An Asymmetric Hybrid Watermarking Mechanism Using Hyperchaotic System and Random Decomposition in 2D Non Separable Linear Canonical Domain

PANKAJ RAKHEJA¹,*, REKHA VIG¹ and PHOOL SINGH²

¹Department of EECE, TheNorthCap University, Gurugram 122 017, India
²Department of Mathematics, SOET, Central University of Haryana, Mahendergarh 123 031, India

(Received on 14 March 2018; Revised on 23 August 2018; Accepted on 24 August 2018)

In this paper, an asymmetric hybrid watermarking scheme utilizing four-dimensional (4D) hyperchaotic system with coherent superposition and random decomposition in 2D non-separable linear canonical domain is proposed. The 4D hyperchaotic framework is used for creating permutation keystream for a pixel-swapping mechanism. Its parameters and initial conditions along with the independent parameters of the 2D Non separable linear canonical transform extend the key-space and consequently strengthen the proposed watermarking scheme. The designed watermarking scheme has an extended key-space to avoid any brute-force attack and is non-linear in nature. The scheme is validated on grayscale images. Computer based simulations have been performed to validate the robustness of the proposed watermarking scheme against different types of attacks. Results demonstrate that the proposed scheme not only offers higher protection against brute force and occlusion attacks but is also invulnerable to special attack.

Keywords: 4D Hyperchaotic System; Random Decomposition; 2D Non-Separable Linear Canonical Transform

Introduction

Watermarking is a powerful methodology with great potential to tackle copyright assurance and security issues of data. From the digital point of view there are two broad classifications of watermarking namely symmetric and asymmetric watermarking. The keys required for watermarks embedding and detection are same in symmetric watermarking schemes whereas in asymmetric watermarking, required keys are different. Data being embedded can also be encoded for further reinforcing the watermarking scheme and for encryption; digital or optical encryption can be carried out. From last few decades optical cryptosystems have gained a lot of popularity among researchers because of their large information capacity with provision of parallel processing. In 1995, Refregier and Javidi (Refregier and Javidi, 1995) proposed double random phase encoding (DRPE). DRPE based optical schemes were later investigated and enhanced by various researchers (Unnikrishnan, Joseph and Singh, 2000; Kumar Nishchal et al., 2004; Situ and Zhang, 2004; Cheng et al., 2008; Chen, Chen and Sheppard, 2010; Deng and Zhao, 2012). To enhance the security of optical encryption schemes various advanced technologies were also combined (Tajahuerce et al., 2000; Liu, Mi and Zhu, 2001; Liu et al., 2011; Liu, Liu and Liu, 2013; Chen and Zhao, 2006; Zhou, Wang and Gong, 2011; Huang et al., 2012; Zhao et al., 2015; Singh, Yadav and Singh, 2017).

Extensive research has also been carried out in optical watermarking area were work has been done in Fourier domain (Sheng et al., 2009), gyrator wavelet domain (Abuturab, 2015), gyraor domain (Li, 2014; Yadav et al., 2015; Liansheng et al., 2017); fractional Fourier transform domain (Guo, Liu and Liucora, 2011; Lang and Zhang, 2014); wavelet domain (Mendlovic and Konforti, 1993; Javidi et al., 2006; Okman and Akar, 2007; Li et al., 2008, 2009; Hwang, Chan and Cheng, 2014; Mehra and Nishchal, 2015); kinoform transform (Deng, Yang and Xie, 2015).

*Author for Correspondence: E-mail: pankajrakheja@ncuindia.edu
804

Pankaj Rakheja et al.

2011); using orthogonal transforms: discrete cosine transform (DCT), discrete wavelet transform (DWT), Hadamard-Walsh (Ishikawa, Uehira and Yanaka, 2012); in DCT domain (Starchenko, 2011); based on 5-DWT, fast Fourier transform (FFT) & singular value decomposition (SVD) (Mittal, Bisen and Gupta, 2017).

Here in all these transforms number of independent variables were limited as gyrator transform and fractional Fourier transform has one independent variable, Fresnel transform has two independent variables whereas there is no independent variable in Fourier transform. So, these transforms can extend key-space to a limited extent only. In order to extend or enhance the key-space, a family of integral transforms that is linear canonical transform (Healy et al., 2016) can be utilized which has more independent variables than classical transforms. Moreover two-dimensional non-separable linear canonical transform 2D NS - LCT (Koç, Ozaktas and Hesselink, 2010; Ding and Pei, 2011a; Zhao, Healy and Sheridan, 2014) which has ten independent variables can further enhance the key space strengthen the encryption process.

Cai et al. (Cai et al., 2015) in 2015, proposed an asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition (EMD) where a random phase mask was added to the input image and two equal moduli masks were generated, where one acts as ciphertext whereas other serves as private key. However, Deng (Deng, 2015) investigated and proved the vulnerability of EMD based schemes to special attacks and its variants. In order to enhance the security of cryptosystems based on EMD, many schemes were later proposed (Fatima, Mehra and Nishchal, 2016; Barfungpa and Abuturab, 2016; Chen et al., 2017). Wang et al. (Wang, Quan and Tay, 2016) proposed an alternative scheme to EMD cryptosystem popularly known as random decomposition where two random masks of different moduli were produced, it was done to limit the available constraint conditions for executing iterative transform based attacks. Later, Xu et al. (Xu et al., 2018) exposed the vulnerability of EMD based systems and extended the random modulus decomposition in Fresnel domain which extended the key space and enhanced the security of the existing system in Fourier domain.

Through the process of scrambling the image, correlation amongst the adjacent pixels can be reduced. This can be accomplished best by using chaotic systems. Many researchers have employed various types of chaotic systems like 3D Lorentz chaotic system (Sharma et al., 2017), 2D logistic maps (Chai, Chen and Broyde, 2017), chaotic Baker map (Elshamy et al., 2013; Chen et al., 2014) and 4D hyperchaotic system (Fu et al., 2018) for this purpose. It not only extended the key space but also increased the amount of uncertainty in the resultant ciphertext image.

Here in this paper an asymmetric watermarking scheme based on single random decomposition in two-dimensional non separable linear canonical transform 2D NS - LCT is proposed. Here the ten independent variables of 2D NS - LCT matrix are used as additional keys to strengthen the scheme. And to decorrelate encrypted watermark image’s pixels 4D hyper chaotic system has been employed. The proposed watermarking system is invulnerable to special attack, and robust against noise attack and occlusion attack. Section 2, of the paper briefly describes the basic principle and theory behind: 4D hyper chaotic systems, random decomposition, two-dimensional non separable linear canonical transform and the proposed scheme. Section 3, has results obtained through MATLAB simulations to demonstrate the validity and robustness of the proposed scheme and it also explores the significance of the results of the work. Concluding remarks are summarized in the final section of the paper.

**Related Background**

In this section, 4D hyperchaotic system, random decomposition and 2D non-separable linear canonical transform are explained in brief. Thereafter, the proposed cryptosystem is explained in detail.

**Permutation Keystream Generation Using 4D Hyperchaotic System**

The proposed encryption scheme employs the hyperchaotic Lü system (Chen et al., 2006) for generating permutation keystream sequence (Fu et al., 2018). The 4D chaotic framework is very much depicted by equation (1)
An Asymmetric Hybrid Watermarking Mechanism

\[
\begin{align*}
\frac{dx}{dt} &= a(y-x)+u \\
\frac{dy}{dt} &= -xz+cy \\
\frac{dz}{dt} &= xy-bz \\
\frac{du}{dt} &= xz+du.
\end{align*}
\]

Here \(a, b\) and \(c\) are constants of the system and \(d\) is its control parameter as described in (Chen et al., 2006). When \(a=36, b=3, c=20,\) and \(-0.36 < d \leq 1.30\), the Lü system exhibits a hyperchaotic behaviour, and the projections of its phase portrait are shown in Fig. 1. As the initial values of \((x, t, z, u)\) remarkably decide the chaotic trajectory of the framework, along with these lines, they fill in as secret key for getting permutation sequence.

The pixels of the input image are scrambled using the permutation sequence generated by 4D hyperchaotic system. To carry out the permutation process first pixels of the input image \((size H \times W)\) are organized into a one dimensional array \(1\text{D} \text{array} = \{p_0, p_1, \ldots, p_{M \times N-1}\}\) in the order from left to right and top to bottom. Hyperchaotic sequence of length \(\text{Len}_\text{per} = \text{length}(1\text{Darray}) - 1\) is generated by iterating hyperchaotic system. For keeping away the destructive impacts of transitional methodology, pre-iterate the 4D hyperchaotic system \(N_1\) (constant) number of times. The fourth order Runge-Kutta method (Butcher, 1987) can be employed for numerically solving the system with the step size \(h_2 = 0.005\) as shown below (2)

\[
\begin{align*}
x_{n+1} &= x_n + \frac{h_2}{6}(K_1 + 2 \times K_2 + 2 \times K_3 + K_4), \\
y_{n+1} &= y_n + \frac{h_2}{6}(L_1 + 2 \times L_2 + 2 \times L_3 + L_4), \\
z_{n+1} &= z_n + \frac{h_2}{6}(M_1 + 2 \times M_2 + 2 \times M_3 + M_4), \\
u_{n+1} &= u_n + \frac{h_2}{6}(N_1 + 2 \times N_2 + 2 \times N_3 + N_4),
\end{align*}
\]

where,

\[
\begin{align*}
K_j &= a(y_n-x_n)+u_n, \\
L_j &= -x_nz_n+cy_n, \\
M_j &= x_ny_n-bz_n, \\
N_j &= x_nz_n+du_n,
\end{align*}
\]

with \(j = 1\)

\[
\begin{align*}
K_1 &= a \times \left[ (y_n + \frac{h_2 \times K_{j-1}}{2}) - (x_n + \frac{h_2 \times K_{j-1}}{2}) \right] + \left( u_n + \frac{h_2 \times N_{j-1}}{2} \right), \\
L_1 &= -\left( x_n + \frac{h_2 \times K_{j-1}}{2} \right) \left( z_n + \frac{h_2 \times M_{j-1}}{2} \right) + c \\
& \quad \times \left( y_n + \frac{h_2 \times L_{j-1}}{2} \right)
\end{align*}
\]  

Fig. 1: The projections of phase portrait of the hyperchaotic system (Fu et al., 2018) with \(a=36, b=3, c=20,\) and \(d=1.10.\) (a) \(x-y\) plane; (b) \(x-z\) plane; (c) \(x-u\) plane; (d) \(y-z\) plane; (e) \(y-u\) plane; (f) \(z-u\) plane respectively.
\[
M_j = \left( x_n + \frac{h_x \times K_{j-1}}{2} \right) \left( y_n + \frac{h_y \times L_{j-1}}{2} \right) - b
\]
\[
\times \left( z_n + \frac{h_z \times M_{j-1}}{2} \right)
\]
\[
N_j = \left( x_n + \frac{h_x \times K_{j-1}}{2} \right) \left( z_n + \frac{h_z \times M_{j-1}}{2} \right) + d
\]
\[
\times \left( u_n + \frac{h_u \times N_{j-1}}{2} \right)
\]
with \( j = 2, 3 \)
\[
K_j = a \times \left[ \left( y_n + h_y L_{j-1} \right) - \left( x_n + h_x K_{j-1} \right) \right] + \left( u_n + h_u N_{j-1} \right)
\]
\[
L_j = -\left( x_n + h_x K_{j-1} \right) \left( z_n + h_z M_{j-1} \right) + c
\]
\[
\times \left( y_n + h_y L_{j-1} \right)
\]
\[
M_j = -\left( x_n + h_x K_{j-1} \right) \left( y_n + h_y L_{j-1} \right) - b
\]
\[
\times \left( z_n + h_z M_{j-1} \right)
\]
\[
N_j = -\left( x_n + h_x K_{j-1} \right) \left( z_n + h_z M_{j-1} \right) + d
\]
\[
\times \left( u_n + h_u N_{j-1} \right)
\]
with \( j = 4 \).

To extricate the permutation keystream the chaotic sequence obtained is arranged and sorted into a row matrix. Then the pixels or elements of 1Darray are adjusted as per the sorted sequence. Then at last the scrambled 1Darray is reshaped into a matrix of size HxW.

**Random Decomposition**

Random decomposition was designed by Wang et al. (Wang et al., 2016) as an alternative to equal modulus decomposition. Here two complex-valued masks of different moduli are obtained from Fourier spectrum of the input image. One of the masks acts as the private key while the other serves as ciphertext. First level of decomposition is shown in the Fig. 2, where random phase mask \( R(x) \) and random argument functions \( \alpha \) and \( \beta \) are used in random decomposition process and they all serve as public keys.

For simplicity, one dimensional notation is used here. If \( I(x) \) refers to the intensity distribution of the image taken as input then \( I'(u) \) can be obtained by using the equation (4) below

\[
I'(u) = FT \left\{ \sqrt{I(x)R(x)} \right\}
\]  
(4)

where \( FT \) denotes the Fourier transform. Amplitude and phase part of \( I'(u) \) can be represented as \( A(u) = \text{abs}(I'(u)) \) and \( \varphi(u) = \text{arg}(I'(u)) \), respectively. Figure 3 shows the basic principle of random decomposition wherein \( I'(u) \) is divided into \( P_1(u) \) and \( P'_1(u) \), where \( \alpha_1 \) and \( \beta_1 \) are random function distributed in interval \([0, 2\pi]\).

\[
P_1(u) = \frac{A(u)}{2 \sin(\beta_1 + \alpha_1)} \exp(i(\varphi(u) - \alpha_1))
\]  
(5)

\[
P'_1(u) = \frac{A(u)}{2 \sin(\beta_1 + \alpha_1)} \exp(i(\varphi(u) + \beta_1))
\]  
(6)

**2D Non-separable Linear Canonical Transform**

The two-dimensional non-separable linear canonical transform (2D NS-LCT) is a more general integral transform, wherein the two dimensions are coupled to each other by four additional cross-parameters,
increasing the total number of free parameters to ten. The continuous \(2D\, NS-LCT\) of a signal \(f(x,y)\) can be defined by (Koç et al., 2010; Ding and Pei, 2011a; Zhao et al., 2014)

\[
F(x', y') = L_M \{f(x, y)\} \{x', y'\}
\]

where

\[
k_i = d_{11}b_{22} - d_{12}b_{21}, \quad k_2 = 2(-d_{11}b_{22} + d_{12}b_{11})
\]

\[
k_3 = -d_{21}b_{22} + d_{22}b_{11}, \quad p_1 = a_{11}b_{12} - a_{21}b_{12}
\]

\[
p_2 = 2(a_{12}b_{22} - a_{22}b_{21}), \quad p_3 = -a_{12}b_{21} + a_{22}b_{11}
\]

The transform matrix of the system is defined as

\[
M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}
\]

where \(A, B, C\) and \(D\) are \(2\times2\) submatrices and \(\det(B) \neq 0\). Matrix \(M\) has 16 parameters as in equation 10, which must satisfy the following constraints

\[
AB^T = BA^T \quad \text{OR} \quad A^T C = C^T A
\]

\[
CD^T = DC^T \quad \text{OR} \quad B^T D = D^T B
\]

\[
AD^T - BC^T = I \quad A^T D - C^T B = I
\]

Here \(I\) is a \(2\times2\) identity matrix and these constraints or equations reduce the number of independent variables to ten (Alieva and Bastiaans, 2005; Koç et al., 2010; Ding and Pei, 2011b; Ding, Pei and Liu, 2012; Zhao, Healy and Sheridan, 2013). And the inverse of \(2D\, NS-LCT\) of \(F(x', y')\) can be obtained by

\[
f(x, y) = L_M^{-1} \{F(x', y')\}(x, y)
\]

The Scheme

The schematic flowchart of the proposed watermarking scheme is shown in Fig. 4 below. Herein one level random decomposition (Wang et al., 2016) is performed on two-dimensional non-separable linear canonical transform \(2D\, NS-LCT\) of 4D chaotic scrambled image.

\(I(x)\) here refers to the intensity distribution of the input watermark image taken, whereas the intensity distribution of the image obtained after scrambling pixels of input watermark image \(I\) as per permutation sequence obtained through hyperchaotic Lü system (Chen et al., 2006) is represented by \(I_{SC}(x)\). \(I_{SC}'(u)\) denotes the intensity distribution of \(I_{SC}(x)\) in the \(2D\, NS-LCT\) domain obtained from the following equation (17).

\[
I_{SC}'(u) = 2D\, NS-LCT \left\{\sqrt{I_{SC}(x)} \cdot RPM_1\right\}
\]

where \(2D\, NS-LCT\) represents two-dimensional non-separable linear canonical transform and
$RPM_1 = \exp(i\pi \text{rand}(x))$ is the random phase mask, \text{rand}(x) is a pseudo-random number generator having values between [0,1], obtained using MATLAB. Another random phase mask $RPM_2 = \exp(i\pi \text{rand}(x))$ is applied on $I_{SC}'(u)$ to get $I_{SCm}'(u)$.

Then later two masks $P1(u)$ and $P1'(u)$ are generated with the help of random decomposition, given by the equations below:

$$P1(u) = \frac{A(u)}{2 \sin(\beta_1 + \alpha_1)} \cdot \exp(i(\varphi(u) - \alpha_1)) \quad (17)$$

$$P1'(u) = \frac{A(u)}{2 \sin(\beta_1 + \alpha_1)} \cdot \exp(i(\varphi(u) + \beta_1)) \quad (18)$$

where $A(u)$ and $\varphi(u)$ represents the phase and amplitude part of $I_{SCm}'(u)$, $\alpha_1$ and $\beta_1$ are random function distributed uniformly in interval $[0, 2\pi]$. Normalized encrypted watermark is obtained by amplitude truncation of $P1'(u)$

$$E_W = P1'(u) / \text{abs}(P1'(u)) \quad (19)$$

Normalized encrypted watermark image $E_W$ is added to host image $I_h(x)$ to get watermarked image $I_w(x)$

$$I_w(x) = I_h(x) + \beta E_W \quad (20)$$

Here $\beta$ is the attenuation parameter. Two non-orthogonally oriented cylindrical lenses ($L_1$ and $L_2$) of focal lengths $f_1$ and $f_2$ can be used for optically realizing 2D NS-LCT (Kumar et al., 2018) as shown in Fig. 5. These lenses are placed in a plane parallel to the input and output planes while being
perpendicular to the optical axis, $z$. While $L_1$ is shown to be lying along the $y$ axis whereas $L_2$ is tilted at an angle, $h$, with respect to the $x$ axis, about the optical axis, as shown in Fig. 5. A potential optical setup for the decryption of the encrypted watermark is shown in Fig. 6. Here the system is illuminated by coherent light. The inserted dashed box represents the optical setup for the inverse $2D$ NS - $LCT$. The complex image $I_{dsc}(x)$ is obtained by combining the two input complex masks $P1'(u)$ and its $P1(u)$ as per equation (23). These complex input masks can be displayed with help of spatial light modulator (SLM) (Lee et al., 2007). Then the resultant $I_{dsc}(x)$ can be displayed on SLM which is further descrambled by inverse 4D hyperchaotic system with help of PC and the final retrieved image can be recorded on CCD.

The Fig. 7 below shows the schematic flowchart of the watermark extraction process of the proposed watermarking scheme.

Here $E_w$ is extracted from the watermarked image $I_w(x)$ by

$$E_w = \frac{I_w(x) - I_h(x)}{\beta}$$

(21)

From $E_w$, private key $P1(u)$ and public keys $\alpha_1$ and $\beta_1, P1'(u)$ can be obtained using

$$P1'(u) = \frac{abs(P1(u))\sin \alpha_1}{\sin \beta_1} E_w$$

(22)

$I_{dsc}(x)$ is obtained by taking inverse $2D$ NS-$LCT$

$$I_{dsc}(x) = 2D \text{NS} - LCT^{-1} \left\{ (P1'(u)) + P1(u), \text{RPM}_2^* \right\}$$

(23)

Applying inverse 4D hyperchaotic process on $I_{dsc}(x)$ gives watermark image $I_r(x)$

$$I_r(x) = 4D\text{chao}^{-1}(I_{dsc}(x))$$

(24)

**Results and Discussions**

Computer based simulations are performed on MATLAB 9.3 platform to check the validity and performance of the proposed watermarking mechanism. Simulations are carried out on the grayscale pictures of ‘Lena’ and ‘Peppers. Figure 8 shows scheme validation results, wherein Figs. 8 (a)-(p) are (a) watermark image $I(x)$; (b) scrambled image $I_{sc}(x)$; (c) random phase mask $\text{RPM}_1$; (d) random phase mask $\text{RPM}_2$; (e) $2D$ NS-$LCT$\{ $\sqrt{I_{sc}(x)} \times \text{RPM}_1$\} (f) $I_{sc}(u) \times \text{RPM}_1^*$ (g) $A(u)$; (h) $\varphi(u)$; (i) $\alpha_1$; (j) $\beta_1$; (k) $P_1(u)$; (l) $P_1'(u)$; (m) $E_w$; (n) $I_h(x)$; (o) $I_w(x)$ and (p) $I_r(x)$ respectively. For generating permutation keystream (Fu et al., 2018) from 4D chaotic system the parameters $a = 36$, $b = 3$, $c = 20$ and $d = 1.1$ with initial conditions of $x = 4.1437594350718$, $y = 5.3052357062825$, $z = 26.36372354340482$ and $u = 28.5802537020945$ have been used. The $2D$ NS - $LCT$ matrix $M$ used in the proposed scheme is given by

$$M = \begin{bmatrix} 8 & 9 & 1 & 0.5 \\ 10 & -3 & 0.5 & 0.5 \\ 122 & -58 & 5 & 6 \\ -26 & 164 & 7 & 0 \end{bmatrix}$$

(25)

Fig. 7: Schematic flowchart of the watermark extraction
The proposed watermarking scheme effectively hides the normalized encrypted input watermark image in the host image. Ciphertext of the input watermark image produced is quite similar to white stationary noise, though input watermark image can be extracted effectively utilizing the right estimations of 4D chaotic parameters \((a, b, c, d)\) and initial conditions of \((x, y, z, u)\); along with all public keys \(RPM_1, RPM_2\) and other private keys that is ten independent variables of matrix \(M, P1(u)\) and attenuation parameter \(\beta\). Here parameters and initial conditions of 4D hyperchaotic framework are also taken as private keys as entire permutation depends on them. In this way, they give additional security to encoded watermark image along with diminishing the correlation amongst pixels by scrambling them at global level.

Figures 9(a)-(d) below are the recovered watermark images with wrong values of 4D hyperchaotic parameters and initial conditions that is by taking \(a = 36.1\) instead of 36; \(b = 3.1\) instead of 3; \(c = 20.1\) instead of 20; \(d = 1.11\) instead of 1.1; \(x(1) = 4.1437594350717\) instead of \(4.143759435071\); \(y(1) = 5.3052357062824\) instead of \(5.3052357062825\); \(z(1) = 26.36372354340481\) instead of \(26.36372354340482\) and \(u(1) = -28.5802537020944\) instead of \(-28.5802537020945\) respectively.

So, on analysing the results obtained above, the watermark image can be recovered successfully only after using all correct values of public keys, private keys: hyperchaotic parameters and initial conditions and elements of matrix \(M\).
An Asymmetric Hybrid Watermarking Mechanism

\[ \sum_{i=1}^{H} \sum_{j=1}^{W} \left( I(i,j) - I_r(i,j) \right) \]
\[ CC = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} I_r(i,j) - I(i,j)}{\sqrt{\sum_{i=1}^{H} \sum_{j=1}^{W} (I(i,j) - I(i,j))^2}} \]  
\[ \text{MSE}(I(i,j), I_r(i,j)) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (I(i,j) - I_r(i,j))^2 \]  
\[ \text{SSIM}(I, I_r) = \frac{2 \mu_I \mu_{I_r} + C_1}{\mu_I^2 + \mu_{I_r}^2 + C_1} \frac{2 \sigma_I \sigma_{I_r} + C_2}{\sigma_I^2 + \sigma_{I_r}^2 + C_2} \]  

Here \( I(i,j) \) and \( I_r(i,j) \) represent input watermark image and recovered watermark image of size \( H \times W \) respectively. \( \bar{I}(i,j) \) is the mean value of the input image computed by using equation (29) below:

\[ \bar{I}(i,j) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} I(i,j) \]  

Similarly, the mean of recovered image \( I_r(i,j) \) can be obtained.

Statistical Analysis

Statistical analysis comprises of histogram analysis, 3D plots, Information entropy and correlation distribution of input watermark image, scrambled image and encrypted watermark image has been carried out. The sensitivity of scheme against attenuation parameter has also been investigated in detail.

Histogram Analysis

Figure 12 shows the histogram analysis of the encryption process employed in the proposed watermarking scheme. Figure 11(a-c) shows the histogram plots of the input watermark image, encrypted image \( I_e(x) \) and extracted watermark image \( I_e(x) \) at the receiver end respectively. Moreover, it is very evident that histogram of the encoded image has great resemblance to that of white noise as it distributes all pixels over the complete range. Furthermore, even after that encrypted watermark image has been
recovered successfully with similar pixel distribution with value of \( CC = 1 \) and \( SSIM = 1 \).

### 3D Plot Analysis

Figure 13(a-d) displays 3D plots which demonstrate the image pixel intensity distribution of \( I(x) \); \( I_{sc}(x) \); \( I_e(x) = P_1(u) \mod 255 \), and \( I_r(x) \) respectively. It is clear from the figure that scrambled image \( I_{sc}(x) \) and encrypted watermark image \( I_e(x) \) do not have any correlation amongst their pixels and they are disseminated well in space. Table 1 below shows the \( CC \) and \( SSIM \) values obtained between \( I(x) \), \( I_{sc}(x) \) and \( I_e(x) \) respectively.

The \( CC \) and \( SSIM \) values clearly demonstrate the effectiveness and strength of the encryption process. Encryption scheme successfully encodes the watermark into an uncorrelated ciphertext. Though with correct keys watermark image can be recovered with value of \( CC \) and \( SSIM \) being unity.

### Correlation Distribution Analysis

Effectiveness of an encryption process can also be demonstrated through correlation distribution analysis. We have plotted randomly selected 1000 sets of adjacent pixels from the input watermark image, 4D chaotic scrambled image and encrypted watermark image in horizontal, diagonal and vertical directions. Figure 14 (a,d,g) shows that input image’s adjacent pixels have high correlation in all the three directions, whereas, Figure 14 (b,e,h) shows no recognizable connection in the adjacent pixels of the 4D chaotic scrambled image in horizontal, diagonal and vertical directions respectively. Figure 14(c,f,i) shows that correlation of the adjacent pixels of encrypted watermark image is extremely poor and pixels are distributed randomly in both the dimensions in all directions.

### Information Entropy

Information entropy is basically used for statistically measuring the level of arbitrariness or randomness in an image, which later is utilized to display image texture. Information entropy \( H(m) \) of source \( m \) is defined as

\[
H(m) = \sum_{k=1}^{256} P(m_k) \log_2 \frac{1}{P(m_k)}
\]  

Here \( P(m_k) \) refers to the probability of \( m_k \). Value of entropy for a grayscale image lies in the range of 0 to 8. The entropy of input watermark grayscale image of Lena has a value of 7.3523 whereas the entropy of encrypted watermark image is 7.9955.

### Sensitivity of Attenuation factor

Figure 15 shows \( CC \), \( MSE \) and \( SSIM \) plots between original and extracted watermark for different values

---

**Table 1: \( CC \) and \( SSIM \) values between \( I(x), I_{sc}(x) \) and \( I_e(x) \) respectively**

<table>
<thead>
<tr>
<th></th>
<th>( I(x) )</th>
<th>( I_{sc}(x) )</th>
<th>( I_e(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( CC )</td>
<td>0.0118</td>
<td>-0.0013</td>
<td></td>
</tr>
<tr>
<td>( SSIM )</td>
<td>0.00093349</td>
<td>0.00024384</td>
<td></td>
</tr>
</tbody>
</table>
of $\beta$ respectively. It shows that $CC=1$, $MSE$ is almost zero, and $SSIM=1$ only at correct value of $\beta=0.6$. At other points $MSE$ has very high value of order $10^4$ whereas $CC$ and $SSIM$ are almost zero. This implies that watermark can only be extracted only at a particular value of attenuation factor $\beta$ elsewhere the extracted watermark does not convey any information. This illustrates that the proposed scheme is highly sensitive to the attenuation factor $\beta$. 

Fig. 13: 3D-plots of (a) $I(x)$; (b) $I_{SC}(x)$ (c) $I_{w}(x)$and (d) $I_{r}(x)$

Fig. 14: Correlation distribution of the input image $I(x)$ (a,d,g), scrambled image $I_{sc}(x)$ (b,e,h) and encrypted image $I_{c}(x)$ (c,f,i) in horizontal, diagonal and vertical directions respectively

Attack Analysis

In attack analysis, scheme has been tested against various attacks such as brute force attack, occlusion attack and iterative transform based special attacks.

Brute Force Attack

The proposed watermarking scheme can successfully resists brute force attack as it has very large key space: two random masks (of size 256×256), four hyper chaotic parameters, four initial conditions of hyper chaotic system, ten independent parameters of two-dimensional non-separable linear canonical transform 2D NS-LCT, attenuation parameter $\beta$ and private key $P_1(u)$. The entire key space is approximately $10^{32} \times 10^8 \times 10^{40} \times 10^{30} \times 10^{16} = 10^{130}$ which is large enough to resist any brute force attack. And as per results shown above too, watermark image cannot be extracted successfully even if any of the key or parameter is found missing.

Occlusion Attack

In real time scenario, the information of the watermarked image may be lost partially or completely because of any unavoidable circumstances such as network errors or failures. So, proposed watermarking scheme needs to be evaluated for such contamination also. Figure 16 (a-c) shows the occluded watermarked images and their corresponding recovered images without filtering, with application of min filter alone and on applying median filter to output of min filtered images for Lena for 10%, 30% and 50%, occlusions respectively. The occluded pixels are replaced here by zero values. Actually, on occlusion the extracted watermark gets corrupted with white noise and thus degrades, so it needs to be processed to get any meaningful information from it. And results obtained show remarkable improvement in the image. And figure 17 shows the $CC$ curve against percentage of occlusion for extracted watermark image, its corresponding min filtered output, and output of min filtered images passed through median filter respectively. It is very clear from the figure that with combination of min and median filtering $CC$ is enhanced remarkably. It is almost 90% up to 70% occlusion.

Special Attack Analyses

The proposed watermarking scheme encrypts watermark image using 4D chaotic scrambling process and single level random decomposition in two-dimensional non-separable linear canonical transform 2D NS-LCT domain and it is also tested against special attacks. Here in this paper hyper chaotic parameters and initial conditions serve as additional keys. And the two-dimensional non-separable linear canonical transform 2D NS-LCT strengthens the encryption process as it has ten independent parameters which extend the key-space of the proposed scheme. Here as normalized encrypted watermark is inserted in the host image as explained in the above sections. The attacker just has information of phase part of $P_1(u)$ and does not have any clue about its amplitude so...
without the correct knowledge of the private key $P1(u)$ he won’t be able to even initialize special attack on the encrypted watermark image. Moreover, to extract the watermark image all public and private keys are required. Here special attack has been carried for the worst-case scenario that attacker has all the keys (which is hypothetical assumption) except $P1(u)$. Figure 18 shows special attack results on the proposed scheme, as is clear from the figure that $CC$ and $SSIM$ of the extracted watermark image is very low and almost zero even after 100 iterations. Even $MSE$ between original and extracted watermark images is of the order $10^4$ after 100 iterations, so, the designed scheme can successfully resist special attack even with single level decomposition. And hyper chaotic system and 2D NS-LCT further strengthens the scheme.
Conclusions

In this paper, an asymmetric optical cryptosystem based on 4D hyperchaotic system and single level random decomposition in two-dimensional non separable linear canonical transform 2D NS-LCT domain is proposed. 4D hyperchaotic system is used for generating permutation sequence for pixel swapping mechanism employed on the input image to scramble it. The independent parameters of the 2D NS-LCT matrix serve as extra keys to oppose any brute-force attack. Here one level of random decompositions is used. The masks generated by random decomposition don’t have equal moduli unlike equal modulus decomposition process; and one of the mask acts as private key while amplitude truncated version of the other acts as ciphertext, so ciphertext does not convey any information regarding private key thus limits the available constraints to break the encoded image through iterative transform-based attacks. Hyperchaotic parameters and initial conditions also extend the key space thus provide more security to the watermarking mechanism. MATLAB simulations have verified the validity of the proposed system. It has great performance against brute force, occlusion and special attack. Alongside this it holds the benefit of key management and non-linear characteristics of asymmetric optical cryptosystems.

References

Barfungpa S P and Abuturab M R (2016) Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum Optical and Quantum Electronics 48 520
Chen W, Chen X and Sheppard C J R (2010) Optical image encryption based on diffractive imaging Optics Letters 35 3817-3819
Chen H, Tanougast C, Liu Z and Sieler L (2017) Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains Optics and Lasers in Engineering 93 1-8
Chen L and Zhao D (2006) Optical image encryption with Hartley transforms Optics Letters 31 3438-3440
Chen J-X, Zhu Z-L, Fu C, Zhang L-B and Zhang Y (2014) Cryptanalysis and improvement of an optical image...
An Asymmetric Hybrid Watermarking Mechanism


Li J (2014) An optimized watermarking scheme using an encrypted gyrotor transform computer generated hologram based on particle swarm optimization Optics Express 22 10002-10016


Liu S, Mi Q and Zhu B (2001) Optical image encryption with multistage and multichannel fractional Fourier-domain
filtering *Optics Letters* 26 1242-1244

Mehra I and Nishchal N K (2015) Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging *Optics and Lasers in Engineering* 68 74-82

Mendlovic D and Konforti N (1993) Optical realization of the wavelet transform for two-dimensional objects *Applied Optics* 32 6542-6546


Refregier P and Javidi B (1995) Optical image encryption based on input plane and Fourier plane random encoding *Optics Letters* 20 767-769


Sheng Y, Xin Z, Alam M S, Xi L and Xiao-feng L (2009) Information hiding based on double random-phase encoding and public-key cryptography *Optics Express* 17 3270-3284


Starchenko A P (2011) Using the discrete cosine transformation to construct a hologram for the task of embedding hidden watermarks *Journal of Optical Technology* 78 176-179


