Real Time Medical Image Encryption Based on Digital Hologram in Various Optical Domains

R GIRIJA (girija.srikanth09@gmail.com)
Vellore Institute of Technology: VIT University  https://orcid.org/0000-0001-6635-7975

Hukum Singh
The NorthCap University

G ABIRAMI
SRMIST: SRM Institute of Science and Technology

Research Article

Keywords: Digital Hologram, DRPE, Medical images, PSNR, MSE

DOI: https://doi.org/10.21203/rs.3.rs-684879/v1

License: ☒ ☑ This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License
REAL TIME MEDICAL IMAGE ENCRYPTION BASED ON DIGITAL HOLOGRAM IN VARIOUS OPTICAL DOMAINS

R. Girija*, H. Singh2, G. Abirami3,
1SCOPE, VIT University, Chennai Campus, India,
*Girija.srikanth09@gmail.com
2Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurugram, India
hukumsingh@ncuinida.edu,
3Department of CSE, SRMIST, Kattankulathur, India.
abiramig@srmist.edu.in

Abstract –

The use of digital hologram (DH) in optical medical images is analyzed in this paper. These analyses are done in various domains of double random phase encoding and it has been proposed. The domains are fractional Fourier, Gyrator, Fractional Hartley and Fresnel. In order to use in real time scheming, this proposal are used many medical images such as MRI Scan, X-ray and mammograms. These medical images are optically explored with the various domains of double random phase encoding. At that time, various encryption areas in double random phase encoding (DRPE) are considered with boosted confidence of security. The encryption and decryption process in various domains makes the complete chart analysis for all kind of medical images which can be used for real time processing. Simulation analysis and results shows the legitimacy and efficiency of proposed scheme.

Keywords: Digital Hologram, DRPE, Medical images, PSNR, MSE

I. Introduction

The fast and quick propagation of optical medical image handling schemes delivers numerous gradations of self-determination for safeguarding records, data, or imageries. These can be done for two dimensional (2D) imaging aptitudes, in elevation rapidity, and the parallelisms [1][2]. Researchers deeply analyzed about double random phase encoding. Javidi [3] initiated this system using Fourier transforms. Many of the researchers started to perform in various transforms such as Fresnel[5-8], gyrator transforms[9-11], fractional Fourier transform [12-15]. But all these transforms renovates input information into dissimilar mixed space-frequency domains. But most of the designed cryptosystems are symmetric and they are vulnerable to chosen plaintext attacks, chosen cipher text attacks and known plaintext attacks. In order to overcome these attacks, asymmetric cryptosystem [16-22] has been designed. Moreover digital holographic [23-24] methods uses a charge coupled device (CCD) camera for straight footage of a hologram must develop obtainable due to the growth of the imaging machinery. Popular the residence of old-fashioned random phase masks, many researchers developed different masks such as SPM( structured phase masks)[25-27] and it delivers additional benefit of consuming extra encryption secrets for enlarged confidence. It is usually whole after a Fresnel zone plate (FZP) and a spiral phase plate (SPP). Barrera et al. [27, 28] presented a structure phase masks named Toroidal zone plate (TZP). Some other phase masks are Deterministic phase masks [28-30]. One another masks is also generated which is called as chaotic structured phase masks can be used in double random phase encoding. Many simulations are performed with respect to real time medical images. All these analysis
are based upon digital hologram and it is done in numerous domains which is categorized as Fresnel, fractional Fourier and gyrator transforms.

II. PROPOSED MODULE

a. Mathematical Principle

Figure 1. Schematic Optical experiment set up and Figure 2 discusses about the optical experiment set up in Fourier transform domains. $d_1$ and $d_2$ are distances.

![Optical set up](image)

Interference outlines among an objective wave and position wave as holograms can stand verified as follows:

$$ h(x, y) = |B(x, y)|^2 + |E(x, y)|^2 + B^*(x, y)E(x, y) + B(x, y)E^*(x, y) $$

(1)

Where $B$ and $E$ is the object wave field and reference field respectively. Complex conjugate is denoted by *. The holograms remain essentially a two dimensional intensity distribution. Supplementary, it is also called as two dimensional or three dimensional distributions can be scrambled by means of visual systems such as double random phase encryption and other direct and indirect optical encrypting procedures. Equation 1 completely denotes the interference patterns at the hologram plane. Now, this can be promoted and administered in numerous Optical transforms (OPT). Some of the OPTs are Fractional Fourier Transforms (FrFT), Fresnel Transforms (FrT) and Gyrator Transforms (GT) to encrypt holograms. The encryption of all hologram created on double random phase encoding will be applied by double consecutive OPTs [4,12,13–18]. Process of doing encryption is given in below equation.

$$ E(\xi, \eta) = OPT2\{OPT1[h(x, y) \times RPM1(x, y)] \times RPM2(u, v)\} $$

(2)

Where $RPM1$ and $RPM2$ are the statistically independent two random phase masks. $(\xi, \eta)$ and $(u, v)$ are the coordinates. Many domains such as FrFT, FrT and GT are implemented in equation 2.
The first Optical transform domain is fractional Fourier transform (FrFT). FrFT is the sweeping statement of Fourier transform. Solicitations of FrFT are in numerous grounds are such as image and signal dealing out techniques, watermarking, visual gesture dispensation, period filtering and multiplexing. Opto-electronic setup of DRPE in FrFT domain is represented in Figure 2. The FrFT of order $\alpha$ of an input function $f(x)$ can be indicated as \[ F^{-\alpha} \{ f(x) \} (u) = \int_{-\infty}^{\infty} K_\alpha(x, u) f(x) dx \] (3)

Where $K_\alpha(x, u)$ is expressed as,

\[
K_\alpha(x, u) = \begin{cases} 
A \exp \left[ i \pi \frac{x^2 \cot \varphi - 2xu \csc \varphi + u^2 \cot \varphi}{4} \right], & \alpha \neq n\pi; \\
\delta(x - u), & \alpha = 2n\pi; \\
\delta(x + u), & \alpha = (2n + 1)\pi;
\end{cases}
\] (4)

\[ A = \frac{\exp \left[ -i \frac{\pi \text{sgn}(\varphi) \varphi}{4} \right]}{\sqrt{|\sin \varphi|}} \] (5)

Where $\varphi = \frac{\alpha \pi}{2}$ is the angle analogous to the transform order $\alpha$ along the x-axis.

The second Optical transform domain is Fresnel transform (FrT). Opto electronic set up is represented in Figure 3. There are two planes called as Input plane and Output plane. $d$ is represented as free space propagation distance.

Mathematically, Fresnel transform is represented in equations given below,

\[ F_z(u, v) = FrT_{\lambda z} \{ f(x, y) \} = \int_{-\infty}^{\infty} f(x, y) h_{\lambda z}(u, v, x, y) \cdot dx \cdot dy \] (6)
FrT_{\lambda, z} denotes the Fresnel domain and ($\lambda, z$) are considered as parameters. \( h_{\lambda, z}(u, v, x, y) \) is given in equation 7,
\[
h_{\lambda, z}(u, v, x, y) = \frac{1}{\sqrt{\lambda z}} \exp\left( \frac{2\pi z}{\lambda} \right) \exp\left( \frac{i\pi}{\lambda z} (u - x)^2 + (v - y)^2 \right).
\] (7)

The third optical transform domain is gyrator transform. The complete representation of optical set up of gyrator transform is shown in Figure. 4. GT is called as gyrator transform and L1 is the combination of cylindrical lens.

![Gyrator Transform Diagram](image)

**Fig.4.** Optical set up in Gyrator domain.

The gyrator transform is analogous to the fractional Fourier transform (FrFT). It comes under the group of LCT (Linear canonical transform) which harvests the revolution in the depraved position-spatial occurrence planes. There are many similarities between FrFT and GT. Fractional Fourier transform practices a kernel which is the multiplication result of spherical and plane waves while Gyrator transform routines kernel which is the multiplication result of hyperbolic and smooth waves. The two dimensional function of gyrator transform can be represented as,
\[
G(u, v) = G^\alpha \{f(x, y)\}(u, v) = \iint f(x, y) K_\alpha(x, y; u, v) \, dx \, dy
\] (8)

The kernel of the GT is defined as,
\[
K_\alpha(x, y; u, v) = \frac{1}{|\sin \alpha|} \exp\left[ \frac{2\pi i}{\sin \alpha} \left( xy + uv \cos \alpha - xv - yu \right) \right]
\] (9)

where \( \alpha \) and \( G(u, v) \) are transform angle and output of gyrator transform respectively. In case, if \( \alpha = 0 \), it says about the identity transform. In case, if \( \alpha = \pm \frac{\pi}{2} \), then the GT is called as Fourier transform or inverse Fourier transform with the \((u, v)\).

**b. Encryption and Decryption**

Encryption and decryption of our proposed system is given below. Before starting the encryption and decryption, this proposed system considered medical images such as MRI Scan, lung cancer, retina, skin cancer and breast cancer. As a sample, original spectrum, high pass spectrum and high pass image for MRI scan is shown in figure 5.
In order to generate the Gaussian beam, initialize the basenum as 1 (any number other than 0), consider $x$ and $y$ each with 10000 points between -2 to 2, with the help of following equation,

$$x = \text{linspace}(-2 \times \text{basenum}, 2 \times \text{basenum}, 5000)$$

(10)

Similarly, perform for variable $y$. After generating $x$ and $y$, produce the 2D array for plot using meshgrid by the following equation,

$$[X \ Y] = \text{meshgrid}(x,y)$$

(11)

The given formula is used to generate the pattern for Gaussian beam,

$$\text{intensity} = \exp(-2 \times \frac{x^2+y^2}{\text{basenum}^2})$$

(12)

From the intensity pattern, display only the central portion, which is called as Gaussian beam.
After generating the gaussian beam, our encryption process starts:
Read any medical image using imread() function and resize the image according to the size of Gaussian beam.

\[ e = f(x_1, y_1) \cdot \exp(i \cdot gb); \]  

(13)

Where \( f(x_1, y_1) \) is the input image and \( gb \) is the Gaussian beam.

![Image](image1.png)

Figure. 7. Proposed model: (a) Original MRI image, (b) After adding gaussian spectrum (c) Encrypted image (d) Decrypted image (f) Stem plot

\[ f_k = \text{fft2(fftshift(e))}; \]

\[ f_{k1} = \text{fft2(fftshift(f_k))}; \]  

(14)

Perform the transformation as per the equation. 14. Consider two random phase masks R1 and R2. Both are statistically independent of each other. R1 and R2 creation is given in equation 15.

\[ R1 = \exp(i \cdot 2.\pi \cdot \text{rand}(256, 256)) \]

\[ R2 = \exp(i \cdot 2.\pi \cdot \text{rand}(256, 256)) \]  

(15)
\[ e_1 = f_{k_1} \ast R_1 \]  
Multiplying the image which has been created from equation 14 into the first random phase mask. Then apply any optical transform OPT such as fractional Fourier, gyrator and Fresnel transform.

\[ e_2 = OPT(e_1); \]  
From equation 17, it has been divided into two portions; absolute and angular portions. Absolute portion and angular portion from equation 17 is denoted as PT and PR respectively.

\[ PT = \text{abs}(e_2); \] 
\[ PR = \text{angle}(e_2); \]  
Where PT and PR represents the Phase truncation and Phase reservation respectively.

\[ e_3 = PT \ast R_2; \] 
\[ e_4 = IOPT(e_3); \]  
Where IOPT represents the inverse optical transforms. The phase truncation quota is receiving reproduced with one more random phase mask. The creation is transformed with inverse of the optical transform such as Fresnel, fractional Fourier and gyrator transforms which is mentioned in equation 19.

The absolute portion of \( e_4 \) is termed as scrambled image \( E(x, y) \) which is mentioned in the below equation.

\[ E(x, y) = \text{abs}(e_4); \]  
Two private keys \( R_3 \) and \( R_4 \) are calculated from 18 and 19.

\[ R_3 = \text{angle}(e_2); \] 
\[ R_4 = \text{angle}(e_4); \]
The decryption procedure is follows.

\[ d_1 = E(x, y) \cdot \exp(i \cdot R_4); \quad (22) \]

The above equation undergoes to any optical transformation to form the equation 23.

\[ d_2 = OPT(d_1); \quad (23) \]

After this transformation, the absolute portion from equation 23 is extracted and used in below equation,

\[ d_3 = (abs(d_2) \cdot \exp(i \cdot R_3)); \quad (24) \]

Apply the inverse optical transformation to the above equation,
\[ d4 = IOPT(d3) \]  
(25)

Where IOPT stands for inverse optical transformation such as IFrFT (inverse fractional Fourier transform), IFrT (inverse Fresnel transform) and IGT (inverse gyrator transform). The decrypted image is obtained by extracting the absolute portion from the equation 25.

Figure. 9. Proposed model: (a) Original breast cancer image, (b) After adding gaussian spectrum (c) Encrypted image (d) Decrypted image (f) Stem plot

Figure 7, 8 and 9 represents the proposed model for all the medical images such as MRI scan, skin cancer and breast cancer. (a) Denotes the original medical image, (b) represents the image original image added with Gaussian beam, (c) and (d) denotes the encrypted and decrypted images respectively.

c. Performance Analysis
The performance analysis has been performed such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Relative Error (RE).

1. Mean Square Error (MSE) [29-31]:

   \[ MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{(|P(x,y)| - |P'(x,y)|)^2}{MN} \]  
   \hspace{1cm} (26)

   Where \( P(x,y) \) and \( P'(x,y) \) denotes the plain image and decrypted image respectively. \( MN \) shows the size of the image.

2. Peak Signal To Noise Ratio (PSNR)

   \[ PSNR = 10 \log \left( \frac{255^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{(|P(x,y)| - |P'(x,y)|)^2}{MN}} \right) \]  
   \hspace{1cm} (27)

   Where \( P(x,y) \) and \( P'(x,y) \) denotes the plain image and decrypted image respectively. \( MN \) shows the size of the image.

3. Relative Error (RE):

   \[ RE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (|P(x,y)| - |P'(x,y)|)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} (P(x,y))^2} \]  
   \hspace{1cm} (28)

   Where \( P(x,y) \) and \( P'(x,y) \) denotes the plain image and decrypted image respectively. \( MN \) shows the size of the image [29-31]. Table 1. Represents the values for the proposed model.

| Algorithm | Input Image    | MSE     | PSNR    | RE           |
|-----------|----------------|---------|---------|--------------|
| Proposed Model | MRI scan      | 9.515 x10^{-26} | 333.29  | 2.807x10^{-26} |
|            | Skin cancer    | 8.045 x10^{-27} | 301.265 | 4.804x10^{-27} |
|            | Breast Cancer  | 9.400 x10^{-26} | 338.35  | 3.753x10^{-26} |

**d. Noise Analysis**
The noise analysis has been made for the proposed model [29-31]. The plot is made between MSE and the noise factor. If the noises are increases in the system, of course the MSE value also gets increased. For all the three medical images, plot has been drawn. For all the three medical images, noise plot has been made MSE Vs. Noise factor and it is shown in Figure. 10.

### e. Sensitivity Analysis
The sensitivity analysis has been carried out for out proposed model. It has been done for all the OPT’s such as fractional Fourier, Fresnel and gyrator transforms.

**Fractional Fourier transforms:**
As discussed in the mathematical background, it needs two security parameters \((\alpha, \beta)\). In the proposed model, these two values are fixed with \(\alpha = \beta = 0.5\).

**Gyrator transforms:**
As discussed in the mathematical background, rotation angle plays as a security parameter.
Conclusion:

When Digital hologram is combined with double random phase encoding and it had been proposed for medical images. All the analysis had been performed with various transforms such as fractional Fourier, gyrator and Fresnel. In instruction to use in real time devious, this suggestion are used for many medical images such as MRI Scan, X-ray, skin cancer and mammograms. These medical images are optically discovered with the various domains of double random phase encoding. At that time, various encryption areas in double random phase encoding (DRPE) are considered with advanced self-confidence of security.

References

[1] Chen, W., Javidi, B., & Chen, X. (2014). Advances in optical security systems. *Advances in Optics and Photonics*, 6(2), 120-155.
[2] S. Liu, C. Guo, and J.T. Sheridan, “A review of optical image encryption techniques,” Opt. Laser. Technol.
[3] Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics letters*, 20(7), 767-769.
[4] Javidi, B. & Nomura, T (2000). Securing information by use of digital holography. *Optics letters*, 25(1), 28-30.
[5] Situ, G., & Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett., 29(14), 1584-1586 (2004).
[6] Rajput, S. K., & Nishchal, N. K.: Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain. Appl. Opt., 52, 4343-4352 (2013).
[7] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K.: Optical image encryption using devil’s vortex toroidal lens in the Fresnel transform domain. Intl. J. of Opt. (2015).
[8] Vilardy, J. M., Millán, M. S., & Pérez-Cabré, E.: Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. Appl. Opt., 53, 1674-1682 (2014).
[9] Rodrigo, J. A., Alieva, T., & Calvo, M. L.: Applications of gyrator transform for image processing. Opt. Commun., 278, 279-284 (2007).
[10] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K.: Fully phase image encryption using double random-structured phase masks in gyrator domain. Appl. Opt., 53, 6472-6481 (2014).
Singh, H., Yadav, A. K., Vashisth, S., & Singh, K.: Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. Opt. and Lasers in Engg., 67, 145-156 (2015).

Unnikrishnan, G., & Singh, K.: Double random fractional Fourier-domain encoding for optical security. Opt. Engg., 39, 2853-2859 (2000).

Unnikrishnan, G., Joseph, J., & Singh, K.: Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. lett., 25, 887-889 (2000).

Garcia, J., Mas, D., & Dorsch, R. G.: Fractional-Fourier-transform calculation through the fast-Fourier-transform algorithm. Applied optics, 35, 7013-7018 (1996).

Hennelly, B. M., & Sheridan, J. T.: Image encryption and the fractional Fourier transform. Optik-Intl. J. for light and Electron opt., 114, 251-265 (2003).

W. Qin X. Peng.: Asymmetric cryptosystem based on phase-truncated Fourier transform, Opt. Lett. 35,118-120 (2010)

W. Qin, X. Peng X. Meng B. Gao.: Universal and special keys based on phase-truncated Fourier transform, Opt. Eng., 50, 080501 (2011)

S. K. Rajput N.K. Nishchal.: Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask, Appl. Opt., 51, 5377-5786 (2012)

S. Vashisth, A.K.Yadav H. Singh K. Singh.: Watermarking in gyrator domain using an asymmetric cryptosystem, Proc. of SPIE , 9654 96542E-1/8 (2015)

Ding, X., Deng, X., Song, K., & Chen, G.: Security improvement for asymmetric cryptosystem based on spherical wave illumination. Appl. Opt., 52, 467-473. (2013)

Deng, X., & Zhao, D. Single-channel color image encryption based on asymmetric cryptosystem. Opt. & Laser Technol., 44, 136-140 (2012).

Mehra, I., Rajput, S. K., & Nishchal, N. K.: Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification. Opt. Engg., 52, 028202-028202 (2013).

Javidi, B., & Nomura, T. (2000). Securing information by use of digital holography. Optics letters, 25(1), 28-30.

Osamu Matoba and Bahram Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," Opt. Lett. 27, 321-323 (2002)

Vashisth, S., Singh, H., Yadav, A. K., & Singh, K.: Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval. Optik-Intl. J. for Light and Electron Opt., 125, 5309-5315 (2014).

Vashisth, S., Singh, H., Yadav, A. K., & Singh, K.: Devil’s vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform. Intl. J. of Opt. (2014)

Barrera, J. F., Henao, R., & Torroba, R.: Optical encryption method using toroidal zone plates. Opt. commn., 248, 35-40 (2005).

Zamrani, W., Ahouzi, E., Lizana, A., Campos, J., & Yzuel, M. J.: Optical image encryption technique based on deterministic phase masks. Optl. Engg., 55, 103108-103108 (2016).

Girija, R., Singh, H. A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition. Opt Quant Electron 50, 210 (2018). https://doi.org/10.1007/s11082-018-1472-6

Girija, R., & Singh, H. (2019). Triple-level cryptosystem using deterministic masks and modified gerchberg-saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition. Optik, 187, 238-257.

Girija, R., & Singh, H. (2018). Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform. 3D Research, 9(3), 1-20.
[32] Girija, R., & Singh, H. (2018). Enhancing security of double random phase encoding based on random S-Box. *3D Research, 9*(2), 1-20.

[33] Girija, R., & Singh, H. (2017, October). A new substitution-permutation network cipher using Walsh Hadamard Transform. In *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)* (pp. 168-172). IEEE.

[34] Khurana, M., & Singh, H. (2018). Asymmetric optical image triple masking encryption based on Gyrator and Fresnel transforms to remove silhouette problem. *3D Research, 9*(3), 1-17.

[35] Yadav, P.L., Singh, H. Security enrichment of optical image cryptosystem based on superposition technique using fractional Hartley and gyrator transform domains deploying equal modulus decomposition. *Opt Quant Electron* **51**, 140 (2019). [https://doi.org/10.1007/s11082-019-1854-4](https://doi.org/10.1007/s11082-019-1854-4)

[36] Maan, P., Singh, H. Non-linear Cryptosystem for Image Encryption Using Radial Hilbert Mask in Fractional Fourier Transform Domain. *3D Res* **9**, 53 (2018). [https://doi.org/10.1007/s13319-018-0205-8](https://doi.org/10.1007/s13319-018-0205-8)