Optica Applicata, Vol. XLVII, No. 3, 2017
DOI: 10.5277/oa170308

Color image encryption using affine transform in fractional Hartley domain

PHOOL SINGH, A.K. YADAV[1*], KEHAR SINGH[2]

[1]Amity School of Applied Sciences, Amity University Haryana, Gurgaon-122413, India

[2]Department of Applied Sciences, The NorthCap University, Gurgaon-122 017, India

[*]Corresponding author: aky68@yahoo.com

A novel scheme for color image encryption using the fractional Hartley and affine transforms is proposed. An input color image is first decomposed in its RGB (red, green and blue) components. Each component is bonded with a random phase mask and then subjected to a fractional Hartley transform followed by affine transform. Thereafter, a second random phase mask is applied to each component before the final transformation by fractional Hartley transform resulting in a component-wise encrypted image. Finally, all three components are combined to give a single channel encrypted image. The scheme is validated with numerical simulations performed on a color image of size 256 × 256 × 3 pixels using MATLAB 7.14. The use of affine transform along with fractional Hartley transform adds to the security. The scheme is evaluated for its sensitivity to the parameters of the fractional Hartley and affine transforms. On analysing the plots of correlation coefficient and mean-squared-error, the scheme is found to be highly sensitive to the encryption parameters. Also, it is evaluated for its robustness against the usual noise and occlusion attacks. The proposed scheme is secure and robust owing to multiplicity of encryption parameters introduced through the type of transforms used.

Keywords: color image encryption, affine transform, fractional Hartley transform, occlusion and noise attacks.

1. Introduction

Rapid growth in internet connectivity leads to a serious concern about information systems security. With growing threats to information systems, it is absolutely important to consider system-level security to shield information resources against malicious attacks. Mathematical theories of cryptography play a big role in information security. Unauthorized use of sensing and imaging is a serious problem as image information can be invaded during transmission in the communication channels. There are limitations of digital security systems and therefore, it is beneficial to add physical parameters to increase security. With high processing speed, parallelism and high-dimensional

encryption, optical information systems offer the advantage of a large key-space in information security [1–3].

Double-random phase-encoding (DRPE) technique is a well-known approach in optical image encryption in which an input image is encrypted in a 4-*f* optical system [4, 5]. Various canonical transforms used in implementation of DRPE technique were based on Fourier transform, Fresnel transform, Hartley transform and gyrator transform [4–6], among others. With a view to increase encryption parameters for enhanced security, some studies based on the fractionalized version of Fourier transform (FrFT) [7, 8], Mellin transform [9–11], and Hartley transform [12–21] have been reported.

The application of fractional Hartley transform (FrHT) is comparatively less explored in image encryption. DAOMU ZHAO *et al*. [15] pointed out that FrHT does not satisfy the additive property, and therefore, the original image cannot be recovered as a result of decryption. They proposed redefined FrHT which uses FrFT and has a period 2. In addition to FrHT's mathematical definition, they also reported its optical implementation. XINXIN LI and DAOMU ZHAO [16] proposed a method for color image encryption by wavelength multiplexing. VILARDY *et al*. [18] have used the Arnold transform in the fractional Hartley domain for double image encryption. Recently, YE LIU *et al*. [19] have reported an algorithm for single-channel color image encryption based on vector operation and FrHT.

Affine transform (AFT) consists of many operations like translation, scaling, rotation and shearing. It is used for pixel scrambling in image encryption study [22]. In many applications, color information is more relevant such as color of the hair, eyes and face to identify a person. Overall, a higher level of security could be provided by color images as compared to monochromatic images. SHUQUN ZHANG and KARIM [23] were the first to propose an encryption method for a color image by converting it to an indexed image before encoding, and many others [16, 19, 24–26] followed thereafter.

In this study, we have proposed a novel encryption scheme for color image encryption using the fractional Hartley and affine transforms. An input color image is first decomposed in its RGB (red, green and blue) components which are bonded with a random phase mask (RPM) and then subjected to a FrHT followed by AFT. Then, a second RPM is applied to each component before the final transformation by FrHT resulting in a component-wise encrypted image. Finally, the components are combined to give a single channel encrypted image. The process of decryption is just the reverse of encryption.

2. The transform framework

2.1. Fractional Hartley transform

The two dimensional fractional Hartley transform (FrHT) of an input image $f(x, y)$ is defined as [15]

$$H^{p,q}(u,v) = \frac{\sqrt{\left[1 - i\cot(\varphi_1)\right]\left[1 - i\cot(\varphi_2)\right]}}{2\pi}$$

$$\times \exp\left\{i\pi\left[\frac{u^2\cot(\varphi_1)}{\lambda f_{s1}} + \frac{v^2\cot(\varphi_2)}{\lambda f_{s2}}\right]\right\}$$

$$\times \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \exp\left[\frac{i\pi x^2\cot(\varphi_1)}{\lambda f_{s1}} + \frac{i\pi y^2\cot(\varphi_2)}{\lambda f_{s2}}\right]$$

$$\times \left\{\frac{1 - i\exp\left[i(\varphi_1 + \varphi_2)/2\right]}{2}\operatorname{cas}\left[\frac{ux\csc(\varphi_1)}{\lambda f_{s1}} + \frac{vy\csc(\varphi_2)}{\lambda f_{s2}}\right]\right.$$

$$\left. + \frac{1 + i\exp\left[i(\varphi_1 + \varphi_2)/2\right]}{2}\operatorname{cas}\left[-\frac{ux\csc(\varphi_1)}{\lambda f_{s1}} - \frac{vy\csc(\varphi_2)}{\lambda f_{s2}}\right]\right\}$$

$$\times f(x,y)\,\mathrm{d}x\,\mathrm{d}y \tag{1}$$

where p and q are the fractional orders of FrHT, $\varphi_1 = p\pi/2$ and $\varphi_2 = q\pi/2$, λ is the wavelength of the input light, cas = cos + sin, f_{s1} and f_{s2} are the standard focal lengths of lenses in the x and y directions, respectively.

In terms of the FrFT, the 2D FrHT can be deduced as follows [15]:

$$H^{p,q}(u,v) = \frac{1 + \exp\left[i(\varphi_1 + \varphi_2)/2\right]}{2}F^{p,q}(u,v) + \frac{1 - \exp\left[i(\varphi_1 + \varphi_2)/2\right]}{2}F^{p,q}(-u,-v) \tag{2}$$

From the expression on the right hand side of Eq. (2), it can be attempted in the four-channel way of FrFT. Two channels represent $F^{p,q}(u,v)$ and $\exp[i(\varphi_1 + \varphi_2)/2] \times F^{p,q}(u,v)$ expressions, whereas the other two channels represent $F^{p,q}(-u,-v)$ and $\exp[i(\varphi_1 + \varphi_2)/2]F^{p,q}(-u,-v)$. In optical implementation, $F^{p,q}(u,v)$ is well-known, whereas $F^{p,q}(-u,-v)$ is obtained by using a cube corner prism by rotating the field of $F^{p,q}(u,v)$ through 180°.

2.2. Affine transform

The affine transform (AFT) is a scrambling operation, which changes the pixel position of an image randomly. Affine transform of a pixel (x, y) of an image $f(x, y)$ of size $N \times N$ pixels is denoted by (x', y') and mathematically defined as [22]

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \text{AFT}\{(x, y), N\} = \begin{bmatrix} a + cx \\ b + dy \end{bmatrix} (\text{mod}\, N) \tag{3}$$

where "mod" denotes the modulo operation, a and b are two random numbers between 1 to N, and c, d are chosen in such a way that they are relative prime to N. Such a choice of c and d leads AFT to map (x, y) to a unique pixel in transformed coordinates. If c and d are not relative prime to N, then AFT maps different pixels to the same pixel

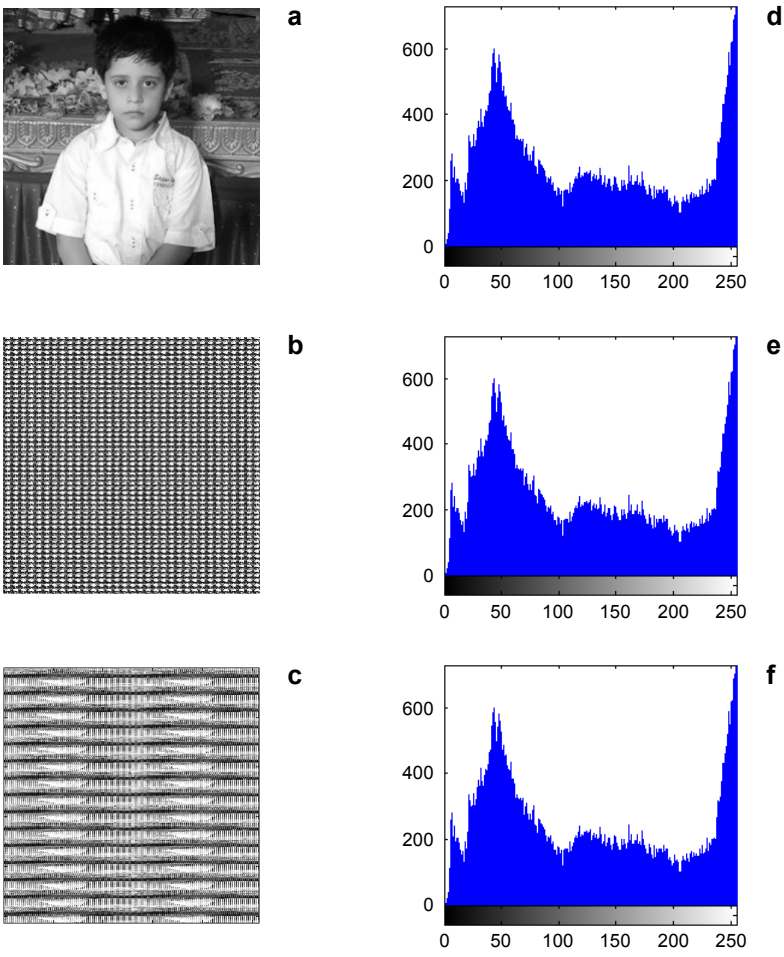

Fig. 1. Affine transform (AFT) of an image of *Boy*. Original image (**a**), AFT with $w = 1$ (**b**), AFT with $w = 20$ (**c**) and respectively histograms of **a**–**c** (**d**–**f**).

in the transformed coordinates [22]. After the AFT, the total energy of the input image remains the same as before. The AFT can be applied iteratively for scrambling operation and the actual number of iterations w can serve as an encryption parameter.

The inverse affine transform (IAFT) restores the pixel (x', y') to its original position (x, y), and is defined as

$$\begin{bmatrix} x \\ y \end{bmatrix} = \text{IAFT}\{(x', y'), N\} = \begin{bmatrix} (x' - a)c^{-1} \\ (y' - b)d^{-1} \end{bmatrix} (\text{mod}\, N) \tag{4}$$

where c^{-1} and d^{-1} are modulo inverse of c and d, respectively. The effect of AFT on a grayscale image of *Boy* (Fig. 1**a**) of size 256 × 256 pixels is illustrated in Figs. 1**b** and 1**c** for two representative values of w (1 and 20). Here, we have considered the following values of AFT parameters: $a = 50$, $b = 70$, $c = 29$ and $d = 31$. Figures 1**d**–1**f** are histograms of Figs. 1**a**–1**c**, respectively. Histograms analysis reveals that energy of the system remains constant before and after applying the AFT.

3. The proposed scheme

In the proposed scheme as shown in the flowchart (Fig. 2), an input color image is first decomposed in its RGB (red, green and blue) channels. Each channel is bonded with a random phase mask $\text{RPM}_1 = \exp\{2\pi i m(x, y)\}$ and transformed by a FrHT of order (p, r) followed by the AFT of order w in the frequency domain. Thereafter, a second random phase mask $\text{RPM}_2 = \exp\{2\pi i n(u, v)\}$ is applied to each component before the final transformation by a FrHT of order (q, s) resulting in a component-wise encrypted image. The functions $m(x, y)$ and $n(u, v)$ are random white sequences uniformly distributed with values between 0 and 1. Thus, the two random phase masks RPM_1 and RPM_2 are statistically independent. Finally, all three components are combined to give a single channel encrypted image. The use of double transform and double phase masks is in accordance with the 4-*f* system followed in optical implementation of the scheme.

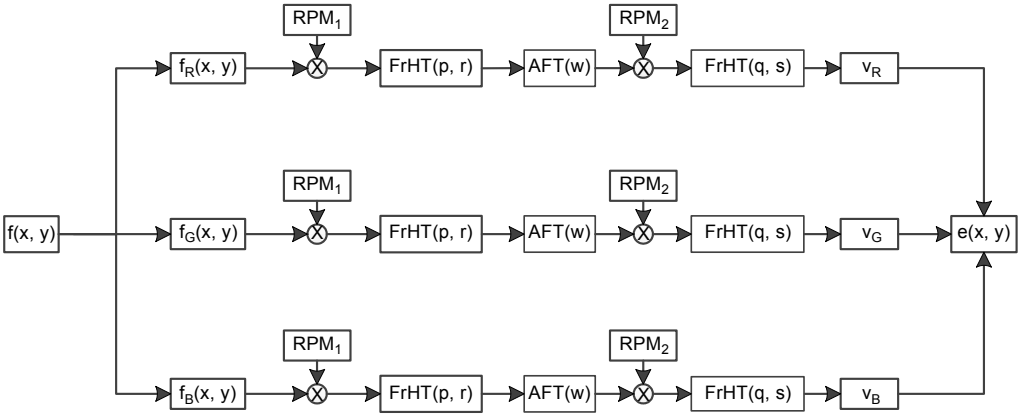

Fig. 2. Flowchart of the proposed scheme of encryption process.

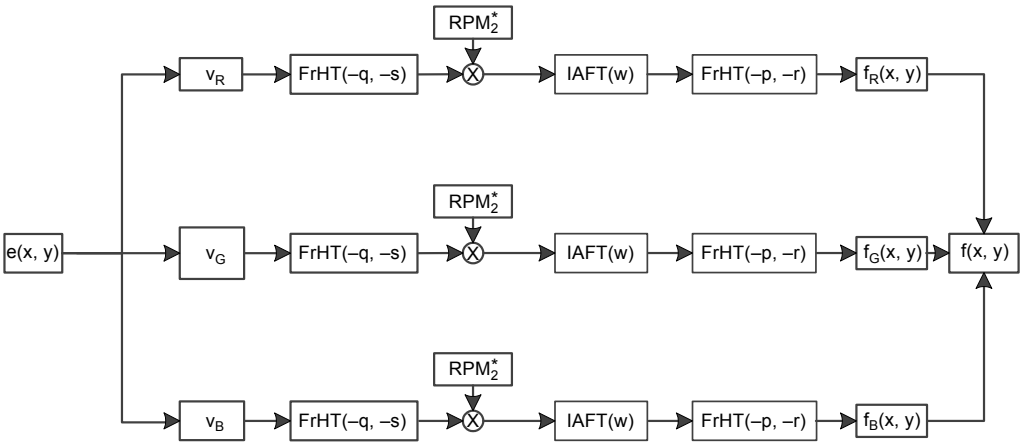

Fig. 3. Flowchart of the proposed scheme of decryption process.

The decryption process is simply reverse of the encryption (Fig. 3). First, the encrypted image is decomposed in its RGB encrypted channels followed by the inverse FrHT of orders $(-q, -s)$. Each encrypted image so obtained in the frequency domain is bonded with conjugate of the second random phase mask RPM_2 followed by the IAFT of the same order. Each resulting image is then subjected to the inverse FrHT of orders $(-p, -r)$. Finally, all the three transformed components are combined to give the recovered image.

4. Results and discussion

The proposed scheme has been validated for color images. Here, we present the simulation results performed on MATLAB 7.14 for an original image of *Boy* (Fig. 4**a**) of size $256 \times 256 \times 3$ pixels. For the sake of simplicity, we have considered FrHT orders $p = r$ and $q = s$ in our simulations. The values of the AFT and FrHT parameters considered in this study are $w = 20$, $p = 0.8$, and $q = 0.5$. The original image is decomposed into RGB channels, each encrypted according to the scheme detailed in Fig. 2. The three components (RGB) of the original image are shown in Figs. 4**b**–4**d**, respectively. The combined and component-wise encrypted images are depicted in Figs. 4**e**–4**h**, respectively. Each encrypted image is completely random and resembles stationary white noise. The original color image as well as its RGB components are completely recovered (Figs. 4**i**–4**l**) using the proposed scheme's decryption process (Fig. 3), thus validating the scheme.

4.1. Sensitivity analysis

A scheme is considered to be secure if it is sensitive to the encryption parameters. In the proposed scheme, the main encryption parameters include the order of the AFT w and

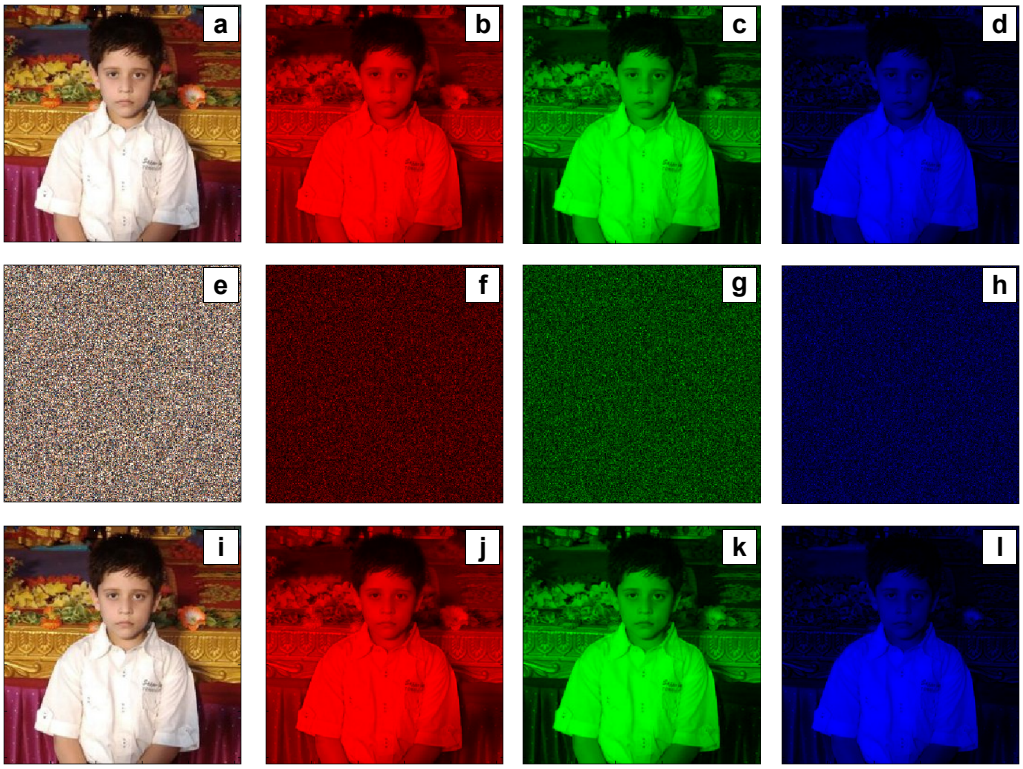

Fig. 4. Results of validation of the proposed scheme. Input color image (*Boy*) 256 × 256 × 3 pixels (**a**); its RGB channels (**b**, **c**, **d**); corresponding encrypted (**e**, **f**, **g**, **h**) and recovered (**i**, **j**, **k**, **l**) images.

the orders of the FrHT. We have performed the scheme's sensitivity to these parameters and presented the results in terms of commonly used metrics such as a correlation coefficient (CC) and a mean-squared error (MSE) which are defined as follows:

$$\mathrm{CC} = \frac{\mathrm{cov}(I_\mathrm{o}, I_\mathrm{r})}{\sigma(I_\mathrm{o})\,\sigma(I_\mathrm{r})} \tag{5}$$

$$\mathrm{MSE} = \frac{1}{N \times N} \sum_{x=1}^{N} \sum_{y=1}^{N} \left| I_\mathrm{o}(x, y) - I_\mathrm{r}(x, y) \right|^2 \tag{6}$$

where $I_\mathrm{o}(x, y)$ and $I_\mathrm{r}(x, y)$ denote respectively the pixel values of the original and the recovered image; cov is covariance and σ is the standard deviation.

The results of the scheme's sensitivity to AFT parameter w are shown in Fig. 5. While Fig. 5**a** shows the plot of MSE against w for the red channel of the color image of *Boy*, Fig. 5**b** gives the recovered image for a wrong value of the AFT parameter. Similar results were obtained for green and blue channels also. This shows a very high

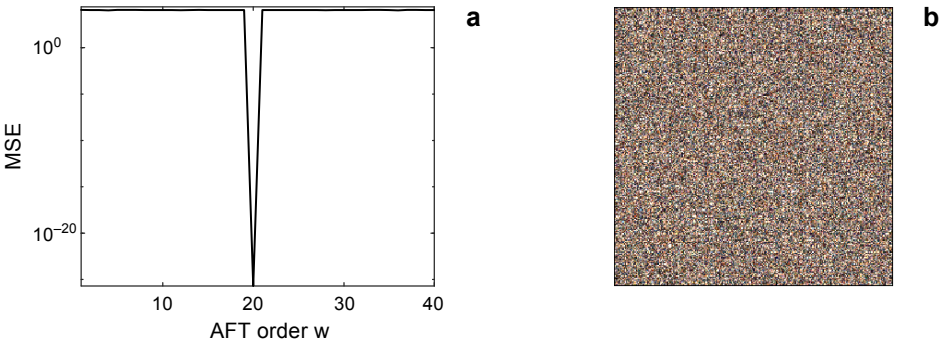

Fig. 5. Sensitivity plots relative to AFT parameter w: MSE (**a**), and decrypted image with wrong AFT parameter ($w = 21$, whereas correct AFT parameter is $w = 20$) (**b**).

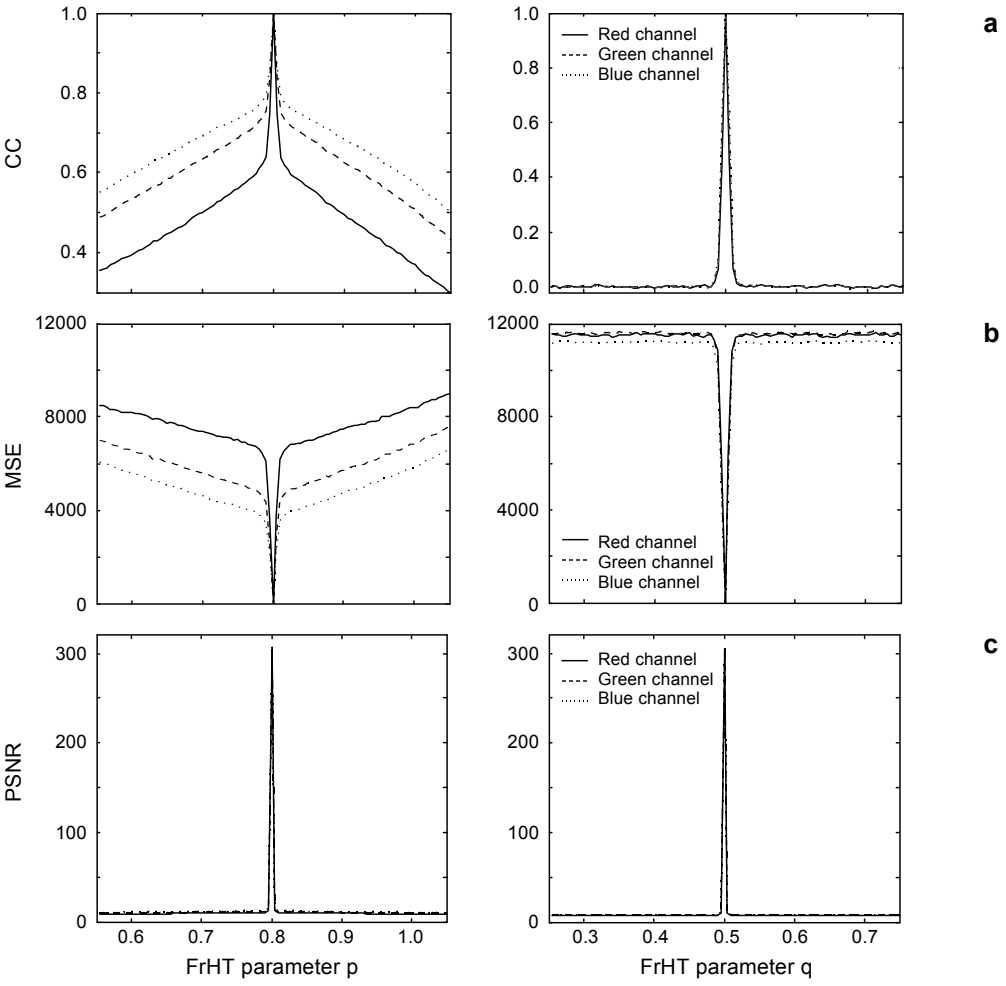

Fig. 6. Sensitivity plots of CC (**a**), MSE (**b**), and PSNR (**c**) relative to FrHT parameters p and q.

degree of sensitivity of the proposed scheme with respect to the AFT parameter w. We have also analysed the scheme's sensitivity to the FrHT orders p and q in the spatial domain and frequency domain, respectively. The sensitivity plots of CC, MSE and PSNR (peak signal-to-noise ratio) with respect to the FrHT orders p and q are shown in Fig. 6. It is observed from Fig. 6 that FrHT order q in the frequency domain shows greater sensitivity to the scheme as compared to the order p. These results establish that the scheme is sensitive to all the encryption parameters appearing as the orders of AFT and FrHT.

4.2. Occlusion and noise attacks analysis

The proposed scheme is also tested for its strength to occlusion and noise attacks. First we performed occlusion attack analysis on the encrypted image of *Boy*. The encrypted image of *Boy* occluded in a gradual manner (20%, 30%, 40%, and 50% occlusion) is shown in Figs. 7**a**–7**d** and the corresponding recovered images are provided in

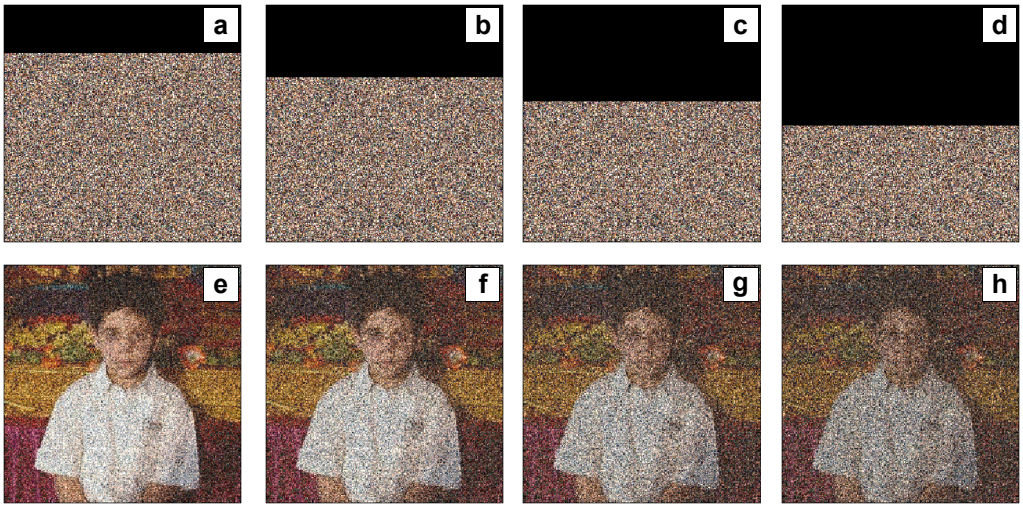

Fig. 7. Occlusion results for the color image for varying degrees of occlusion. Encrypted images of *Boy* with 20%, 30%, 40%, and 50% occlusion (**a**–**d**), and corresponding recovered images (**e**–**h**).

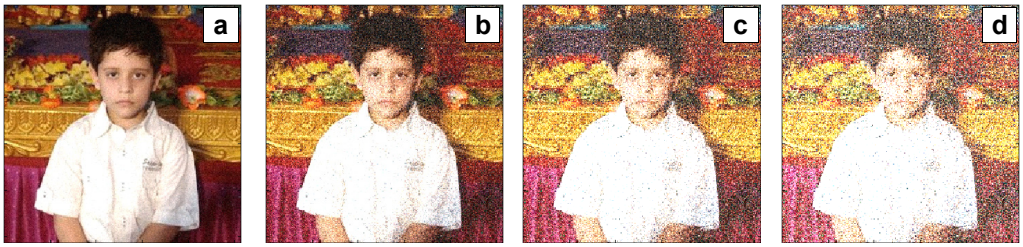

Fig. 8. Results of decryption in the presence of Gaussian multiplicative noise with zero mean and standard deviation 1, and with noise strength $k = 0.2$ (**a**), $k = 0.8$ (**b**), $k = 1.4$ (**c**) and $k = 2$ (**d**).

Figs. 7**e**–7**h**. Although the quality of the recovered image drops with the increase in occluded area, it is recognizable even when the encrypted image is occluded up to nearly 50%. The impact of occlusion for a wider range of occluded area is indicated in the plots of CC and MSE (Figs. 9**c** and 9**d**) for red channel.

Similarly, we have presented the results of noise attack on the encrypted image of *Boy* in Fig. 8 for varying degrees of noise strength k according to the formula [27]

$$E_o = E(1 + kG) \tag{7}$$

where E_o is the noise-affected encrypted image, and G is the Gaussian noise with zero mean and standard deviation unity. Figure 8 gives the recovered images when the encrypted image is noise-affected with increasing noise strength $k = 0.2$, 0.8, 1.4 and 2, respectively. We observe that even in the presence of significant noise in the encrypted image, the quality of recovered image is fairly good.

The extent of drop in the quality of the recovered image can be gauged from the plots of CC and MSE *versus* noise strength k (Figs. 9**a** and 9**b**) for red channel. We

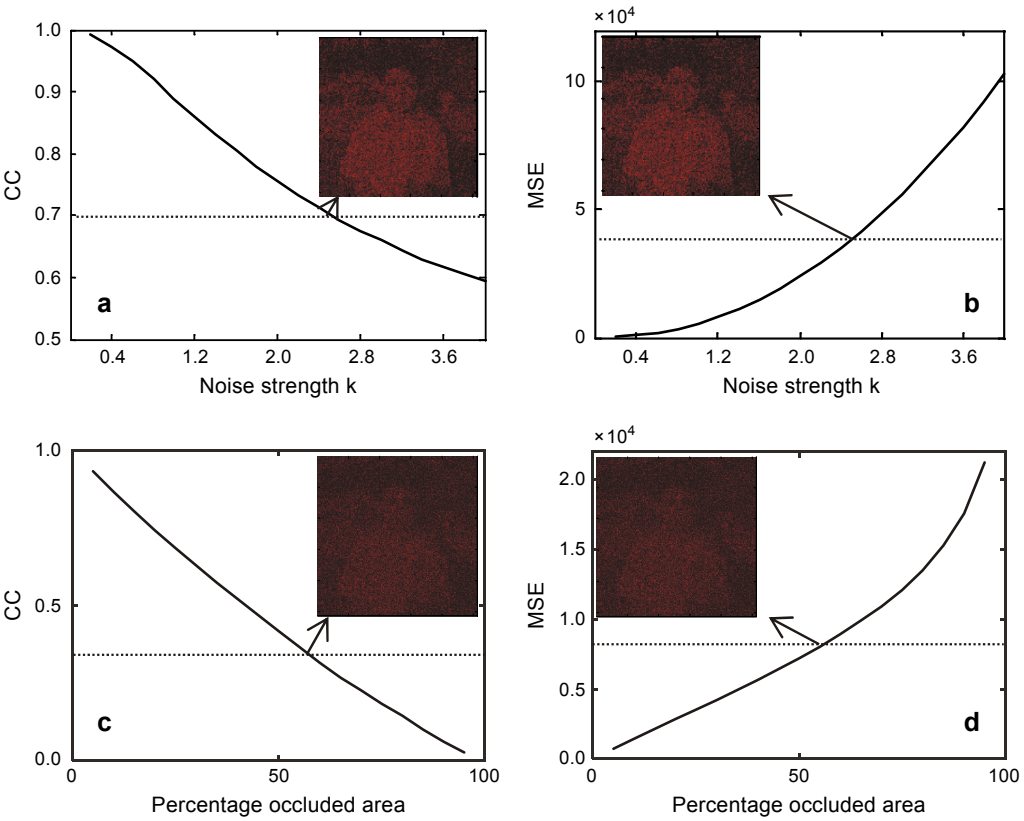

Fig. 9. Plots of noise attack with strength k *versus* CC (**a**) and MSE (**b**). Plots of occlusion attack with percentage occluded area *versus* CC (**c**) and MSE (**d**). Threshold values of noise strength $k = 2.5$ and occlusion equal to 60% are used for the recovered images (inset).

have also shown the recovered images (inset) for threshold values of CC and MSE, respectively. Similar results were also obtained for green and blue channels. We observe that the scheme is quite resistant to the noise and occlusion attacks.

4.3. Histogram analysis

Statistical analysis (histogram) has been performed to validate the proposed scheme. For a good encryption algorithm, the histogram of the encrypted image should be totally different from the histogram of the original image. Figures 10**a**–10**c** show the histograms of the input, encrypted and decrypted images of red channel. It is clearly

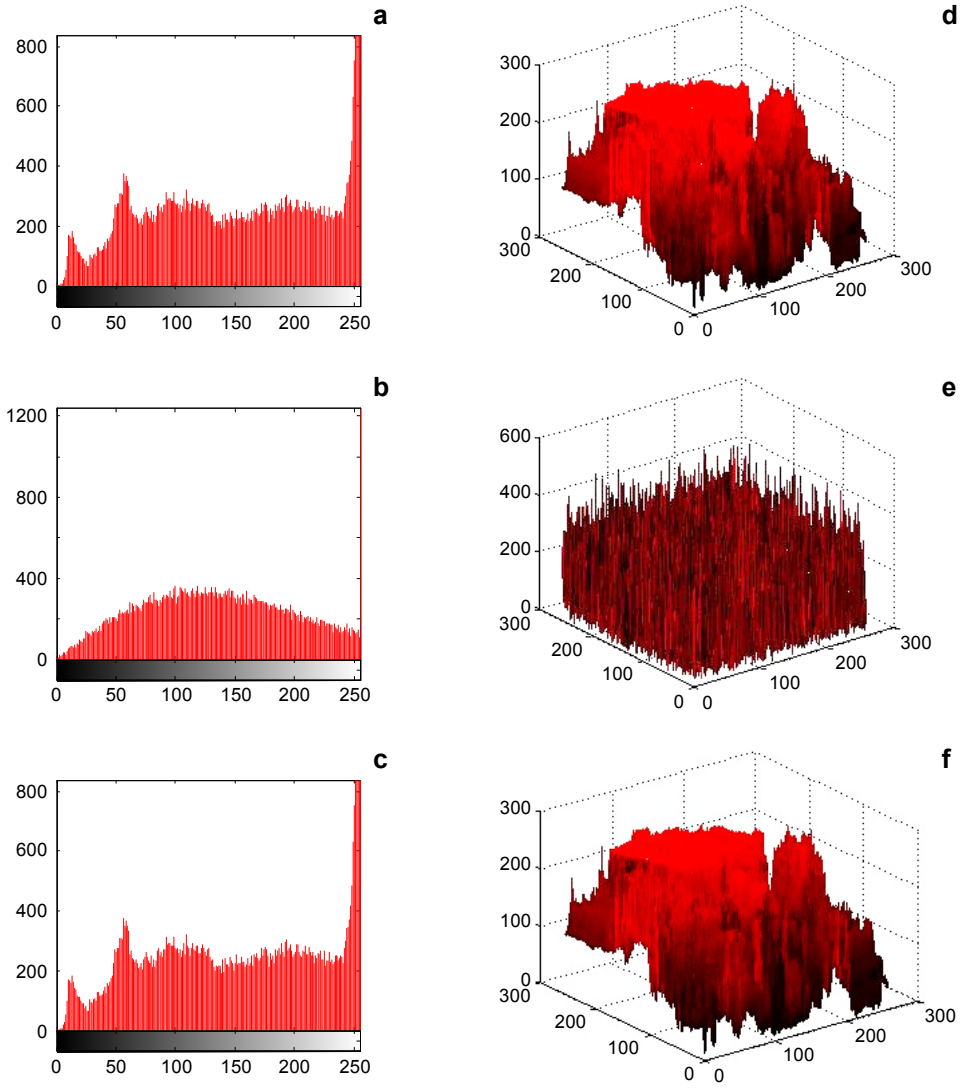

Fig. 10. Histograms and 3D plots of red channel. Input (**a**, **d**), encrypted (**b**, **e**) and decrypted (**c**, **f**) images.

visible that the histograms of the original and decrypted images are identical and the histogram of the encrypted image is totally different from that of the original image for the current scheme. Also, 3D plots of the input, the encrypted and the decrypted images (Figs. 10**d**–10**f** for the red channel), establish the efficacy of the scheme as observed in the histograms.

5. Conclusions

In this study, we have proposed an encryption scheme for color images. It uses the affine transform for pixel scrambling and the FrHT for encryption of each channel of the original color image. The scheme has been validated for input color images of size $256 \times 256 \times 3$ pixels by experiments on MATLAB 7.14. Its performance is tested through statistical analysis based on histograms and 3D plots. We have also investigated the scheme for its sensitivity to the transform orders as the encryption parameters. The scheme shows robustness to the attacks of multiplicative noise and occlusion.

References

[1] PEREZ-CABRE E., MILLAN M.S., *Optical data encryption*, [In] *Optical and Digital Image Processing: Fundamentals and Applications*, Cristobal G., Schelkens P., Thienpont H., [Eds.], Wiley, 2011, pp. 739–767.

[2] WEN CHEN, JAVIDI B., XUDONG CHEN, *Advances in optical security systems*, Advances in Optics and Photonics **6**(2), 2014, pp. 120–155.

[3] JAVIDI B., CARNICER A., YAMAGUCHI M., NOMURA T., PÉREZ-CABRÉ E., MILLÁN M.S., NISHCHAL N.K., TORROBA R., BARRERA J.F., WENQI HE, XIANG PENG, STERN A., RIVENSON Y., ALFALOU A., BROSSEAU C., CHANGLIANG GUO, SHERIDAN J.T., GUOHAI SITU, NARUSE M., MATSUMOTO T., JUVELLS I., TAJAHUERCE E., LANCIS J., WEN CHEN, XUDONG CHEN, PINKSE P.W.H., MOSK A.P., MARKMAN A., *Roadmap on optical security*, Journal of Optics **18**(8), 2016, article ID 083001.

[4] REFREIGER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.

[5] KUMAR P., JOSEPH J., SINGH K., *Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and counter measures*, [In] *Linear Canonical Transforms: Theory and Applications*, Healy J.J., Kutay M.A., Ozaktas H.M., Sheridan J.T., [Eds.], Springer Science, New York, 2016, Chap.13, pp. 367–396.

[6] LINFEI CHEN, DAOMU ZHAO, *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006, pp. 3438–3440.

[7] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000, pp. 887–889.

[8] HENNELLY B.M., SHERIDAN J.T., *Image encryption and the fractional Fourier transform*, Optik – International Journal for Light and Electron Optics **114**(6), 2003, pp. 251–265.

[9] NANRUN ZHOU, YIXIAN WANG, LIHUA GONG, *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242.

[10] VASHISTH S., SINGH H., YADAV A.K., SINGH K., *Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval*, Optik – International Journal for Light and Electron Optics **125**(18), 2014, pp. 5309–5315.

[11] 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*, International Journal of Optics, Vol. 2014, 2014, article ID 728056.
[12] SOO-CHANG PEI, CHIEN-CHENG TSENG, MIN-HUNG YEH, JONG-JY SHYU, *Discrete fractional Hartley and Fourier transforms*, IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **45**(6), 1998, pp. 665–675.
[13] ALIEVA T., BASTIAANS M.J., CALVO M.L., *Fractional transforms in optical information processing*, EURASIP Journal on Advances in Signal Processing **10**, 2005, pp. 1498–1519.
[14] LI XIN-XIN, ZHAO DAO-MU, *Optical image encryption with simplified fractional Hartley transform*, Chinese Physics Letters **25**(7), 2008, pp. 2477–2480.
[15] DAOMU ZHAO, XINXIN LI, LINFEI CHEN, *Optical image encryption with redefined fractional Hartley transform*, Optics Communications **281**(21), 2008, pp. 5326–5329.
[16] XINXIN LI, DAOMU ZHAO, *Optical color image encryption with redefined fractional Hartley transform*, Optik – International Journal for Light and Electron Optics **121**(7), 2010, pp. 673–677.
[17] JIMENEZ C., TORRES C., MATTOS L., *Fractional Hartley transform applied to optical image encryption*, Journal of Physics: Conference Series **274**(1), 2011, article ID 012041.
[18] VILARDY J.M., TORRES C.O., JIMENEZ C.J., *Double image encryption method using the Arnold transform in the fractional Hartley domain*, Proceedings of SPIE **8785**, 2013, article ID 87851R.
[19] YE LIU, JUAN DU, JINGHUI FAN, LIHUA GONG, *Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation*, Multimedia Tools and Applications **74**(9), 2015, pp. 3171–3182.
[20] WEN-LIANG HSUE, WEI-CHING CHANG, *Real discrete fractional Fourier, Hartley, generalized Fourier and generalized Hartley transforms with many parameters*, IEEE Transactions on Circuits and Systems I: Regular Papers **62**(10), 2015, pp. 2594–2605.
[21] SINGH P., YADAV A.K., SINGH K., *Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition*, Optics and Lasers in Engineering **91**, 2017, pp. 187–195.
[22] NAG A., SINGH J.P., KHAN S., GHOSH S., BISWAS S., SARKAR D., SARKAR P.P., *Image encryption using affine transform and XOR operation*, 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011, pp. 309–312.
[23] SHUQUN ZHANG, KARIM M.A., *Color image encryption using double random phase encoding*, Microwave and Optical Technology Letters **21**(5), 1999, pp. 318–322.
[24] ZHENGJUN LIU, JINGMIN DAI, XIAOGANG SUN, SHUTIAN LIU, *Color image encryption by using the rotation of color vector in Hartley transform domains*, Optics and Lasers in Engineering **48**(7–8), 2010, pp. 800–805.
[25] ZHENGJUN LIU, LIE XU, TING LIU, HANG CHEN, PENGFEI LI, CHUANG LIN, SHUTIAN LIU, *Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains*, Optics Communications **284**(1), 2011, pp. 123–128.
[26] ZHENGJUN LIU, YU ZHANG, WEI LIU, FANYI MENG, QUN WU, SHUTIAN LIU, *Optical color image hiding scheme based on chaotic mapping and Hartley transform*, Optics and Lasers in Engineering **51**(8), 2013, pp. 967–972.
[27] SINGH H., YADAV A.K., VASHISTH S., SINGH K., *Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane*, Optics and Lasers in Engineering **67**, 2015, pp. 145–156.

Received December 1, 2016
in revised form January 25, 2017