-valued matrix but simply an intensity vector, which noticeably reduces the number of transmitted bits. Moreover, a 3D space based approach is used as a new method for optical encryption in various encryption architectures [14]. The fundamental feature of this proposed method is that each pixel of the plaintext is axially translated and considered as one particle in the proposed space-based optical image encryption, and the diffraction of all particles forms an object wave in the phase-shifting digital holography. In [15], one of the latest developments in the encryption technology is introduced which involves a new method using a structured illumination based diffractive imaging with a laterally translated phase grating for optical double-image cryptography. In addition, the integration of the photon-counting imaging technique with optical encryption has been recently proposed to obtain a photon-limited version of the encrypted distribution [16].

In this work, a new idea for data-image encryption and decryption is proposed. This idea relies on the use of 3D Photonic Band-Gap structures (PBG). Photonic band-gap structures are periodic structures that are used to control many features of electromagnetic radiation in certain bands of frequencies. The emerging technology of one-dimensional (1D), two-dimensional (2D) and three-dimensional (3D) PBG structures can be suitably exploited to design and make optical devices such as waveguides, splitters, resonant cavities, filters and so on [17–21]. Our proposed design adopts a carefully tailored PBG block that exhibits high reflectivity and constant phase properties within our frequency range of interest. The design of the proposed 3D PBG encryptor depends actually on studying the relation between the reflection properties and the geometrical parameters of the 1D PBG structure. The use of the 3D PBG enhances the security of the encoding system as replacing the complicated encryption-decryption designs by only one stage of 3D hardware key. Also, wide bandwidth operation facilitates the correct sampling of the signal and signal recovery for intruders challenging. To demonstrate the excellent performance of the proposed symmetric encryption system, mean square error between the decrypted and original image has been calculated. Although used in microwave frequencies, the offered design can be easily extended to optical frequency range via the appropriate scaling of the system dimensions. Due to simple fabrication and yet significantly better performance, the designed PBG

encryption/decryption approach renders itself as a highly competitive approach in comparison to recently existing encryption techniques based on diffraction gratings [22].

3D simulator based on Finite Integration Time Domain (FITD) algorithm was used for simulating the PBG structures. The FIDT is a consistent formulation for the discrete representation of the integral form of Maxwell's equations on spatial grids. First proposed by Weiland [23, 24] in 1977. The Perfect Boundary Approximation (PBA) technique that relies on non-uniform mesh applied in conjunction with FIT maintains all the advantages of the structured Cartesian grids, while allowing the accurate meshing around the curved boundaries: a crucial point for modeling PBG structure [25].

The paper is organized as follows. Following this introduction, some analysis and temporal response of the 1D PBG structure is given in Section 2. In Section 3 the generalized 3D PBG encryption/decryption structure is explained. Section 4 presents the simulation results showing the performance of the proposed structure in encryption and decryption of image, Section 5 briefly presents the main conclusions of our study.

2. DESIGN CONCEPT

First, we consider a six periods of Bragg grating structure made of RT/duroid 6010LM ($\varepsilon_r = 10.8$) excited by an electric mode located at the distance equal to 39 mm from its boundary. According to the simple equation relating the Bragg reflected wavelength, the effective refractive index and the grating period [$\lambda = 2n_{eff}A$] [26], the reflection wavelength range will be around 34 GHz for refractive index 3.286, which is essentially in the same frequency range considered in this paper.

The FITD is used to calculate the transmitted and reflected power spectra of the considered structure with schematic diagram shown in Fig. 1(a). Fig. 1(b) shows the input y-polarized mode which is located at the reference x-y plane (P1). Because of the symmetrical nature of the system, only one-quarter of the computational domain size ($x \times y \times z$) (6 mm $\times$ 6 mm $\times$ 56 mm) structure is analyzed. The time variations of the fields are recorded at the reference ports P1 and P2, respectively. Shown in Fig. 1(c) are the results of variation of S_{11} with different mesh densities, and the results clearly demonstrate the numerical convergence of the adopted FITD. It can be noted from the plot that, to keep reasonable accuracy, this structure has been discretized with the mesh cell size equals $\lambda/30$ or less. On a Personal Computer; (Pantium IV, 3.2 GHz, 2 GB RAM), the whole

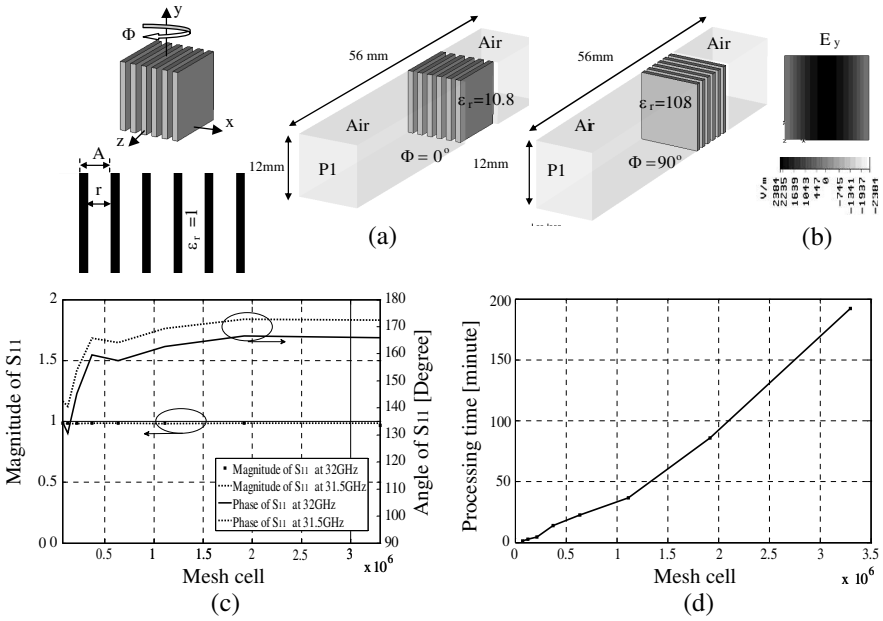

Figure 1. Six period Bragg grating: (a) details of the structure, (b) input TE mode, (c) reflection coefficients vs. the number of mesh cells, (d) computational time vs. the number of mesh cells.

simulation for the prefect meshing period took around 3 hours as shown in Fig. 1(d).

The influence of the r/A ratio of the grating has been investigated considering the geometry with $\Phi = 0°$. Fig. 2 shows the calculated magnitude and phase of the reflection coefficient of the grating with ratio r/A ranges from 0.1 to 0.9 for the frequency range from 30 GHz to 34 GHz. It may be observed from Fig. 2(a) that, the high reflected power and constant S_{11} phase are obtained with the grating characterized by large r/A ratio (0.75 or more), while Fig. 2(b) shows that, variable S_{11} phase is obtained with the grating characterized by small r/A ratios (< 0.7).

The bandwidth of constant S_{11} phase is calculated and plotted versus the r/A ratio in Fig. 3(a). It can be noted from the figure that, the angles of S_{11} at different frequencies tend to be the same at r/A ratio > 0.7. Symmetrical grating configurations at different rotation angle Φ values have been examined. Fig. 3(b) shows, the calculated decibel magnitude and phase curves of the reflection coefficients for $\Phi = 0°$, and $\Phi = 90°$. It can be noted from this figure that, the phase

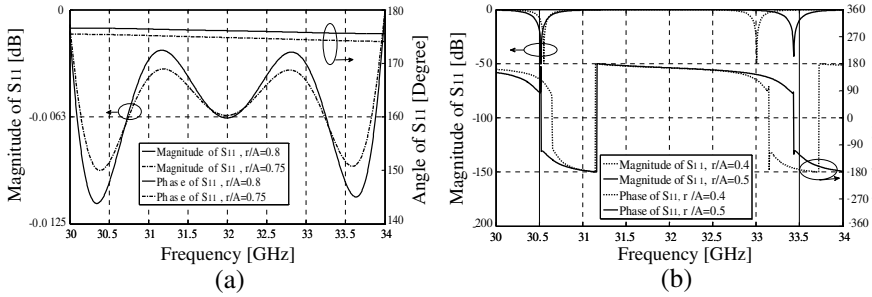

Figure 2. Simulated S_{11}-parameter for different r/A ratios: (a) $[r/A] > 0.7$, (b) $[r/A] \leq 0.5$.

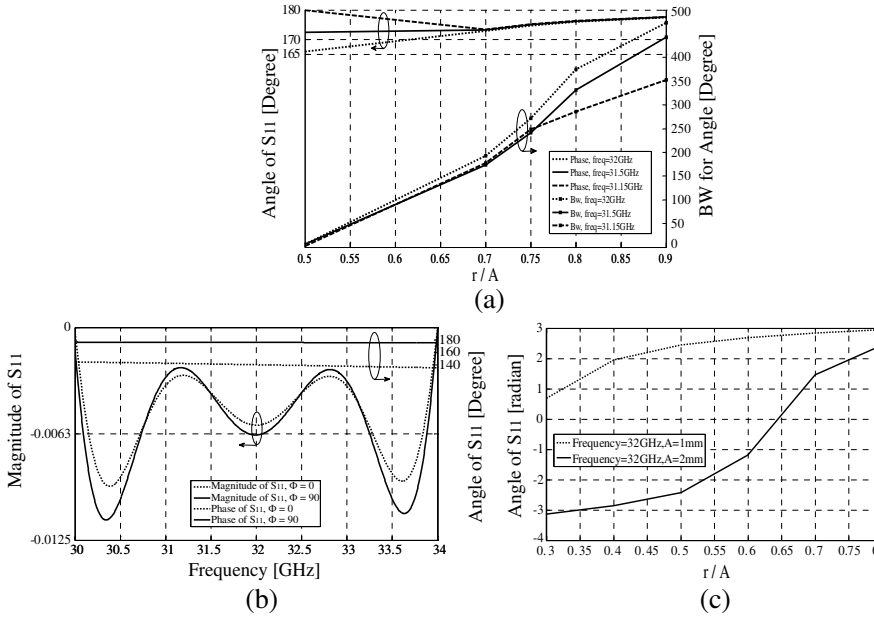

Figure 3. (a) Bandwidth of constant phase, simulated S_{11}-parameter for different values of Φ: (b) rotation angle Φ, (c) lattice constant A.

values of S_{11} increase with increasing the rotation angle Φ. It can be indicated from Fig. 3(c) that, how the phase of S_{11} characteristic of the grating ($\Phi = 90°$) changes as a function of the lattice constant A. It is noticed that, the decrease in the A values causes a significant increase in the S_{11} phase values.

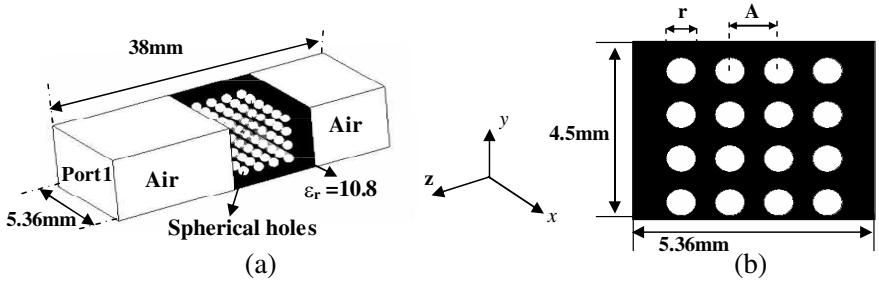

Figure 4. 3D Photonic Bandgap encryptor: (a) details of the 3D structure, (b) transverse 2D plane.

3. ENCRYPTOR/DECRYPTOR DESIGN

The above analyzed 1D PBG is extended to the 3D PBG case in order to perform image encryption scheme. Fig. 4 shows the proposed structure that embodies cubic lattice array of air spherical holes of 1 mm lattice spacing using dielectric substrate (dielectric constant 10.8).

As observed from the analysis of 1D structures, the phase variation is highly sensitive to the orientation of the Bragg-grating plates. However, by employing symmetric 3D PBG structure, the waves impinging on the structure will always face the same scatterers, i.e, the phase relationship will remain unchanged and that is the main advantage of 3D PBG over the 1D component. The photonic band-gap of different configurations with different spherical hole diameters are tested by calculating the reflection coefficient (S_{11}) as shown in Fig. 5. The figure shows that, the hole diameter $r = 0.7$ mm, results in a stop band (S_{11} magnitude near 0 dB and variable S_{11} phase) over 32.532–32.535 GHz, whereas the hole diameter $r = 0.9$ mm, results in a stop band (S_{11} magnitude near 0 dB and constant S_{11} phase 127°) over 32.51–32.55 GHz, respectively. The curves prove that, a large bandwidth of the complete band-gap with constant phase is obtained by large r/A ratio as previously studied.

Next, lattice spacing optimization is applied to increase the S_{11} phase from 127° to 180°. Fig. 6(b) shows the calculated magnitude and the phase of the scattering parameter S_{11} which are nearly 0 dB and 180° over 31.1–31.19 GHz, at lattice spacing $A = 0.8$ mm, and hole diameter $r = 0.72$ mm.

Figure 7 shows the steady state real part of the y-polarized electric field along the propagation direction z at the central frequency 31.095 GHz for the chosen values (0.72 mm, 0.8 mm) for hole diameter

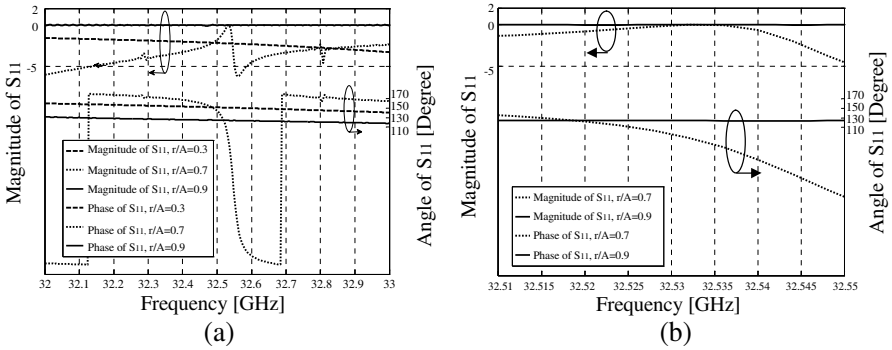

Figure 5. Simulated S_{11}-parameter for different $[r/A]$ ratios, lattice spacing, $A = 1\,\text{mm}$ vs. the frequency bands: (a) 32–33 GHz, (b) 32.51–32.55 GHz.

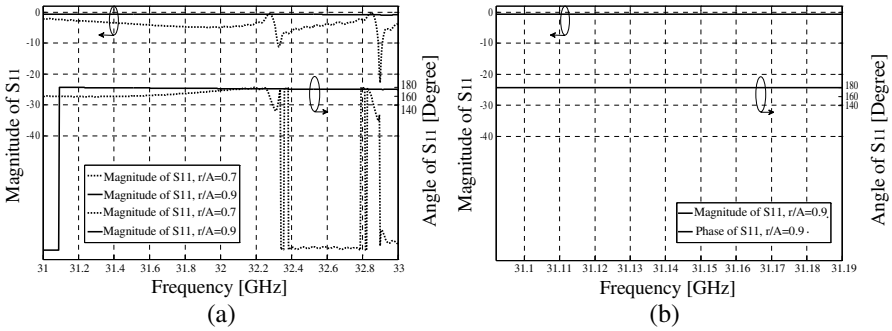

Figure 6. Simulated S_{11}-parameter for different $[r/A]$ ratios, $A = 0.8\,\text{mm}$ vs. the frequency bands: (a) 31–33 GHz, (b) 31.1–31.2 GHz.

and lattice constant, respectively. Computation time for the displayed example is about 2 hours. It is evident from Fig. 7 that, the reflected wave along the structure is highly confined and also reaches the steady state sinusoidal variations at the frequency 31.095 GHz which lies within the operating bandwidth. This reflected wave confinement clearly agrees with the behavior of S_{11} shown earlier in Fig. 6(b).

As discussed, the optimum design of our encryptor is at $A = 0.8\,\text{mm}$ where we obtain phase of 180°. However, in an attempt to work out beyond this value of A, we will lose the wave completely due to the simple fact that it is impossible to catch any reflected waves out of PBG range.

3D PBG technology has become much more mature in the recent years, spanning a number of application areas such as

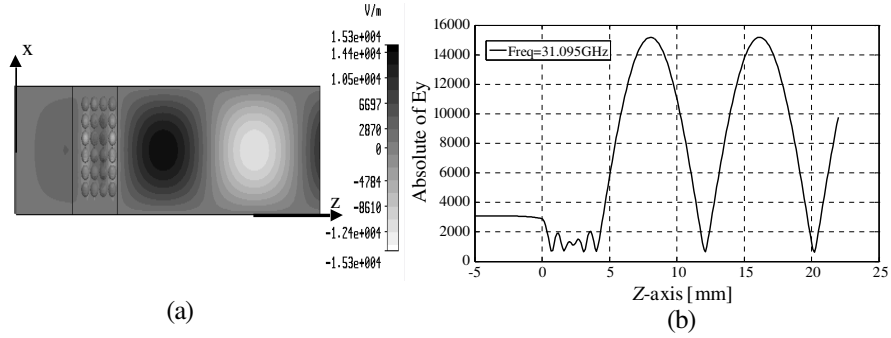

Figure 7. Steady state field profile at $F = 31.095\,\text{GHz}$ versus: (a) xz plane, (b) z-axis.

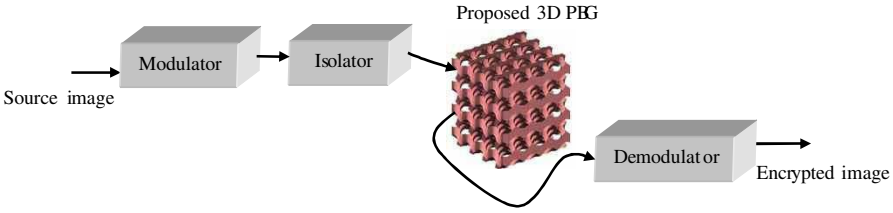

Figure 8. Architecture of symmetric key encryption.

telecommunication, sensing, filtering and now, for the first time to our best knowledge in encryption as suggested in this paper. The authors believe that the fabrication of 3D PBG is not difficult and has been already implemented [27].

4. SIMULATION RESULTS

The main idea behind the proposed method to encrypt digital images is to create an easiest and secure hardware key. This paper proposes a new encryption technique which uses the previously designed 3D PBG section as a band-stop filter (zero transmission) with a constant phase of 180° over the frequency range of the modulated image. The architecture of the proposed symmetric encryption technique is depicted in Fig. 8. The encryption technique is realized using the following steps:

Step1: modulate the source image to a central carrier frequency 31.14 GHz.

Step2: the modulated image will be applied to the designed 3D

PBG block with reflection results given in Fig. 6(b) through an isolator. The isolator device is placed to prevent the reflected wave from a PBG be reapplied to the modulator block. At this point, the signal will be totally reflected with its phase modified by 180° over the image frequency range.

Step3: Apply the reflected signal to the demodulator block to obtain the encrypted image.

It is worth mentioned that the modulator and demodulator blocks are merely simple codes programmed on a computer unit to deal with the digital image.

Reversely, to retrieve the decrypted image, the same block diagram can be used where the encrypted image will be the input to the system. The output of the decryption phase will be the source image with its phase modified by 360° which equal to approximately zero. Thanks to the adopted symmetric encryption approach, the overall encryption/decryption system renders itself as easy to implement.

To evaluate the proposed encryption system, this method is tested on the gray level cameraman image of [256 × 256] pixels as shown in Fig. 9(a). The encryption result is shown in Fig. 9(b). To find the accuracy of the results and the robustness of the encryption, a root mean square (*rms*) of error is calculated. These criteria provide the error between source image and decrypted image. The *rms* value can be described by the following relation [28]:

$$rms = \sqrt{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[g(i,j) - f(i,j)]^2}, \tag{1}$$

where the $g(i, j)$ is the pixel intensity of the original image, $f(i, j)$ is the pixel intensity of the decrypted image. The row and column numbers of these two images are defined by N. Again to determine the quality of the decrypted image, the difference between the original image and the decrypted image is computed. To determine the difference between the original and decrypted images, the *rms* signal-to-noise ratio $(SNR)_{rms}$ is calculated. The $(SNR)_{rms}$ is given by [29]:

$$(SNR)_{rms} = \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} g^2(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}[g(i,j) - f(i,j)]^2}}, \tag{2}$$

where the variable term in the denominator is the noise expressed in terms of the original and the decrypted images. Using the data of

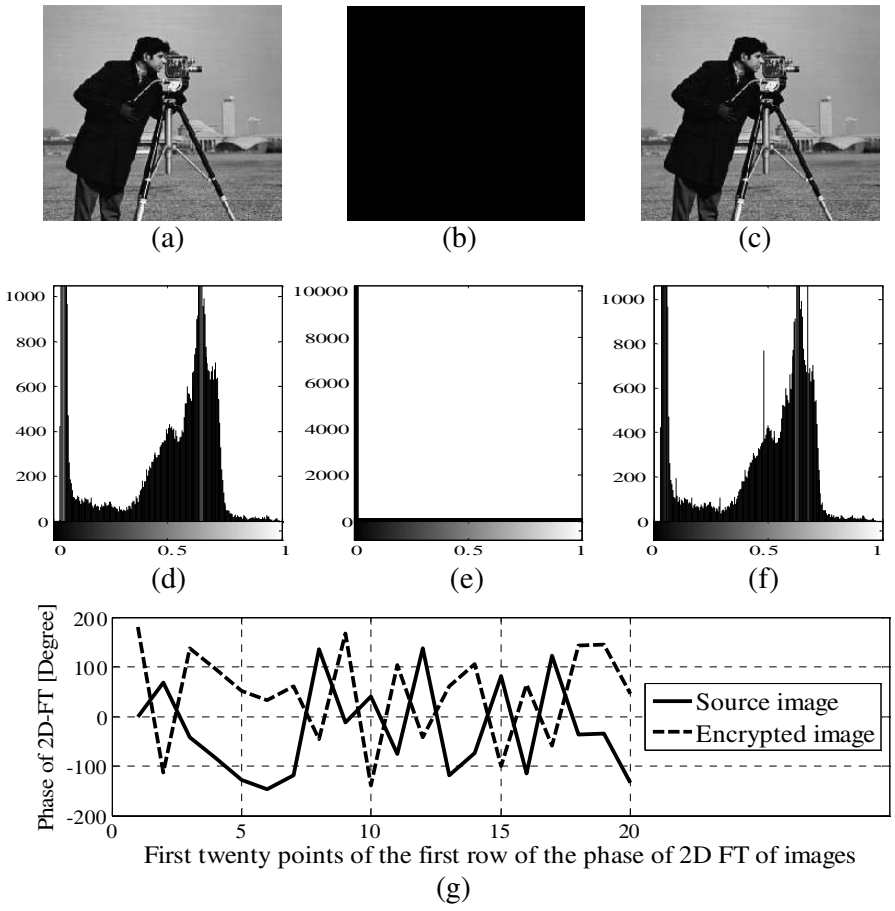

Figure 9. (a) Source of cameraman image, (b) encrypted image, (c) decrypted image, (d) histogram of the source image, (e) histogram of the encrypted image, (f) histogram of the decrypted image, (g) phase samples of the 2D FT of the source and encrypted images.

the original image of Fig. 9(a) and the data of retrieved image shown in Fig. 9(c), the values of the *rms*, and $(SNR)_{rms}$, are 0.0759, 6.426, respectively. Figs. 9(d), 9(e), and 9(f) show the histograms of the source, the encrypted and the decrypted images, respectively. The obtained simulation results of the encryptor design of $(SNR)_{rms}$ and *rms* clearly agree with the plotted histograms of the source and the decrypted images where, the histograms are approximately the same. Moreover, it may be noted from the Figs. 9(d), 9(e) that the histogram

of the encrypted image is completely different from the histogram of the source image. This reflects the efficiency and good quality of our suggested encryption system. It may be observed from these histograms that the most of the encrypted image tends to lie within the black color giving rise to its pixels taking negative values. This negative sign can be explained as it is the added 180° phase shift by the 3D PBG block and this is clearly illustrated from the Fig. 9(g). That figure shows the computed samples of phases of the 2D Fourier Transform [FT] for the source and the encrypted images. It may be noted from the figure that the phase difference between the phase (FT) of the source image and phase (FT) of the encrypted image is approximately 180°. To evaluate the system in the case of attacks, the noise added by encryption to the source image have been quantified as difference between the encrypted image power and the source image power. By normalizing this encryption noise power to the source image power, we have achieved *SNR* as good as −3 dB, therefore, the system is reasonably immune to external attack.

The computational time of the encryption or decryption process has been estimated approximately 86 Ps which is the time taken by the wave to complete one propagation trip (forward and backward) through the PBG block. This extremely low computational time reflects the fact that our encryption model is competitively fast.

5. CONCLUSIONS

In this paper, a novel image encryption scheme has been proposed which utilizes three dimensional photonic bandgap structures. The proposed encryption system has been modeled using the rigorous and accurate FITD method. In the proposed encryption process, reflection with constant phase 180° over the frequency range 31.1–31.2 GHz band is used to encrypt the pixels of the image. The use of the 180° phase has been demonstrated to enhance the security of the encoding system as encryption and decryption keys are kept the same. Also, the demonstrated relatively wide bandwidth operation facilitates the correct sampling of the signal and signal recovery for intruders challenging. To evaluate the reliability of the technique, the root mean square error (*rms*) and the *rms* signal-to-noise ratio $(SNR)_{rms}$ using the data of the source and retrieved images have been calculated. The obtained test results $rms = 0.0759$, $(SNR)_{rms} = 6.426$ reveal the good quality of the image retrieved by the suggested decryptor and proof the good overall performance of our design. Also, We have quantified the noise added by encryption to the image as difference between the encrypted image power and the source image power. By

normalizing this encryption noise power to the source image power, we have achieved *SNR* as good as −3 dB, therefore, the system is reasonably immune to external attack. Finally, we conclude with the remark that with the mature fabrication technology of PBGs, the proposed system is a competitive candidate for useful practical imaging systems covering both microwaves and photonics frequency ranges.

ACKNOWLEDGMENT

The authors would like to acknowledge the Reviewers for the useful suggestions to enhance the technical quality of our work.

REFERENCES

1. Refregier, P. and B. Javidi, "Optical image encryption based on input plane and fourier plane random encoding," *Opt. Lett.*, Vol. 20, 767–769, 1995.
2. Chang, H. K. L. and J. L. Liu, "A linear quad tree compression scheme for image encryption," *Signal Process.*, Vol. 10, No. 4, 279–290, 1997.
3. Holtsnider, B. and B. D. Jaffe, *IT Manager's Handbook: Getting Your New Job Done*, 2nd Edition, 373, Morgan Kaufmann, 2006.
4. Qin, W. and X. Peng, "Asymmetric cryptosystem based on phase-truncated fourier transforms," *Opt. Lett.*, Vol. 35, 118–120, 2010.
5. Monaghan, D. S., U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," *App. Opt.*, Vol. 46, 6641–6647, 2007.
6. Kishk, S. and B. Javidi, "Information hiding technique with double phase encoding," *App. Opt.*, Vol. 41, 5462–5470, 2002.
7. Tao, R., Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional fourier domain," *Opt. Express*, Vol. 15, 16067–16077, 2007.
8. Frauel, Y., A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express*, Vol. 15, 10253, 2007.
9. Joshi, M., C. shakher, and K. Singh, "Color image encryption and decryption for twin images in fractional Fourier domain," *Opt. Commun.*, Vol. 281, 5713–5720, 2008.
10. Castro, J. M., I. B. Djordjevic, and D. F. Geraghty, "Novel super structure bragg gratings for optical encryption," *J. Lightwave Technol.*, Vol. 24, 1875–1885, 2006.

11. Singh, M., A. Kumar, and K. Singh, "Encryption and decryption using a phase mask set consisting of a random phase mask and sinusoidal phase grating in the fourier plane," *ICOP 2009 — International Conference on Optics and Photonics*, CSIO, Chandigarh, India, Oct. 30–Nov. 1, 2009.
12. Naughton, T. J., B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," *J. Opt. Soc. Am. A*, 25, 2608–2617, 2008.
13. Clemente, P., V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," *Opt. Lett.*, Vol. 35, 2391–2393, 2010.
14. Chen, W. and X. Chen, "Space-based optical image encryption," *Opt. Express*, Vol. 18, 27095–27104, 2010.
15. Chen, W., X. Chen, and C. J. R. Sheppard, "Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating," *Appl. Opt.*, Vol. 50, 5750–5757, 2011.
16. Pérez-Cabré, E., M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.*, Vol. 36, 22–24, 2011.
17. Joannopoulos, J. D., R. D. Meade, and J. N. Winn, *Photonic Crystals: Molding the Flow of Light*, Princeton University Press, Princeton, NJ, USA, 1995.
18. D'Orazio, A., M. De Sario, V. Petruzzelli, and F. Prudenzano, "Numerical modeling of photonic band gap waveguiding structures," *Recent Research Developments in Optics*, S. G. Pandalai Editor, 2002.
19. Koshiba, M., "Wavelength division multiplexing and demultiplexing with photonic crystal waveguide couplers," *J. Lightw. Technol.*, Vol. 19, No. 12, 1970–1975, 2001.
20. Sharkawy, A., S. Shi, and D. W. Prather, "Multichannel wavelength division multiplexing with photonic crystals," *Appl. Opt.*, Vol. 40, 2247–2252, 2001.
21. Ozbay, E., M. Bayindir, I. Bulu, and E. Cubukcu, "Investigation of localized coupled-cavity modes in twodimensional photonic band gap structures," *IEEE J. Quantum Electron.*, Vol. 38, 837–843, 2002.
22. Samra, A. S., S. S. Kishk, and S. S. Elnaggar, "A compact lens-less optical image encoding system using diffraction grating," *IJCSNS International Journal of Computer Science and Network Security*, Vol. 10, No. 6, Jun. 2010.
23. Weiland, T., et al., "Verfahren und anwendungen der feldsimula-

tion," Darmstadt, 2002.

24. Krietenstein, B., R. Schuhmann, P. Thoma, and T. Weiland, "The perfect boundary approximation technique facing the challenge of high precision field computation," *Proceedings of the XIX International Linear Accelerator Conference (LINAC'98)*, 860–862, Chicago, USA, 1998.
25. Weiland, T., "Time domain electromagnetic field computation with finite difference methods," *International Journal of Numerical Modelling*, Vol. 9, 295–319, 1996.
26. Canning, J., "Fiber gratings and devices for sensors and lasers," *Lasers Photonics Rev.*, Vol. 2, No. 4, 275–289, Wiley, USA, 2008.
27. Prather, D. W., A. Sharkawy, S. Shi, J. Murakowski, and G. Schneider, *Photonic Crystals, Theory, Applications and Fabrication*, Wiley, Jun. 2009.
28. Servin, M., D. Malacara, and R. Rodriguez-Vera, *Appl. Opt.*, Vol. 33, 2589–2595, 1994.
29. Gonzalez, R. C. and P. Wints, *Digital Image Processing*, 2nd Edition, Addison Wesley Publishing Company, USA, 1987.