Security of RGB image data by affine hill cipher over $SL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ domains with Arnold transform

D.C. Mishra a,*, R.K. Sharma a, Rakesh Ranjan b, M. Hanmandlu b

a Department of Mathematics, Indian Institute of Technology, Delhi, Hauz Khas 110016, New Delhi, India
b Department of Electrical Engineering, Indian Institute of Technology, Delhi, Hauz Khas 110016, New Delhi, India

A R T I C L E   I N F O
Article history:
Received 23 June 2014
Accepted 20 July 2015

Keywords:
RGB image encryption
RGB image decryption
Cryptography
Arnold transform
Affine hill cipher

A B S T R A C T
These days, security of sensitive information is a major concern. Cryptography allows transmission of data from one end to the other, both, securely and secretly. Here we have designed a novel cryptosystem for security of RGB images by affine hill cipher (AHC) over $SL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ domains with Arnold transform (AT). The security of color images is designed by the existing techniques with the help of keys only, but proposed cryptosystem provides security of RGB image data on the basis of the keys and the arrangement of AHC parameters. Additionally, key multiplication side (pre or post) with a RGB image data is also inevitable to know, to correctly decrypt the encrypted image data. In this approach, we have considered multiplicative keys of affine hill cipher from $SL_n(\mathbb{F}_q)$ domain and additive keys of affine hill cipher from $M_n(\mathbb{F}_q)$ domain, which provides exorbitant key space for the proposed cryptosystem. Experimental results and security analysis of the cryptosystem are given to the justification for the stalwartness of the proposed cryptosystem. This method would have large potential usage in digital RGB image processing and security.

© 2015 Elsevier GmbH. All rights reserved.

1. Introduction

Cryptographic systems are used extensively to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way that it is understood only at the receiver end. The original image data is the plaintext [1,2], which must be kept secure. This is encrypted into the ciphertext (encrypted image data), which is then transmitted through unsecured network. The procedure of secure transmission of RGB image data as well as the keys through insecure network is given in Fig. 1. At the receiver end, transmitted data is decrypted back into the plaintext. The aim of cryptography is to ensure high end communication between the sender and receiver without any loss of information. Security, refers to the following aspects: confidentiality, data integrity, authentication and non-repudiation. Cryptanalysts try to break the security of data, and this process is known as hacking. There are several techniques by which image data may be encrypted and decrypted. But the security of color images by the proposed cryptosystem is developed by affine hill cipher over $SL_n(\mathbb{F}_q)$ [3] and $M_n(\mathbb{F}_q)$ domains with Arnold transform. The technique [4] provides security of RGB images by two stage random matrix affine cipher (RMAC) associated with discrete wavelet transform for each component of RGB image data. The security of the approach [4] is based on the keys and the arrangement of RMAC parameters. But in the proposed cryptosystem, the security of color images developed by each channel of color image with two phase affine hill cipher (TPAHC) over $SL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ domains and Arnold transformation (AT), which is designed to ensure secure transmission of color image data. Here, we have considered the highly sensitive parameters like keys, arrangement of AHC parameters, and position (pre or post) of key multiplication with image data for security of RGB image data. Various schemes have been developed for security of image data; such as [5–8] which provide image encryption and decryption using, Fourier transformation; [9–11] deal with security of image data by using gyrator transform domain combined with some other techniques; [14–16] have presented image coding using wavelet transform; [17–19] are concerned with security of image data. Now, scheme [20] is designed for the security of grayscale-image by random hill cipher with discrete wavelet transform. However, according to, recent studies for the security of RGB images, some attacks such as: brute-force attack, cropping attack, noise attack, etc. can penetrate the security (robustness) of the cryptosystem. The proposed cryptosystem is free from such types of attacks.

http://dx.doi.org/10.1016/j.opticon.2015.07.117
0030-4026/© 2015 Elsevier GmbH. All rights reserved.
2. Affine hill cipher and Arnold transform

In the proposed cryptosystem, we have designed the security of RGB images of size \( m \times m \) by affine hill cipher (AHC) and Arnold transform (AT). The matrix of each channel of RGB image of size \( m \times m \) is divided into equal blocks of size \( n \times n \) such that \( n|m \), we call it as block matrix (sub image), the size of the sub image is the same as the size of the key of affine hill cipher, which is defined by the user. In proposed cryptosystem, the multiplicative keys of affine hill cipher are chosen from \( SL_n(\mathbb{F}_q) \) domain and additive keys, chosen from \( M_n(\mathbb{F}_q) \) domain, such that \( n \) divides \( m \). Suppose the user chooses a type of block matrix (sub image), in which the order of block matrix does not divide order of original image matrix \( (n|m) \), then user needs to add some redundant rows or columns or both in the original image matrix. The procedure for block creation of RGB image data is illustrated in Fig. 2. \( SL_n(\mathbb{F}_q) \) is the set of all \( n \times n \) matrices that contains those elements of \( GL_n(\mathbb{F}_q) \) whose determinant is 1 over field \( \mathbb{F}_q \). The mathematical formulation of \( SL_n(\mathbb{F}_q) \) is as follows:

\[
SL_n(\mathbb{F}_q) = \{ A \in GL_n(\mathbb{F}_q) | \det(A) = 1 \},
\]

where \( GL_n(\mathbb{F}_q) \) is general linear group over domain \( \mathbb{F}_q \). Because \( SL_n(\mathbb{F}_q) \) contains those elements from \( GL_n(\mathbb{F}_q) \), whose determinant is equal to 1, for large size of \( n \) the order of \( SL_n(\mathbb{F}_q) \) is very large. If \( \mathbb{F}_q \) is containing \( q \) elements then

\[
|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{|GL_n(\mathbb{F}_q)/SL_n(\mathbb{F}_q)|} = \frac{|GL_n(\mathbb{F}_q)|}{|SL_n(\mathbb{F}_q)|} = \frac{|GL_n(\mathbb{F}_q)|}{q - 1},
\]

where \( H = \sum_{j=1}^{n-1} j = \left( \frac{n}{2} \right) \) and \( \mathbb{F}_q \) be a finite field containing \( q \) elements, where \( q \) is a large prime number. Since determinant of every element of \( SL_n(\mathbb{F}_q) \) is 1, then the inverse of hill cipher keys \( (K^{-1}) \) is equal to adjoint of hill cipher keys \( (adj(K)) \), because \( K^{-1} = \frac{adj(K)}{det(K)} \). Now, mathematical formulation of \( M_n(\mathbb{F}_q) \) is given as

\[
M_n(\mathbb{F}_q) = \{ A = [a_{ij}]_{n \times n} | a_{ij} \in \mathbb{F}_q \}.
\]

Formulation of affine hill cipher (AHC) for a block matrix (sub image) of size \( n \times n \) is given as:

\[
E_{n \times n} = B_{n \times n} \cdot K_{n \times n} + C_{n \times n} \mod 256,
\]

where \( B_{n \times n} \) is a block matrix (sub image) of a color image such that \( 1 \leq n \leq m \), \( K_{n \times n} \) is a key matrix from \( SL_n(\mathbb{F}_q) \) domain, \( C_{n \times n} \) be an

1.1. Organization of the paper

Section 2 discusses about the proposed affine hill cipher (AHC) and Arnold transform (AT). The mathematical formulation of the affine hill cipher (AHC) and the Arnold transform (AT) for the security of RGB image is given in the same section. In Section 3, we have discussed about the encryption and decryption process of the color image data with affine hill cipher (AHC) and Arnold transform (AT); and we have also talked about the arrangement of AHC parameters and the number of keys used in this approach. Demonstration of the procedure for color image encryption and decryption is mentioned in Section 4. The security analysis and statistical analysis of the proposed cryptosystem is given in Sections 5 and 6, respectively. Comparison of this approach with some existing techniques for color image security is presented in Section 7. Finally, the conclusion of the cryptosystem has been summed up in Section 8.
additive key of affine hill cipher from \( M_n(F_q) \) domain, and \( E_{n \times n} \) be an encrypted block image of size \( n \times n \).

Formulation for inverse affine hill cipher (iAHC) for block matrix (sub image) of size \( n \times n \) is given as:

\[
B_{n \times n} = (E_{n \times n} - C_{n \times n})K^{-1}_{n \times n} \pmod{256},
\]

where \( K^{-1}_{n \times n} \) is the multiplicative inverse of \( K \in SL_n(F_q) \). The same process is applied on the remaining block matrix (sub image) of the original RGB image. Since matrix multiplication is noncommutative, then the position of \( K^{-1} \) with \( E_{n \times n} - C_{n \times n} \) at decryption process, depends on the position of \( K^{-1} \) with \( B_{n \times n} \) in the encryption process. Suppose, if attacker multiplies \( K^{-1}_{n \times n} \) with \( E_{n \times n} - C_{n \times n} \) without knowing the exact position of \( K^{-1}_{n \times n} \) with \( B_{n \times n} \), then original image cannot be recovered.

In this cryptosystem, we have also used discrete Arnold transform or cat map transform [24] to scramble each channel of the RGB image. For the size of \( m \times m \) image, the 2-dimensional Arnold transform (2D-AT) is defined as

\[
\begin{bmatrix}
x' \\
y'
\end{bmatrix} = \begin{bmatrix}
2 & 1 \\
1 & 1
\end{bmatrix} \begin{bmatrix}
x \\
y
\end{bmatrix} \pmod{m}
\]

where \([x, y]^T\) and \([x', y']^T\) represent the position vector of image pixel before and after performing the Arnold transform, respectively.

Now, corresponding to the 2-dimensional inverse Arnold transform (2D-iAT) of Eq. (6) is define as

\[
\begin{bmatrix}
x \\
y
\end{bmatrix} = \begin{bmatrix}
1 & m - 1 \\
m - 1 & 2
\end{bmatrix} \begin{bmatrix}
x' \\
y'
\end{bmatrix} \pmod{m}
\]

The additive inverse of \( a \) with respect to modulo \( m \) is equal to \( m - a \) [25].

3. Encryption and decryption process

In this cryptosystem, we have designed, the security of RGB images by two phase affine hill cipher (TPAHC) over \( SL_n(F_q) \) and \( M_n(F_q) \) domains with Arnold transform (AT). Proposed algorithm is applied on red (R), green (G), and blue (B) channels of an RGB image data in the encryption process. The procedure of encryption algorithm applied on RGB images is represented in Fig. 3, while procedure of decryption for an encrypted RGB image is illustrated in Fig. 4. In the proposed cryptosystem, we have used 12 keys for affine hill cipher and 3 keys for Arnold transform. In the first stage, we have used 6 (3 for multiplicative and 3 for additive) keys for the affine hill cipher, which is applied on an RGB image. Similarly, in the next stage (second stage) 6 keys are also used for the affine hill cipher key. Therefore, the total number of possibilities of the affine hill cipher keys applied on RGB images including both stages is 12! These options (12!) mentioned here form an arrangement of the affine hill cipher parameters, which is called the arrangement of AHC parameters. And 3! options are also available for arrangement of Arnold parameters, which are more sensitive.

The encryption procedure for each component of RGB image data is given in Fig. 3. In the first stage, we apply \( K_1 \) and \( C_1 \) keys \( (K_{1R} \) and \( C_{1R} \) for red, \( K_{1G} \) and \( C_{1G} \) for green, and \( K_{1B} \) and \( C_{1B} \) for blue) for AHC, then Arnold transform (AT) is applied on partially encrypted red (R), green (G), and blue (B) components of RGB image. Now, \( K_2 \) and \( C_2 \) keys \( (K_{2B} \) and \( C_{2B} \) for red, \( K_{2G} \) and \( C_{2G} \) for green, and \( K_{2B} \) and \( C_{2B} \) for blue) are applied on each channel of RGB image data for second stage AHC. The similar procedure is applied for decryption process which is delineated in Fig. 4. In the first stage, we have chosen keys for the inverse affine hill cipher (iAHC) denoted as \( K^{-1}_1 \) and \( C^{-1}_1 \), that is the inverse of second stage keys of the affine hill cipher thereafter, inverse Arnold transform (iAT) is applied on the partially decrypted RGB image. We have applied in the second stage, iAHC with \( K^{-1}_2 \) and \( C^{-1}_2 \) keys, i.e. inverse of first stage keys on the partially decrypted image. Then, finally original image is recovered. The security of the proposed cryptosystem is developed on the basis of 15 keys (12 keys used for AHC and 3 keys for AT). The size of the affine hill cipher keys depends on the size of block matrix (size of sub image), which is the choice of user. The security of the proposed technique not only depends on the keys, but also on the arrangement of AHC parameters and position (pre or post) of keys multiplication with RGB image data, which are highly sensitive. The encrypted and decrypted results are given in Fig. 5.

4. Demonstration of the procedure

We have considered RGB Lena image data of size \( 512 \times 512 \times 3 \) pixels for experimental analysis, which is given in Fig. 5(a). Fig. 5(b) represents, the encrypted RGB image data with the following keys, the affine hill cipher (AHC) keys in the first stage are (before applying AT):
For red (R) component of RGB image:

\[
K_{1R} = \begin{bmatrix} 26 & 3 & 169 & 175 \\ 43 & 5 & 230 & 128 \\ 0 & 0 & 17 & 49 \\ 0 & 0 & 26 & 75 \end{bmatrix}, \quad C_{1R} = \begin{bmatrix} 114 & 172 & 79 & 89 \\ 254 & 180 & 209 & 64 \\ 29 & 84 & 43 & 177 \\ 168 & 229 & 243 & 153 \end{bmatrix},
\]

\[
K_{2R}^{-1} = \begin{bmatrix} 132 & 197 & 68 & 81 \\ 207 & 144 & 21 & 25 \\ 57 & 25 & 0 & 0 \\ 73 & 32 & 0 & 0 \end{bmatrix}, \quad C_{2R} = (-1)\begin{bmatrix} 97 & 143 & 89 & 73 \\ 243 & 33 & 169 & 140 \\ 59 & 48 & 93 & 180 \\ 203 & 178 & 153 & 123 \end{bmatrix},
\]

For green (G) component of RGB image:

\[
K_{1G} = \begin{bmatrix} 79 & 11 & 0 & 0 \\ 43 & 6 & 0 & 0 \\ 189 & 219 & 73 & 57 \\ 111 & 239 & 32 & 25 \end{bmatrix}, \quad C_{1G} = \begin{bmatrix} 87 & 45 & 188 & 221 \\ 199 & 211 & 135 & 47 \\ 98 & 29 & 66 & 153 \\ 209 & 161 & 173 & 44 \end{bmatrix},
\]

\[
K_{2G}^{-1} = \begin{bmatrix} 0 & 0 & 25 & 81 \\ 0 & 0 & 21 & 68 \\ 49 & 17 & 172 & 99 \\ 75 & 26 & 183 & 153 \end{bmatrix}, \quad C_{2G} = (-1)\begin{bmatrix} 168 & 29 & 88 & 193 \\ 49 & 219 & 118 & 41 \\ 159 & 207 & 117 & 44 \\ 68 & 96 & 169 & 143 \end{bmatrix},
\]

For blue (B) component of RGB image:

\[
K_{1B} = \begin{bmatrix} 81 & 25 & 177 & 243 \\ 68 & 21 & 251 & 231 \\ 0 & 0 & 23 & 89 \\ 0 & 0 & 8 & 31 \end{bmatrix}, \quad C_{1B} = \begin{bmatrix} 254 & 219 & 179 & 231 \\ 188 & 201 & 133 & 149 \\ 69 & 33 & 83 & 43 \\ 217 & 205 & 119 & 209 \end{bmatrix},
\]

\[
K_{2B}^{-1} = \begin{bmatrix} 132 & 197 & 68 & 81 \\ 207 & 144 & 21 & 25 \\ 57 & 25 & 0 & 0 \\ 73 & 32 & 0 & 0 \end{bmatrix}, \quad C_{2B} = \begin{bmatrix} 0 & 0 & 25 & 81 \\ 0 & 0 & 21 & 68 \\ 168 & 29 & 88 & 193 \\ 49 & 219 & 118 & 41 \end{bmatrix},
\]

The correctly decrypted RGB image is given in Fig. 5(c) with exact keys and correct arrangement of AHC parameters applied on encrypted image (Fig. 5(b)) at decryption process. The inverse affine hill cipher (iAHC) keys in the first stage are (before applying iAT):

\[
K_{2G}^{-1} = \begin{bmatrix} 17 & 49 & 38 & 92 \\ 26 & 75 & 121 & 49 \\ 0 & 0 & 81 & 25 \\ 0 & 0 & 68 & 21 \end{bmatrix}, \quad C_{2B} = (-1)\begin{bmatrix} 201 & 173 & 133 & 159 \\ 11 & 147 & 30 & 205 \\ 131 & 230 & 176 & 180 \\ 65 & 198 & 86 & 77 \end{bmatrix},
\]

Now, we are applying the inverse affine transform (iAT) to the intermediate decrypted image. The iAHCC keys for second stage are (after applying inverse Arnold transform (iAT)):
For red (R) component:

\[ K_{IR}^{-1} = \begin{bmatrix} 26 & 3 & 169 & 175 \\ 43 & 5 & 230 & 128 \\ 0 & 0 & 17 & 49 \\ 0 & 0 & 26 & 75 \end{bmatrix}^{-1} \]

\[ C_{IR}^{-1} = (-1) \begin{bmatrix} 114 & 172 & 79 & 89 \\ 254 & 180 & 209 & 64 \\ 29 & 84 & 43 & 177 \\ 168 & 229 & 243 & 153 \end{bmatrix} \]

For green (G) component of RGB image:

\[ K_{IG}^{-1} = \begin{bmatrix} 79 & 11 & 0 & 0 \\ 43 & 6 & 0 & 0 \\ 189 & 219 & 73 & 57 \\ 111 & 239 & 32 & 25 \end{bmatrix}^{-1} \]

\[ C_{IG}^{-1} = (-1) \begin{bmatrix} 87 & 45 & 188 & 221 \\ 199 & 211 & 133 & 47 \\ 98 & 29 & 66 & 153 \\ 209 & 161 & 173 & 44 \end{bmatrix} \]

For blue (B) component of RGB image:

\[ K_{IB}^{-1} = \begin{bmatrix} 81 & 25 & 177 & 243 \\ 68 & 21 & 251 & 231 \\ 0 & 0 & 23 & 89 \\ 0 & 0 & 8 & 31 \end{bmatrix}^{-1} \]

\[ C_{IB}^{-1} = (-1) \begin{bmatrix} 254 & 219 & 179 & 231 \\ 188 & 201 & 133 & 149 \\ 69 & 33 & 83 & 43 \\ 217 & 205 & 119 & 209 \end{bmatrix} \]

For green (G) component of RGB image:

\[ K_{IG}^{-1} = \begin{bmatrix} 0 & 0 & 25 & 81 \\ 0 & 0 & 21 & 68 \\ 49 & 17 & 172 & 99 \\ 75 & 26 & 183 & 153 \end{bmatrix}^{-1} \]

\[ C_{IG}^{-1} = (-1) \begin{bmatrix} 254 & 219 & 179 & 231 \\ 188 & 201 & 133 & 149 \\ 69 & 33 & 83 & 43 \\ 217 & 205 & 119 & 209 \end{bmatrix} \]

Now, we are applying the inverse Arnold parameters \( AT_{IR}^{-1} = 5^{-1} \) for red (R) channel, \( AT_{IG}^{-1} = 4^{-1} \) for green (G) channel, and \( AT_{IB}^{-1} = 5^{-1} \) for blue (B) channel of RGB image data at intermediate stage.

The iAHC keys for second stage are (after applying iAT):

For red (R) component:

\[ K_{IR}^{-1} = \begin{bmatrix} 26 & 3 & 169 & 175 \\ 43 & 5 & 230 & 128 \\ 0 & 0 & 17 & 49 \\ 0 & 0 & 26 & 75 \end{bmatrix}^{-1} \]

\[ C_{IR}^{-1} = (-1) \begin{bmatrix} 114 & 172 & 79 & 89 \\ 254 & 180 & 209 & 64 \\ 29 & 84 & 43 & 177 \\ 168 & 229 & 243 & 153 \end{bmatrix} \]

For green (G) component of RGB image:

\[ K_{IG}^{-1} = \begin{bmatrix} 79 & 11 & 0 & 0 \\ 43 & 6 & 0 & 0 \\ 189 & 219 & 73 & 57 \\ 111 & 239 & 32 & 25 \end{bmatrix}^{-1} \]

\[ C_{IG}^{-1} = (-1) \begin{bmatrix} 159 & 207 & 117 & 44 \\ 114 & 172 & 79 & 89 \\ 254 & 180 & 209 & 64 \\ 29 & 84 & 43 & 177 \\ 168 & 229 & 243 & 153 \end{bmatrix} \]
For blue (B) component of RGB image:

\[
K^{-1}_{1B} = \begin{bmatrix}
81 & 25 & 177 & 243 \\
68 & 21 & 251 & 231 \\
0 & 0 & 23 & 89 \\
0 & 0 & 8 & 31
\end{bmatrix}^{-1},
\]

\[
C^{-1}_{2B} = (-1) \begin{bmatrix}
97 & 143 & 89 & 73 \\
243 & 33 & 169 & 140 \\
59 & 48 & 93 & 180 \\
203 & 178 & 153 & 123
\end{bmatrix},
\]

Fig. 5(e) represents decrypted RGB image with exact parameters of AHC and its arrangement but slightly changed parameters of Arnold transform; i.e., we have used Arnold parameters \(AT^R = 6\) for red (R) channel, \(AT^C = 2\) for green (G) channel, and \(AT^B = 7\) for blue (B) channel of RGB image data.

Fig. 5(f) represents incorrectly decrypted image with exact parameters of AHC and AT but without knowing the correct arrangement of multiplicative parameters of AHC. The iAHC keys in the first stage are (before applying iAT):

For red (R) component:

\[
K^{-1}_{1R} = \begin{bmatrix}
79 & 11 & 0 & 0 \\
43 & 6 & 0 & 0 \\
189 & 219 & 73 & 57 \\
111 & 239 & 32 & 25
\end{bmatrix}^{-1},
\]

\[
C^{-1}_{2R} = (-1) \begin{bmatrix}
97 & 143 & 89 & 73 \\
243 & 33 & 169 & 140 \\
59 & 48 & 93 & 180 \\
203 & 178 & 153 & 123
\end{bmatrix},
\]

For green (G) component of RGB image:

\[
K^{-1}_{1G} = \begin{bmatrix}
81 & 25 & 177 & 243 \\
68 & 21 & 251 & 231 \\
0 & 0 & 23 & 89 \\
0 & 0 & 8 & 31
\end{bmatrix}^{-1},
\]

\[
C^{-1}_{2G} = (-1) \begin{bmatrix}
168 & 29 & 88 & 193 \\
49 & 219 & 118 & 41 \\
159 & 207 & 117 & 44 \\
68 & 96 & 169 & 143
\end{bmatrix},
\]

For blue (B) component of RGB image:

\[
K^{-1}_{1B} = \begin{bmatrix}
26 & 3 & 169 & 175 \\
43 & 5 & 230 & 128 \\
0 & 0 & 17 & 49 \\
0 & 0 & 26 & 75
\end{bmatrix},
\]

\[
C^{-1}_{2B} = (-1) \begin{bmatrix}
201 & 173 & 133 & 159 \\
11 & 147 & 30 & 205 \\
131 & 230 & 176 & 180 \\
65 & 198 & 86 & 77
\end{bmatrix},
\]

Now, we are applying inverse Arnold parameters \(AT^R = 5\) for red (R) channel, \(AT^C = 4\) for green (G) channel, and \(AT^B = 5\) for blue (B) channel of RGB image data at intermediate stage. The iAHC keys for second stage are (after applying iAT):

For red (R) component:

\[
K^{-1}_{2R} = \begin{bmatrix}
49 & 17 & 172 & 99 \\
75 & 26 & 183 & 153
\end{bmatrix},
\]

\[
C^{-1}_{1R} = (-1) \begin{bmatrix}
114 & 172 & 79 & 89 \\
254 & 180 & 209 & 64 \\
29 & 84 & 43 & 177 \\
168 & 229 & 243 & 153
\end{bmatrix},
\]

For green (G) component of RGB image:

\[
K^{-1}_{2G} = \begin{bmatrix}
17 & 49 & 38 & 92 \\
26 & 75 & 121 & 49
\end{bmatrix},
\]

\[
C^{-1}_{1G} = (-1) \begin{bmatrix}
87 & 45 & 188 & 221 \\
199 & 211 & 135 & 47 \\
98 & 29 & 66 & 153 \\
209 & 161 & 173 & 44
\end{bmatrix},
\]

For blue (B) component of RGB image:

\[
K^{-1}_{2B} = \begin{bmatrix}
132 & 197 & 68 & 81 \\
207 & 144 & 21 & 25
\end{bmatrix},
\]

\[
C^{-1}_{1B} = (-1) \begin{bmatrix}
254 & 219 & 179 & 231 \\
188 & 201 & 133 & 149 \\
69 & 33 & 83 & 43 \\
217 & 205 & 119 & 209
\end{bmatrix},
\]
5. Security analysis of the proposed technique

5.1. Key’s space of the cryptosystem

The key space of the cryptosystem refers to the set of all possible keys that can be used to generate a key for encryption, and is one of the most important attributes that support to the robustness and immenseness of a cryptosystem. A secure encryption algorithm should have a large key space to resist attacks, effectively. Large key space of the cryptosystem provides robustness against brute-force attack, known-plaintext attack, chosen-ciphertext attack, etc. In this technique, we have used 12 keys for the affine hill cipher; of which six are multiplicative keys, which are chosen from $SL_n(F_q)$ domain and reaming six are additive keys, which are selected from $M_n(F_q)$ domain. For large size of sub image, the $SL_n(F_q)$ and $M_n(F_q)$ contain large number of elements. The key space for multiplicative keys for each channel (red (R), green (G), and blue (B) channels) of affine hill cipher are

$$ |SL_n(F_q)| = \frac{|GL_n(F_q)|}{|SL_n(F_q)|} = \frac{|M_n(F_q)|}{|SL_n(F_q)|} = \frac{|GL_n(F_q)|}{q - 1} $$

where $H = \sum_{j=1}^{n} j^2$. Now, the key space of additive keys for each components of RGB image data is

$$ |M_n(F_q)| = q^{n^2} $$

Therefore, the possible key space for the affine hill cipher of an RGB image is $|SL_n(F_q)||M_n(F_q)|$. For large size of $n$, the cardinality of $SL_n(F_q)$ and $M_n(F_q)$ is also large then the key space of the whole cryptosystem is enormous. In this cryptosystem, we have considered two phase affine hill cipher (first phase before Arnold transform and second phase after Arnold transform). In each phase a user may choose different sizes of the block matrix, in such a case the keys space of the cryptosystem is very large. Therefore, the exhaustive keys search is not possible for the hacker. The proposed cryptosystem is free from brute-force attack, known-plaintext attack, chosen-ciphertext attack, etc.

5.2. Sensitivity analysis of the proposed cryptosystem

High sensitivity is required, to prevent the attacker from breaking the cryptosystem, that is, the encrypted RGB image data cannot be decrypted correctly, even if the exact parameters are slightly changed. The robustness of the cryptosystem is fully based on the sensitivity of the keys. The proposed cryptosystem for color image security should be sensitive to all parameters, which are used for encryption and decryption. In this cryptosystem, we have designed security of RGB image data on the basis of the parameters of affine hill cipher, Arnold transform and position (pre or post) of keys multiplication. The multiplicative keys, additive keys, arrangement of AHC parameters and position (pre or post) of keys multiplication with image data are highly sensitive. Fig. 6(a) represents the encrypted image. Fig. 6(b) is obtained when a small change in the keys of proposed cryptosystem at decryption process, while Fig. 6(c) shows the decrypted image, when the position (pre or post) of keys multiplication is not correct. Fig. 6(b) and (c) is completely different from original RGB image (Fig. 5(a)), which represents that no information can be obtained, even if, there is slight change in the keys and position of the keys multiplication side with RGB image data. The sensitivity analysis of the proposed cryptosystem represent that the keys and position (pre or post)

![Fig. 6. Sensitivity analysis: (a) encrypted image; (b) decrypted RGB image data with slightly change in exact parameters; (c) decrypted RGB image with all exact parameters of AHC and AT but without knowing the correct position (pre or post) of keys multiplication.](image)

of keys multipication are very sensitive. Moreover, the arrangement of parameters is also sensitive, which is already discussed in Fig. 5(d) and (f). The statistical analysis of these figures are given in Section 6.

5.3. Robustness of the approach when encrypted RGB image data occluded

In this section, we have discussed about robustness of the proposed approach when encrypted RGB image data occluded with 25% and 50% pixels. Encrypted RGB image (Fig. 5(b)) is occluded from left and right with 25% pixels, which is given in Fig. 7(a) and (b), respectively. Fig. 7(e) is the decrypted image of Fig. 7(a) when the exact keys and the correct arrangement of AHC parameters are applied on occluded image: similarly, Fig. 7(f) is the decoded image of Fig. 7(b) when all the exact parameters are used. This analysis indicates that the proposed approach is robust against the 25% occluded encrypted RGB image data. Now, encrypted RGB image data is occluded with 50% pixels from left and right, which is shown in Fig. 7(c) and (d), respectively and the corresponding decrypted image is presented in Fig. 7(g) and (h), respectively with all the exact keys and the correct arrangement of AHC parameters. Fig. 8(e), (f), (g), and (h) are decrypted images of Fig. 8(a), (b), (c), and (d), respectively. These decrypted images are obtained when the exact keys and the correct arrangement of AHC parameters are applied on occluded images. Further, the proposed technique is also robust when encrypted image data is occluded with 50% from inner, upper from diagonal, and lower from diagonal, which are given in Fig. 9(a), (b), and (c), respectively, and the corresponding decrypted images are given in Fig. 9(d), (e), and (f), respectively. The above analysis indicates that the proposed technique is robust against

![Fig. 7. Results (exact keys and correct arrangement of AHC parameters): (a) encrypted image occluded left with 25% pixels; (b) encrypted image occluded right with 25% pixels; (c) encrypted image occluded left with 50% pixels; (d) encrypted image occluded right with 50% pixels; (e) decrypted image of (a) with exact keys and correct arrangement of AHC parameters; (f) decrypted image of (b) with correct keys and exact arrangement of AHC parameters; (g) decrypted image of (c) with exact keys and arrangement of AHC parameters; (h) decrypted image of (d) with correct keys as well as correct arrangement of AHC parameters.](image)
the occlusion of 25% and 50% encrypted data. So, it is confirmed that in all cases, the partially encrypted RGB image data can be successfully decrypted. By analyzing all the above facts, we can say that proposed approach is robust against such types of occlusion attacks.

6. Statistical analysis

The statistical analysis supports the robustness of the cryptosystem. In this section, we will discuss the distribution of data, before and after encryption and decryption. We will also discuss about the mean square error (MSE) analysis, peak signal noise ratio (PSNR), and correlation coefficient analysis between two images.

6.1. Histogram analysis of color image data

An RGB image histogram is a graphical representation of the pixel intensity distribution of the RGB image. Therefore, an image histogram provides a clear illustration of how the pixels in an image are distributed, by plotting the number of pixels at each intensity level. Histogram of the original color image (Fig. 5(a)) is given in Fig. 10(a) and histogram of the encrypted image (Fig. 5(b)) is given in Fig. 10(b). The histogram of the encrypted image is totally different from the histogram of the original color image, which indicates that the encrypted image data is completely changed from the original image data. The histograms of Fig. 5(c) and 5(e) are given in Fig. 10(c) and 10(d), respectively. Now, the histogram of correctly decrypted image is exactly similar to the histogram of the original color image, which shows that the image is completely recovered after applying the exact keys and the correct arrangement of AHC parameters. While, Fig. 11(a), and (b) is histogram of Fig. 6(b), and (c), respectively.

The distribution of data in these figures indicates that the encrypted data is secured from attacks.

6.2. Mean square error, peak signal-to-noise ratio, and correlation analysis of color image

The mean square error (MSE) between the reconstructed color image data and the original color image data for red (R), green (G), and blue (B) components is computed from

\[
\text{MSE} = \frac{1}{N \times M} \sum_{g=1}^{N} \sum_{h=1}^{M} [g \Delta x, h \Delta y] - f_0(g \Delta x, h \Delta y)]^2,
\]

where \(n\) and \(m\) are the pixels of a RGB image, \(\Delta x\) and \(\Delta y\) are the pixel sizes.

The peak signal-to-noise ratio (PSNR) between the reconstructed image and the original color image for red (R), green (G), and blue (B) components is computed by

\[
\text{PSNR} = 10 \cdot \log_{10} \left( \frac{\text{MAX}_i^2}{\text{MSE}} \right) = 20 \cdot \log_{10} \left( \frac{\text{MAX}_i}{\sqrt{\text{MSE}}} \right) = 20 \cdot \log_{10}(\text{MAX}_i) - 10 \cdot \log_{10}(\text{MSE})
\]
Table 1
Statistical analysis between Fig. 5(b) and (a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>$8.0522 \times 10^3$</td>
<td>9.0716</td>
<td>$5.6359 \times 10^{-4}$</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>$6.4876 \times 10^3$</td>
<td>10.0099</td>
<td>$-1.700 \times 10^{-3}$</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>$4.4517 \times 10^3$</td>
<td>11.6455</td>
<td>$-1.3889 \times 10^{-4}$</td>
</tr>
</tbody>
</table>

Table 2
Statistical analysis between Fig. 5(c) and (a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>0.00</td>
<td>$\infty$</td>
<td>1.00</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>0.00</td>
<td>$\infty$</td>
<td>1.00</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>0.00</td>
<td>$\infty$</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Here, $\text{MAX}_i$ is the maximum possible pixel value of the image. More generally, when samples are represented using linear PCM with B bits per sample, $\text{MAX}_i$ is $2^B - 1$.

Now, correlation coefficient ($C_r$) of red (R), green (G), and blue (B) channels of original image and reconstructed image is computed by

$$C_r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\sum_m \sum_n (A_{mn} - \bar{A})^2 \sum_m \sum_n (B_{mn} - \bar{B})^2}}$$

(12)

where $\bar{A}$ and $\bar{B}$ are, respectively, the mean of output and input images. The correlation coefficient between two images varies from $-1$ to $+1$, i.e. $-1 \leq C_r \leq +1$. Two images $A$ and $B$ have a strong positive linear correlation if the correlation coefficient $C_r$ is close to $+1$. The $-1$ value of the correlation coefficient $C_r$ indicates a negative relationship between the two images and the correlation coefficient ‘zero’ represents that there is no relationship between the two images. The MSE, PSNR, and $C_r$ of red (R), green (G), and blue (B) channel of output and input color images are given in Tables 1–7.

The mean square error values, PSNR, and correlation coefficient for red (R), green (G), and blue (B) channels of encrypted color image (Fig. 5(b)) are given in Table 1, high MSE and low PSNR, and correlation coefficient values indicate that the original image data is completely changed. Therefore, no information about the original image can be obtained from encrypted image without knowing the exact keys and the correct arrangement of AHC parameters. The mean square error values, PSNR, and correlation coefficient of decrypted color image (Fig. 5(c)) for red (R), green (G), and blue (B) channel are given in Table 2. The zero MSE values, infinite PSNR and ‘1’ correlation coefficient of red, green, and blue indicates that the original image has been recovered completely without any loss of sensitive information of the RGB image data. The mean square error values, PSNR, and correlation coefficient for red (R), green (G), and blue (B) channel of Fig. 5(d), (e), and (f) is mentioned in Tables 3, 4, and 5, respectively. These values also show that the information about the original image cannot be obtained even if the decoder knows all the exact keys, but is not aware of the correct arrangement of AHC parameters. Now, in Tables 6 and 7 we have given the MSE, PSNR, correlation coefficient of Fig. 6(b) and (c), respectively. Thus, the statistical analysis of color image shows, that the proposed approach is robust against cryptanalytic because security of this approach not only depends on the keys, but also on the position (pre or post) of keys multiplication and the arrangement of AHC parameters.

6.3. Pixels intensity distributions of the images at horizontal, vertical, and diagonal pixels

The pixel intensity distributions at horizontal, vertical, and diagonal pixels of the original image (Fig. 5(a)) and encrypted image (Fig. 5(b)) are discussed in Fig. 12. Now, the pixel intensity distributions of the original image and the decrypted image (Fig. 5(c)) at horizontal, vertical, and diagonal pixels are given in Fig. 13. The pixel intensity distributions of the two neighboring pixels at different directions (horizontal, vertical, and diagonal) of the original and encrypted image are given in Fig. 12(a) and (b), respectively. The pixel intensity distributions of the encrypted image are uniformly distributed in the domain, which is completely different from pixels distributions of the original image. The distribution of data of the encrypted image indicates that no information of the original image can be obtained from the encrypted image. So, the encrypted color image is secured from

Table 3
Statistical analysis between Fig. 5(d) and (a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>$1.1225 \times 10^4$</td>
<td>7.6289</td>
<td>$1.9124 \times 10^{-4}$</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>$9.4912 \times 10^4$</td>
<td>8.3576</td>
<td>$8.5606 \times 10^{-4}$</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>$7.6011 \times 10^4$</td>
<td>9.3220</td>
<td>$1.4363 \times 10^{-4}$</td>
</tr>
</tbody>
</table>
attacks. Fig. 13(a) and (b) is the pixel intensity distributions of two neighboring pixels at horizontal, vertical, and diagonal directions of the original and the correctly decrypted image, respectively. The pixel distributions of the correctly decrypted image is exactly similar to the pixels distributions of the original image, which represents that the image is completely recovered on applying the exact keys and the correct arrangement of parameters.

7. Comparison of the proposed technique with existing methods

This cryptosystem is compared with the earlier developed cryptosystems for color images such as: Abuturab [10], Liu et al. [12], and Chen and Zhao [13]. Abuturab [10] and Liu et al. [12] designed a cryptosystem for color images with the help of Arnold transform. In the decryption process, Abuturab [10] and Liu et al. [12] used the periodicity property of Arnold transform, which is time consuming, but in our proposed cryptosystem we have used inverse Arnold transform for decryption process. Owing to this reason, the decryption process of our cryptosystem is faster than the techniques [10] and [12]. Furthermore, the security of both the cryptosystems depends on the keys only. The results of the techniques [10] and [12] are discussed in Figs. 14 and 15, respectively. Now, Chen and Zhao [13] have also given image encryption and decryption, in dual fractional Fourier-wavelet domain with random phases. The security provided by this technique is based on the keys only. The experimental analysis of this technique is given in Fig. 16. So, in the above techniques, if the attacker knows all the exact keys, then he/she can recover original information. But our cryptosystem provides security of RGB images with the help of the keys and the arrangement of AHC parameters and hence it is very difficult to recover the original image even if the hacker has the exact keys. The experimental results and robustness analysis of the proposed cryptosystem are given in Figs. 5 and 6.

Table 4
Statistical analysis between Fig. 5(e) and (a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>1.2176 × 10^4</td>
<td>7.2757</td>
<td>0.0080</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>1.0576 × 10^4</td>
<td>7.8875</td>
<td>0.0054</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>8.7072 × 10^3</td>
<td>8.7320</td>
<td>0.0042</td>
</tr>
</tbody>
</table>

Table 5
Statistical analysis between Fig. 5(f) and (a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>1.3018 × 10^4</td>
<td>6.9854</td>
<td>−6.9802 × 10^−3</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>1.1312 × 10^4</td>
<td>7.5955</td>
<td>−1.1859 × 10^−4</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>9.4136 × 10^3</td>
<td>8.3932</td>
<td>−1.3820 × 10^−4</td>
</tr>
</tbody>
</table>

Table 6
Statistical analysis between Figs. 6(b) and 5(a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>7.3236 × 10^3</td>
<td>9.4835</td>
<td>0.1969</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>6.2869 × 10^3</td>
<td>10.1464</td>
<td>0.2861</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>5.3503 × 10^3</td>
<td>10.8470</td>
<td>0.1443</td>
</tr>
</tbody>
</table>

Table 7
Statistical analysis between Figs. 6(c) and 5(a).

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Components of color image</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Red component of color image</td>
<td>1.2494 × 10^4</td>
<td>7.1637</td>
<td>−1.1424 × 10^−4</td>
</tr>
<tr>
<td>2.</td>
<td>Green component of color image</td>
<td>1.0789 × 10^4</td>
<td>7.8009</td>
<td>−1.1177 × 10^−4</td>
</tr>
<tr>
<td>3.</td>
<td>Blue component of color image</td>
<td>8.8942 × 10^3</td>
<td>8.6397</td>
<td>−1.6250 × 10^−4</td>
</tr>
</tbody>
</table>

Fig. 14. Results of proposed color image encryption and decryption: (a) original image with 512 × 512 pixels and 24 bits used in numerical simulation; (b) encrypted image, (c) decrypted image with all the correct keys; and (d) decrypted image with transformation angles for component images changed by 0.004 but correct iterative numbers and random phase functions. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Fig. 15. Results: (a) original image; (b) encryption image; (c) decrypted image.

Summing up, the facts presented above, including all-experimental results, key’s space analysis, sensitivity analysis, statistical analysis of the proposed cryptosystem of color image data, and comparison with the existing techniques, demonstrate to the robustness and appropriateness of the presented cryptosystem.
8. Conclusion

In this technique, we have presented a new cryptosystem for the RGB image data of size $m 	imes m$, which is designed using the affine hill cipher (AHC) over $SL_n(F_q)$ and $M_n(F_q)$ domains with 2-dimensional Arnold transform (AT). We have considered multiplicative keys from $SL_n(F_q)$ domain and additive keys from $M_n(F_q)$ domain such that $n$ divides the size of image matrix $(m)$, which provides enormous key space for the presented cryptosystem. In the proposed method, the encryption procedure is usual but decryption procedure is more inconvenient, since there is no idea about the exact keys of affine hill cipher and the specific arrangement of AHC parameters. Furthermore, even if the attacker has all the exact keys, but is not aware of the correct arrangement of AHC parameters, then he/she cannot recover the original information correctly from the cipher data (encrypted image). Another advantage of this technique is that, in affine hill cipher matrix multiplication is used, which is noncommutative, which is utilized in our encryption process, so decryption process depends on the position (pre or post) of multiplication of inverse multiplicative keys with the encrypted image (on the same position of multiplicative keys used in the encryption process), if there is no information about the specific position (pre or post) of keys multiplication, then the attacker cannot recover the original image. The proposed cryptosystem provides security of RGB image data by the keys, arrangements of AHC parameters and the position (pre or post) of keys multiplication, which are highly sensitive. The mean square error values of correctly decrypted RGB image for red (R), green (G), and blue (B) components are exactly ‘zero’, PSNR and correlation coefficient of these components are ‘infinite’ and ‘1’, respectively, which indicate that the proposed cryptosystem provides security of RGB image data without any impairment of information. The security and statistical analysis vindicate the robustness of the presented cryptosystem. Therefore, the presented cryptosystem for color image data can be used for secure transmission through unsecured channels without any attenuation in the sensitive information.

References