Radon Transforms and Chaotic Mask Based Image Encryption for Information Security

Avinash Kumar Jha, Sajan Ambadiyil and Himanshu Shekhar

Abstract Recent advances in image encryption techniques are capable of protecting the digital images which are being communicated over various transmission media from leakage. Images related to medical or military applications, corporate video conference, etc. need reliable and secure transmission, which can be achieved by encryption. Here we propose an efficient optical image encryption technique using Radon Transforms and Chaotic phase mask.

1 Introduction

Recent advances in image encryption techniques are capable of protecting the digital images which are being communicated over various transmission media from leakage. Images related to medical or military applications, corporate video conference, etc. need reliable and secure transmission, which can be achieved by encryption. With the help of efficient optical encryption and decryption technique, one can fulfill the requirements of security needs of digital images. Multiple image encryption systems based on optical means have been proposed by various research groups' earlier [1–10]. For real time applications, optics and optoelectronics techniques are very useful as these are accurate, fast computing and support parallelism. These methods provide parameter such as wavelength, phase, polarization, etc. which can be used to hide information more securely in various types of images [11]. Li et al. proposed propose a new method for color image encryption by wavelength multiplexing on the basis of two-dimensional (2-D) generalization of fractional Hartley transform [12]. Nishchal et al. proposed and implemented a phase-encrypted memory system they utilized the cascaded extended fractional Fourier transform (FRT) [13]. Madan Singh et al. proposed an encryption method based on double random phase encoding and

A.K. Jha (✉) · H. Shekhar
Hindustan Institute of Technology & Science, Chennai, India
e-mail: ak.vit2006@gmail.com

S. Ambadiyil
Center for Development of Imaging Technology, Trivandrum, India

I. Bhattacharya et al. (eds.), *Advances in Optical Science and Engineering*,
Springer Proceedings in Physics 194, DOI 10.1007/978-981-10-3908-9_40

decoding system for two-dimensional gray scale image [14, 15]. Li et al. proposed a double-image encryption algorithm. This algorithm can encrypt two input images into a single encrypted output image. The method exploits the amplitude of gyrator transform with two different groups of angles to decrypt the images [16, 17]. Narendra Singh and Aloka Sinha proposed a novel method for image encryption, utilizing gyrator transform and chaos theory [18].

Here we propose an efficient optical image encryption Technique Using Radon Transforms and Chaos function. The proposed technique uses Radon Transform and Chaotic Random Phase Mask (CRPM). The technique is highly robust and has great immunity to unauthorized decryption. The original and decrypted image are highly correlated. It is possible to implement this encryption using optical imaging technique which makes it more relevant for radio over fiber communication systems.

1.1 Radon Transform

The radon transform is represented by integral of a function over straight lines. It is utilized predominantly in the field of Medical Imaging, Ground Penetrating Radar (GPR), electron microscopy, hyperbolic partial differential equation etc.

The mathematical model of radon transform in for a two dimensional function can be represented as follows.

Considering f as a mathematical function bound by a large disc in Eucildian plane $\mathbf{R}^2$.

Then it's radon transform can be defined as function $R_{f,}$ which is defined on the space of lines L in $\mathbf{R}^2$ as given in (1).

$$Rf(L) = \int_L f(x)d\sigma(x) \tag{1}$$

the integration is done w.r.t. the arc length measure $d\sigma$ on L. L can be parameterized as follows;

$$L(x(t), y(t)) = (t\sin\alpha, +s\cos\alpha) + (-t\cos\alpha + \sin\alpha)$$

here the distance between L and origin is denoted by s and α signifies the angle it makes with the x axis. Thus (α, s) represents coordinates on the space of all lines in $\mathbf{R}^2$, and in terms of these coordinates Radon transform can be expressed as

$$Rf(\alpha, s) = \int_{-\alpha}^{\alpha} f(x)(t), y(t)dt = \int_{-\infty}^{\infty} f(t(\sin\alpha, -\cos\alpha) + s(\cos\alpha, \sin\alpha))dt \tag{3}$$

1.2 Chaotic Phase Mask

Chaotic functions describe the behavior of certain dynamic systems i.e., systems whose state evolves with time and which may exhibit dynamics that are highly sensitive to initial conditions. Due to this sensitivity, behavior of chaotic systems appears to be random. For certain chaotic systems if the initial conditions are known, their future dynamics can be completely predicted. This is defined as deterministic chaos. In our encryption technique a random phase mask has been generated using logistic map as chaotic map. It is a discrete 1-D function as mentioned in the equation

$$x_{n+1} = rx_n(1 - x_n) \tag{2}$$

here x_n is a positive number between 0 and 1 which represents the population at year *n* and *r* represents the rate of growth i.e.; combined rate of reproduction and starvation in the population.

1.3 Cryptographic Enhancement

For an m × n image two sequence of random number of length m and n corresponding to each row and column of the image are generated. At first each pixel of the image is replaced by the r'th pixel from the right of the original pixel, where r is the random number corresponding to that particular row. Same action is performed with respect to column. During decryption same action is performed in the reverse direction yielding the correct image. The procedure is explained in Fig. 1. The sequence of random number acts as a set of key, and this whole operation adds additional security feature to the encryption.

2 Proposed Technique

The proposed technique utilizes radon transforms and double chaotic random phase mask. Let f(x, y) denotes the original image to be encrypted. The block diagram in Fig. 2a gives an overview of the encryption process.

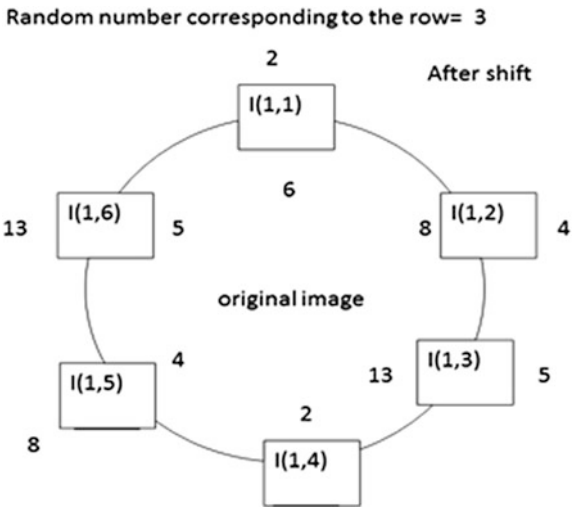

Fig. 1 Cryptographic enhancement

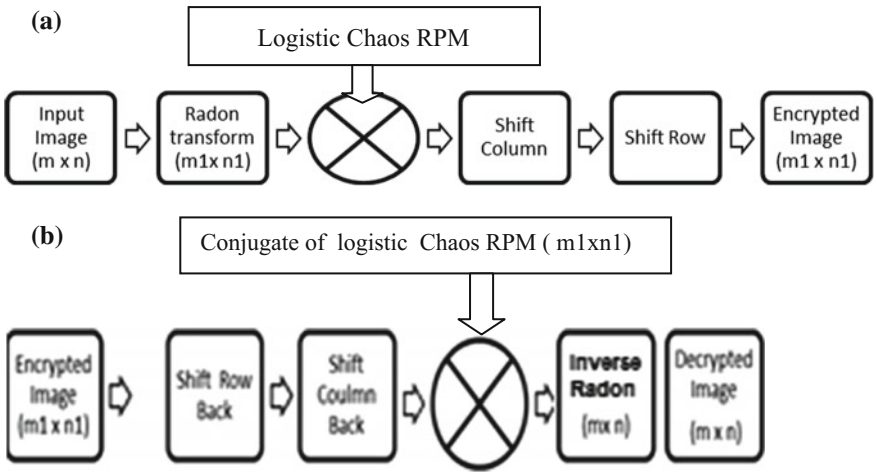

Fig. 2 **a** Block diagram for encryption, **b** block diagram for decryption

2.1 Encryption Process

A gray scaled image of size 256 × 256 is used as input. Radon transform is applied on the input image. The transformation generates an intensity image of different size (367 × 451) with respect to the input image. The number of rows of the

transformed image depends on the number of intensity level present in the image while the number of column depends on the total number of angle for which RT is taken, which acts as a security feature. The transformed image is multiplied with the random phase mask represented by exp(ipiC(x)) here C(x) is the logistic map function. The row column shift operation is performed on this output to generate the encrypted image. The encryption procedure is shown in Fig. 2a.

2.2 Decryption Process

For decryption the pixels are shifted to their original coordinates by applying row column shift operation in the reverse direction, and then this image is multiplied with the conjugate of the random phase mask. Now inverse radon transform applied for the same set angle as of radon transform yields the original input image. Figure 2b illustrates the decryption process.

3 Result and Analysis

The above figure shows the results obtained by the proposed method. To find the robustness of the proposed system MSE error analysis, histogram analysis, correlation of pixel distribution among input, output and un-authenticated decryption image were performed. The original and decrypted image were found to have high correlation coefficient and the method is highly immune to un-authorized decryption.

As shown in Table 1, different value of chaotic mask seed were applied to an image encrypted with the seed value 3.8. It is clearly evident from the graph and table that the MSE value for correct key is negligible. 48.5199, however for wrong

Table 1 MSE w.r.t variation in rate of the logistic function

Rate of logistic map	MSE for lena
3.76	253565.5016
3.78	261938.1427
3.79	262371.1103
3.799	265253.1471
3.7999	264224.9905
3.8	**48.5199**
3.8001	269381.7596
3.801	285538.7191
3.81	276406.204
3.82	355639.5019

key such as 3.7999 the MSE value is extremely high (264224.9905) implying failed decryption as shown in Fig. 3h.

The proposed technique results into a correlation co-efficient of 0.9932 between the input and output and decrypted image (Fig. 4).

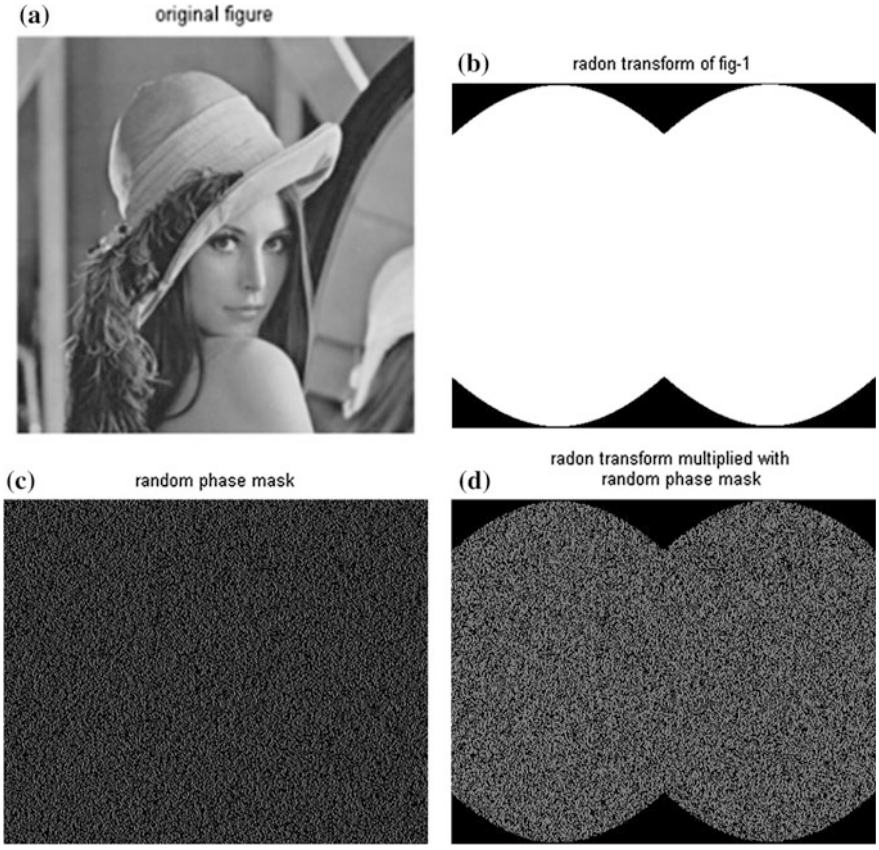

Fig. 3 **a** Input image, **b** radon transform of image, **c** random phase mask, **d** radon transformed image multiplied with phase mask, **e** encrypted image after row column shift, **f** decrypted image with correct procedure, **g** image decrypted without shifting the row-column back, **h** image decrypted with wrong conjugate mask

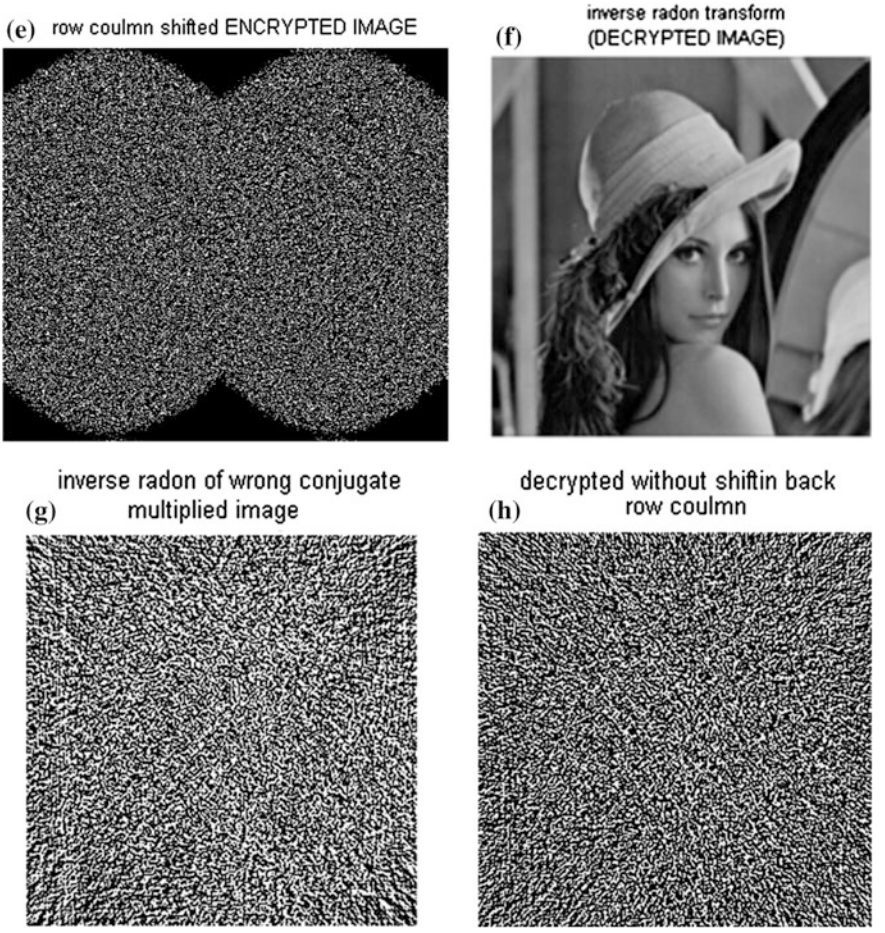

Fig. 3 (continued)

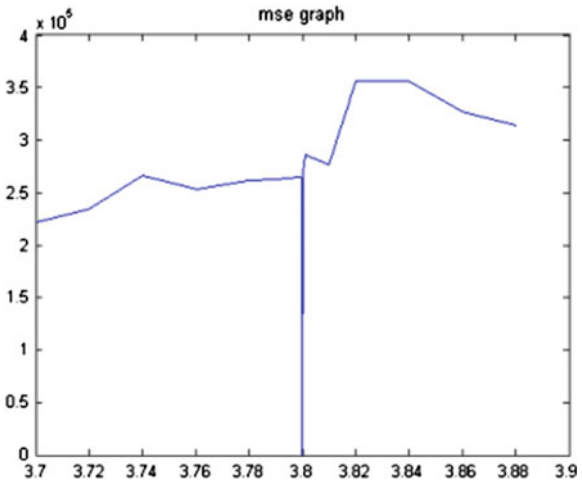

Fig. 4 MSE w.r.t variation in rate of the logistic function

4 Conclusions

A highly efficient image encryption and decryption Technique Using Radon Transforms and Chaos function has been proposed. The technique is highly robust and has great immunity to unauthorized decryption. The original and decrypted image are highly correlated.

References

1. H.K.L. Chang, J.L. Liu, A linear quad tree compression scheme for image encryption, Signal Process. 10 (4) (1997) 279–290.
2. 769 J. Scharinger, Fast encryption of image data using chaotic Kolmogrov flow, J. Electronic Eng 7 (2) (1998) 318–325.
3. N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn. 25 (1992) 567–581.
4. Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (6) (1998) 1259–1284.
5. Refregier, B Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett. 20 (1995) 767.
6. H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.
7. J.C. Yen, J.I. Guo, An efficient hierarchical chaotic image encryption algorithm and its VLSI realization, IEE Proc. Vis. Image Process. 147 (2000) 167–175.
8. J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999, pp. 430–437.
9. C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91. 749–761.
10. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.
11. Nishchal NK, Joseph J, Singh K. Fully phase-encrypted memory using cascaded extended fractional Fourier transform. Opt Lasers Eng 2004;42(2):141–51.
12. X. Li, D. Zhao, Optical color image encryption with re defined fractional Hartley transform, Opt. Int. J. Light Electron. Opt. (2009), doi:10.1016/j.ijleo.2008.10.008.
13. Naveen Kumar Nishchal, Joby Joseph, Kehar Singh, "Fully phase-encrypted memory using cascaded extended fractional Fourier transform", Optics and Lasers in Engineering 42 (2004) 141–151.
14. Madan Singh a, Arvind Kumar b,_, Kehar Singh, "Optical security system using jigsaw transforms of the second random phase mask and the encrypted image in a double random phase encoding system", Optics and Lasers in Engineering 46 (2008) 763–768.
15. M. Singh, et al., Encryption and decryption using a sandwich phase diffuser made by using two speckle patterns and placed in the Fourier plane: Simulation results, Opt. Int. J. Light Electron. Opt. (2008), doi:10.1016/j.ijleo.2008.03.025.
16. Yong-Ying Wang_, Yu-Rong Wang, Yong Wang, Hui-Juan Li, Wen-Jia Sun, "Optical image encryption based on binary Fourier transform computer-generated hologram and pixel scrambling technology", Optics and Lasers in Engineering 45 (2007) 761–765.
17. Huijuan Li, Yurong Wang, "Double-image encryption based on iterative gyrator transform", Optics Communications 281 (2008) 5745–5749.
18. Narendra Singh, Aloka Sinha, "Gyrator transform-based optical image encryption, using chaos", Optics and Lasers in Engineering 47(2009) 539–546.