Optical color image hiding scheme based on chaotic mapping and Hartley transform

Zhengjun Liao\textsuperscript{a,b,c,*}, Yu Zhang\textsuperscript{a, **}, Wei Liu\textsuperscript{d}, Fanyi Meng\textsuperscript{c}, Qun Wu\textsuperscript{c}, Shutian Liu\textsuperscript{d}

\begin{itemize}
\item \textsuperscript{a} Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China
\item \textsuperscript{b} Department of Physics, Harbin Institute of Technology, Harbin 150001, China
\item \textsuperscript{c} Department of Electronic Science and Technology, Harbin Institute of Technology, Harbin 150001, China
\item \textsuperscript{d} Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China
\item \textsuperscript{*} State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
\end{itemize}

\textbf{A R T I C L E  I N F O}

\textbf{A B S T R A C T}

We present a color image encryption algorithm by using chaotic mapping and Hartley transform. The three components of color image are scrambled by Baker mapping. The coordinates composed of the scrambled monochrome components are converted from Cartesian coordinates to spherical coordinates. The data of azimuth angle is normalized and regarded as the key. The data of radii and zenith angle are encoded under the help of optical Hartley transform with scrambled key. An electro-optical encryption structure is designed. The final encrypted image is constituted by two selected color components of output in real number domain.

\section{Introduction}

Information security of color image has been considered based on the encryption algorithms of gray-level image, such as random phase encoding \cite{1}, digital holography \cite{2} and coherent diffractive imaging \cite{3}. The encryption schemes of one or two color images \cite{4–7} have been designed by using double random phase encoding \cite{8,9}. Three kinds of optical color encryption approaches have been reported by using interference technique with Arnold transform \cite{10–12}. A color image encryption method has been represented by use of the rotation of color vectors in Hartley domains \cite{13}. Combining the Arnold transform and color-blend operations, a color image encryption method has been proposed \cite{14}. A dynamical color encryption algorithm has been represented by hiding the information from the three components \cite{15}. The multi-color visual cryptograph has been introduced for information security \cite{16}. The Hartley transform has been applied in color image encryption with random phase encoding or other transforms \cite{17–20}. In most of these color encryption schemes mentioned above, the three components of color image are separated to be hidden as three gray-level images. The final encrypted image is encoded into a color image with RGB components in complex number domain or real number domain. In addition, triple- or multiple-image encryption methods \cite{21–24} can serve as a potential method encoding color image, in which the encrypted image; however, is gray-level.

In this paper, an optical color image algorithm is developed by employing chaotic mapping and Hartley transform. The three components of color secret image are randomized by Baker mapping, which is a scrambling operation \cite{25–29}, and are transformed into the spherical coordinates. The data of normalized azimuth angle, which is random, is extracted and regarded as key. Two functions are defined by radii and zenith angle. Subsequently the two functions are scrambled by chaotic mapping and Hartley transform. The two functions are encoded into two components of the final encrypted color image, where another component has no information and is replaced with 0, in real number domain. An optical system is given to implement the encryption algorithm. Some numerical results have been shown for demonstrating the performance of the proposed encryption scheme.

\section{Color encryption algorithm}

A color image $I_0(x,y)$ is decomposed as a vector as follows:

$$I_0(x,y) = [R_0(x,y), G_0(x,y), B_0(x,y)].$$

where $R_0$, $G_0$ and $B_0$ are RGB components. Baker mapping \cite{29} is
introduced for pixel scrambled and is defined as:
\[ y' = \frac{N}{n_j}(y - N_j) + \text{mod} \left( x, \frac{N}{n_j} \right), \]
\[ x' = \frac{n_j}{N} \left[ x - \text{mod} \left( x, \frac{N}{n_j} \right) \right] + N_j, \]
\[ 0 \leq x, y < N, \sum_{j=1}^{N} n_j = N, N_j = n_1 + \cdots + n_j, N = 0, \]
(2)

where \((x, y)\) and \((x', y')\) are pixel position in discrete case before and after the mapping, respectively. The parameter \(N\) represents the size of the squared image. The sequence \(n_j\) is the main parameters of Baker mapping. Here a limiting condition is that the value of \(N/n_j\) is integer. A pixel scrambling relation is expressed as
\[ R_0(x, y) = \mathbb{R}(x, y) - m, \]
\[ G_0(x, y) = \mathbb{R}(G_0(x, y)) - m, \]
\[ B_0(x, y) = \mathbb{R}(B_0(x, y)) - m, \]
(3)

where the symbol \(\mathbb{R}\) is Baker mapping operator, in which different parameters \(n_j\) are used for randomizing the three components and \([i_1, i_2, i_3]\) are the total iterative number of the mapping. The parameter \(m\) is an expected mean value and is fixed at 128 for 8-bit image in this paper. The scrambled components \([R_0, G_0, B_0]\) are considered for expressing the points in Cartesian coordinates and are converted into spherical coordinates as follows:
\[ r(x, y) = \sqrt{R_0^2(x, y) + G_0^2(x, y) + B_0^2(x, y)}, \]
\[ \theta(x, y) = \arctan(2G_0(x, y), R_0(x, y)), \]
\[ \phi(x, y) = \arccos(B_0(x, y)/r(x, y)), \]
(4)

where the function \(\arctan2\) is to compute four quadrant inverse tangent. The azimuth angle \(\theta\) is normalized by:
\[ K(x, y) = \frac{\theta(x, y)}{2\pi}, \]
(5)

where the function \(K(x, y)\) serves as the main key of this encryption algorithm. Two functions \(i_1\) and \(i_2\) are given as:
\[ i_1(x, y) = r(x, y)\cos(\phi(x, y)), i_2(x, y) = r(x, y)\sin(\phi(x, y)) \]
(6)

A random data \(K^p(x, y)\) is generated by logistic mapping \([30,31]\) and Baker mapping as
\[ T(x, y) = x \times K^{p-i+1}(x, y) \mid 1 - K^{p-1}(x, y) \]
\[ K^p(x, y) = B_{p,m}[T(x, y)], \]
(7)

where \(p = 1, \ldots, p_1, K^{p_0}(x, y) = K(x, y)\). The coefficient \(x\) is the parameter of logistic map and is limited in the range \([3.57, 3.82]\). The \(i_1\) and \(i_2\) are encoded by an affine transform as:
\[ \begin{bmatrix} i_1' \\ i_2' \end{bmatrix} = \begin{bmatrix} 1 + c_1 \cos \beta & 0 \\ 0 & -1 + c_2 \sin \beta \end{bmatrix} \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix} \begin{bmatrix} i_1(1 + c_1 \cos \beta) \\ i_2(1 + c_1 \cos \beta) \end{bmatrix}, \]
(8)

where \(\beta = 2\pi K^{p-1}(x, y)\). The functions \(i_1'(x, y)\) and \(i_2'(x, y)\) are output. The parameters \(c_1\) and \(c_2\) are constant and are located in the interval \((0, 1)\).

Hartley transform is introduced for changing the data of the functions \(i_1'(x, y)\) and \(i_2'(x, y)\). The transform \([32,33]\) is expressed as:
\[ H(u, v) = \mathbb{H}[h(x, y)](u, v) = \int h(x, y) \cos(2\pi xu + 2\pi vy) dx dy = \text{Re}[\mathcal{F}[h(x, y)](u, v)] + \text{Im}[\mathcal{F}[h(x, y)](u, v)], \]
(9)

where \(h\) and \(H\) are the input and output of Hartley transform. The operators \(\mathbb{H}\) and \(\mathcal{F}\) are Hartley transform and Fourier transform, respectively. The function \(\cos(\ldots)\) is equal to \(\cos(\ldots) + \sin(\ldots)\). Optical Hartley transform is in real number domain. By using Hartley transform, \(i_1'(x, y)\) and \(i_2'(x, y)\) are altered as follows:
\[ I_1(u, v) = \mathbb{H}[I_1'(x, y)](u, v), I_2(u, v) = \mathbb{H}[I_2'(x, y)](u, v). \]
(10)

To enhance the security of encryption algorithm, Eqs. (7), (8) and (10) will be performed three or more times. During the iteration, some parameters in chaotic mapping can be taken at different values. The two encoded functions will be regarded as

---

**Table 1**
The parameters of Baker mapping.

<table>
<thead>
<tr>
<th>(n_j)</th>
<th>(k)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i_1)</td>
<td>(i_2)</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>32</td>
</tr>
</tbody>
</table>
the red component and green component of color encrypted image. Here blue component is absent, which is different with the color encryption algorithms [1–7]. Thereby, the storage space of encrypted image is lower in application.

An optical system is considered for implementing the encryption and is displayed in Fig. 1. A tunable laser is employed for generating red beam and green beam. Under the help of computer and spatial light modulator (SLM), the two images in Eq. (10), \( i_0^1 \) and \( i_0^2 \) being a filtering are encoded by red light and green light, respectively. Moreover the two functions are coupled by Eq. (8). The red or blue laser beam is split into two parts for illustrating the Fourier transform system and serving as a reference beam. The cube corner prism (CCP) can combine the real part and imaginary part of Fourier transform spectrum [32]. The in-line holography is utilized for recording the phase distribution, which is binary data, namely 0 and \( \pi \). The setup can also be employed for image decryption due to that inverse Hartley transform is itself. The chaotic mapping and coordinate change in decryption process can be achieved in computer.

3. Numerical results

The color 8-bit image ‘Lena’ having 256 \( \times \) 256 pixels is employed in our numerical simulation and is given in Fig. 2(a). The parameters in Baker mapping are listed in Table 1, where the symbol ‘/’ represents that the corresponding data is empty. The parameter \( n_i \) in the operation \( \beta_{j-n_i} \), which is a set of data in the third row at Table 1, is also employed for generating the function \( K(x,y) \). In the logistic mapping, the coefficient \( x \) is fixed at 3.7. The parameter \( p_1 \) in Eq. (7) equals to 12, 10 and 18 in the three times of encoding operations during the encryption process. The parameters of affine transform \( c_1 \) and \( c_2 \) are taken at 0.8 and 0.6, respectively. An encrypted image is shown in Fig. 2(b), which is a random yellow pattern with red noise and green noise, because the blue component is equal to 0. The distribution of the key \( K \) is shown in Fig. 2(c), which is a random pattern. When all keys are selected at right values, the decrypted image is obtained and displayed in Fig. 2(d).

Here the statistical property of original image and cipher image is test by correlation coefficient (CC), which is defined as follows:

\[
E(x_k) = \overline{x_k}, \\
D(x_k) = \overline{(x_k - E(x_k))^2}, \\
\text{cov}(x_k,y_k) = \overline{(x_k - E(x_k))(y_k - E(y_k))}, \\
\text{corr}(x_k,y_k) = \frac{\text{cov}(x_k,y_k)}{\sqrt{D(x_k)D(y_k)}}. \\
\]

where the overline is to compute average. The symbol ‘corr’ is correlation coefficient function. Two horizontally adjacent pixels of color image [34] is considered for presenting the statistical characters. The 500 pairs of points are selected randomly. The data of encrypted image is converted into the integer in the range [0, 255] linearily, in which the extreme value in Hartley spectrum is replaced with 0. The distribution of pixel values is shown in Fig. 3. The corresponding correlation coefficient values are listed in Table 2, where the parameter values of original image and encrypted image are close to 1 and 0, respectively.

In this color encryption algorithm, the function \( K \) is main key. When a half of data of the key \( K \) is known by attacker, a test is performed. The unknown data of the key \( K \) is replaced with random number or 0.5. The unknown data is located at right side shown as Fig. 4(a). In image decryption other parameters are selected at right values. The recovered images are calculated and illustrated in Fig. 4(b) and (c). Therefore the original secret image is safe for the decryption with a half of correct data of key \( K \).

![Fig. 3. Distribution of two horizontally adjacent pixels of color image: (a), (b) and (c) are the red, blue and green components of original image, (d) and (e) are the red and blue components of cipher image.](image-url)
Furthermore, the sensitivity of key $K$ is proportional to the total iterative number of affine transform and Hartley transform. The parameter $a$ in the logistic mapping can be regarded as an additional key. When $a$ is limited in the range $[3.695, 3.705]$, three mean square error (MSE) curves from the RGB components are calculated and given in Fig. 5. Here the data of key $K$ and the parameters of Baker mapping are adopted at correct values. By using $a = 3.7002$, a retrieved image is shown in Fig. 5(d), which is random pattern. Thereby, the effective interval of extra key $a$ is less than $2 \times 10^{-4}$. The key space is $[3.82 - 3.57] = 1250^K$ from $a$. If the value of the parameter $p_1$, which is the total number of iteration of Eq. (7), is increased, the sensitivity of key $a$ is enhanced. When the parameters $n_i$ and $j_k$ of Barker mapping, two examples are computed and shown in Fig. 6, from which original image cannot be recognized in vision. In this paper, the parameters of Barker mapping are utilized for both generating key and being regarded as an extra key.

The test of occlusion and noise attacks are performed and shown in Fig. 7. In decryption, correct keys are employed. Here the center $64 \times 64$ pixels are cut off and are replaced with 0 in calculation. The recovered image is illustrated in Fig. 7, from which the basic outline of original image can be recognized. The Gaussian noise has then mean value 0 and standard deviation 10. The noise density of salt & pepper is 0.01. The corresponding retrieved images are shown in Fig. 7(c) and (d).
The known-plaintext attack (KPA) [35] and chosen-plaintext attack (CPA) [36] are two kinds of classical tests for analysis of security. Here the double random phase encoding in Fourier transform domain is introduced for the attacks. Fig. 8(a) and (b) are original images having 128 \times 128 pixels. In calculation, Fig. 8(a) and its encrypted images are utilized for obtaining key in KPA and CPA. The iterative phase retrieval algorithm is performed 600 times. The corresponding recovered images are shown in Fig. 8(c) and (d), which are random pattern.

4. Conclusion

We have proposed a color image encryption approach by use of chaotic mapping and Hartley transform. The three components of color image are first scrambled by Baker mapping. The scrambled components are regarded as the positions in Cartesian coordinates and are converted into spherical coordinates. The data of azimuth angle is separated and normalized for serving as main key of this encryption scheme. The data of radius and zenith angle are coupled into two functions. Subsequently the chaotic mapping and Hartley transform are introduced for hiding the two functions. Finally the two encrypted functions are encoded into the red component and blue component of output image in real number domain. An optical system is suggested in order to perform the encryption algorithm. Some numerical results have been represented for validating the performance and security of the proposed color encryption scheme.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grants 11104049, 10974039, 61077075 and 11047153), Specialized Research Fund for the Doctoral Program of Higher education (Grant 20102302120009), the Fundamental Research Funds for the Central Universities (Grant HIT.NSRIF.2009038), the Program for New Century Excellent Talents in University (NCET-12–0148), the Opening Foundations by the State Key Laboratory of Transient Optics and Photonics, Chinese Academy of Sciences (Grant SKLST201105), the State Key Laboratory of Advanced Optical Communication Systems Networks, and State Key Laboratory of Information Security Institute of Information Engineering, Chinese Academy of Sciences, China. The authors wish to thank the anonymous reviewer for the useful comments and suggestions.

References