Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466
Vol. 8, Issue 2 (December 2013), pp. 777 – 791

Applications and Applied Mathematics:
An International Journal
(AAM)

Grayscale-image encryption using Random Hill Cipher over $SL_n(\mathbb{F})$ associated with Discrete Wavelet Transformation

D. C. Mishra and R. K. Sharma

Department of Mathematics
Indian Institute of Technology
Delhi, Hauz Khas-110016, New Delhi, India
deepiitdelhi@gmail.com; rksharma@maths.iitd.ac.in

Received: June 13, 2013; Accepted: November 26, 2013

Abstract

Image data are highly sensitive and prone to incidental decoding by intruders. The security of image data in an insecure network is therefore a major issue. In this paper, we have presented a novel approach for grayscale-image encryption and decryption using Random Hill cipher over $SL_n(\mathbb{F})$ associated with discrete wavelet transformation. Earlier techniques for encryption and decryption of image data discussed missing the keys, but in this approach, both the keys and the arrangement of RHC are emphasized. Additionally, keys multiplication side (pre or post) over a grayscale-image data matrix also inevitable to know, to correctly decrypt the encrypted image data. In proposed approach, consider keys from special linear group over field $\mathbb{F}$. The key space of the whole cryptosystem is exorbitant. We have presented a computer simulation with a standard examples and the results is given to analyze the robustness of the proposed technique. Security analysis and detailed comparison among earlier developed techniques with proposed approach are also discussed for the robustness of the technique.

Keywords: Cryptography; Random hill cipher; Discrete wavelet transformation; Encryption; Decryption; $SL_n(\mathbb{F})$

MSC 2010 No.: 92A64; 65T60; 68U10; 68P25

1. Introduction

Security of images in data transmission is a major concern of global proportions. Image data are highly sensitive and prone to incidental decoding by intruders. Important modes such as: digital techniques, network and communication technologies are widely spread to transfer image data securely over the nations. Images are used in various areas, for instance: online education and training, research and experimental purposes, military services, commercial purposes, etc; in all these areas, maintaining the fidelity, security, and confidentiality of original image data is a critical issue. In this paper the encryption process is based on Two Stage Random Hill Cipher (TSRHC) over $SL_n(\mathbb{F})$ associated with Discrete Wavelet Transformation (DWT) is designed to ensure secure transmission of image data. Several methods have been developed for encryption and decryption of image data securely, authors, such as Jan et al. (1996) proposed image encryption using SCAN patterns and the ciphers based on the SCAN transposition cipher; (Hahn et al., 2006; Hennelly and Sheridan, 2003; Almedia, 1994; Chen et al., 2013) have given image encryption and decryption using fractional Fourier transformation; (Abuturab, 2012b; Abuturab, 2012a; Abuturab, 2012c) have proposed image encoding and decoding over gyrator transform domain; (Chen and Zhao, 2006) have given image security using Hartley transform; (Antonini et al., 1992; Chen and Zhao, 2008) have discussed image coding by wavelet transform; and (Liu et al., 2001; Singh et al., 2009; Zhang et al., 2002) using optical transforms for image encryption. This proposed approach is suitable for secure transmission of large size images. The original image divides into equal block sizes such that block size (order of sub images) must be same as size (order) of hill cipher key and the hill cipher keys are selected from $SL_n(\mathbb{F})$ (Green, 1977) $SL_n(\mathbb{F})$ is a set of all $n \times n$ matrix whose determinant is 1, which forms a group under multiplication over field $\mathbb{F}$. Hill cipher (Rosen, 1984; Stallings, 2006) is one of the most well known technique for encryption and decryption of text data. But in this approach, we have developed security of image data through random hill cipher and DWT. The paper (Samson and Sastry, 2012) describes for an RGB image encrypted using hill cipher and discrete wavelet transformation, that considers involutory matrix for key. (Muttoo et al., 2012) and (Panduranga and Naveen, 2012) consider self invertible matrix (also involutory matrix) for hill cipher key. But our proposed Random Hill Cipher (RHC) is specifically for images presented in matrix and the hill cipher keys are chosen from $SL_n(\mathbb{F})$. Since $SL_n(\mathbb{F})$ is nonabelian group and matrix multiplication is noncommutative then multiplication of hill cipher key with grayscale-image is depending on pre or post multiplication is inevitable to know, to correctly decrypt the encrypted grayscale-image. First, our random hill cipher applied on grayscale-image before DWT, second it is applied after DWT. We define it as Two Stage Random Hill Cipher (TSRHC), where our first stage signifies before applying DWT and second stage signifies after applying DWT. After DWT (Daubechies, 1992; Gonzalez and Woods, 2008) the two dimensional image is decomposed into four sub-images and each of them is a quarter size of the original image. One of the sub-images is a low frequency sub-band which can be decomposed continually and the others are high frequency sub-band in the horizontal direction, vertical direction and diagonal directional, respectively. The image after DWT forms a tree structure arranging from low to high frequency bands. The structure of wavelet decomposition of an image at different levels is shown in Figure 3. The DWT (Daubechies, 1992; Gonzalez and Woods, 2008; Mallat, 1999; Pathak, 2009) is widely used in signal and image processing, data

compression, and sound analysis, etc. Experimental results, security analysis, and comparison between proposed technique with (Samson and Sastry, 2012; Panduranga and Naveen, 2012) are support for the robustness and immenseness of the proposed approach.

In section 2, we explained the proposed approach of RHC and DWT. After a quick overview of RHC and DWT in general, we describe in more detail the ideas and organization of our proposed technique. We have presented in section 3, the method used in this paper for image encryption and decryption for proposed approach using TSRHC associated with DWT. We focus particularly in this section the number of keys chosen and arrangement of RHC keys in the proposed approach. Demonstration of the procedure for image encryption and decryption is mentioned in section 4. Our section 5, discussed about security analysis and robustness of the approach. Section 6, gives in-depth comparison with several other authors. In section 7, we have drawn conclusion of this approach.

2. Random Hill Cipher and Discrete Wavelet Transformation

In our construction we are taking random hill cipher on grayscale-image of size $m \times m$. The pixels of grayscale-image is divided into equal blocks, we call it as block matrix (sub image) of the original image, the sub image size is as same as key size of hill cipher which is defined by the user. In proposed approach the hill cipher keys are consider from $SL_n(\mathbb{F})$ domain such that n divides m. The procedure of block creation (in particular block size 4×4 and 2×2) for grayscale-image data is illustrated in Figure 1. Suppose user chooses such type of block matrix (sub image), and if order of block matrix dose not divide order of original image matrix then we need to add some redundant rows or columns or both in the original image matrix. $SL_n(\mathbb{F})$ is the set of all $n \times n$ matrix that contains those elements of $GL_n(\mathbb{F})$ (Green, 1977) whose determinant is 1 over field $\mathbb{F}$. The mathematical definition of $SL_n(\mathbb{F})$ is as follows:

$$SL_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) | \det(A) = 1\}, \tag{1}$$

where, $GL_n(\mathbb{F})$ is general linear group over field $\mathbb{F}$. Because $SL_n(\mathbb{F})$ contains those elements from $GL_n(\mathbb{F})$, whose determinant is equal to 1 (Equation (1)), so the order of $SL_n(\mathbb{F})$ is very large.

Since determinant of every element of $SL_n(\mathbb{R})$ is one then inverse of hill cipher key (K^{-1}) is same as adjoint of hill cipher key (K), because $K^{-1} = \dfrac{adj(K)}{\det(K)}$.

Formulation for Random Hill Cipher (RHC) of a block matrix (sub image) of size $n \times n$ is given as:

$$C = B.K \pmod{P}, \tag{2}$$

where, B be a $n \times n$ block matrix (sub image) of the grayscale-image of size $m \times m$, K is a $n \times n$ key matrix from special linear group (Equation (1)), and C be a cipher block of size $n \times n$. Formulation for inverse Random Hill Cipher (iRHC) of block matrix (sub image) of size $n \times n$ is given as:

$$B = C.adj(K) \pmod{P}, \tag{3}$$

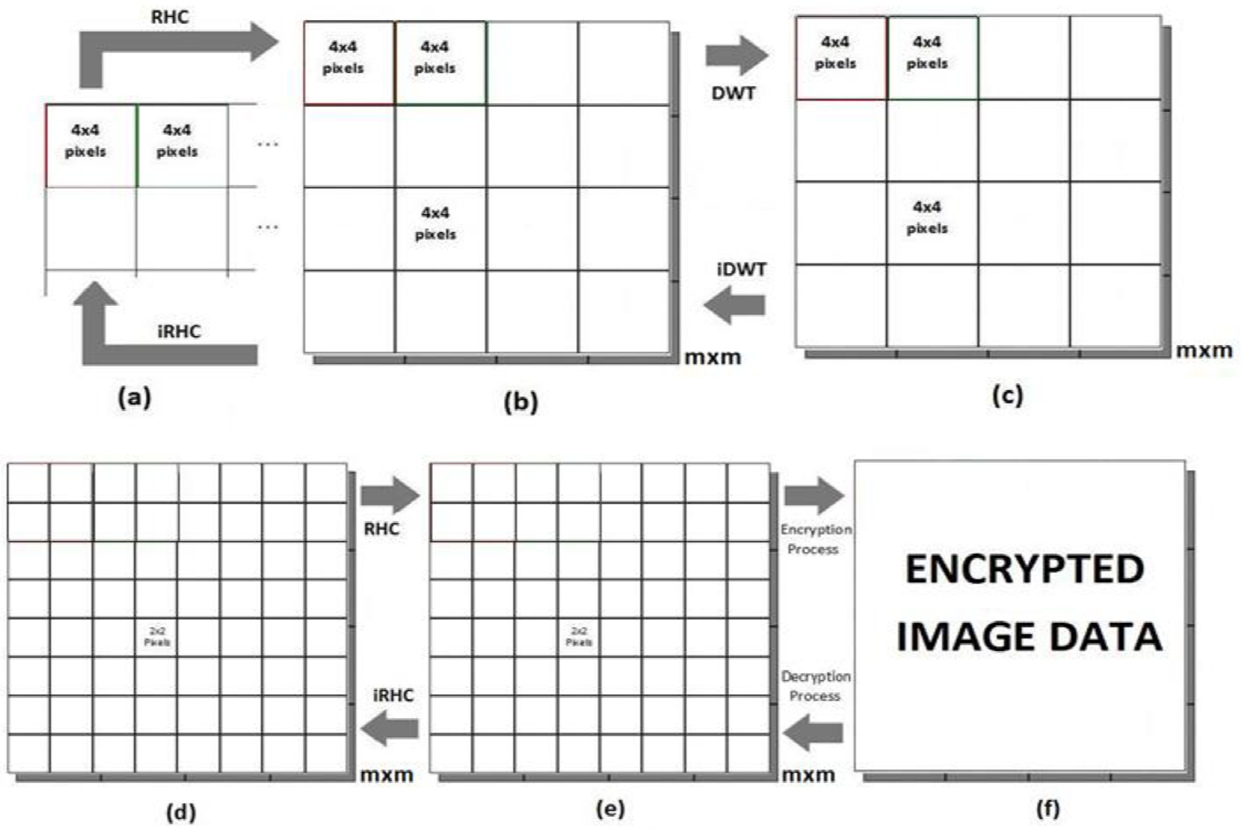

Fig. 1: Process of block creation: (a) Original image divided into 4×4 blocks before applying first stage RHC; (b) Partially encrypted image after applying first stage RHC; (c) Partially encrypted image after applying DWT; (d) Partially encrypted image divided into 2×2 blocks before applying second stage RHC; (e) Encrypted image after applying second stage RHC; (f) Encrypted block image converted into original image size.

where, $adj(K)$ is adjoint of key matrix $K \in SL_n(\mathbb{F})$, and P be unit representation. Similarly, the same process is applied for remaining block matrix (sub image) of the original grayscale-image. In equation (3), the position of $adj(K)$ is fixed according to the position of K (Equation (2)), because matrix multiplication is noncommutative (if attacker multiplies $adj(K)$ with C (Equation (3)) without knowing the exact position of K, then original image can not be recovered correctly).

In our proposed approach we have also used wavelet transformation as keys. In the DWT (Pathak, 2009) domain the general features and the details of a signal and image can be analyzed. Two dimensional DWT (Gonzalez and Woods, 2008) is carried out by performing in the row direction and column direction, separably. When two dimensional DWT is carried out for two dimensional data, such as image, four domains with different frequency characteristics are generated. Each of them are called as a sub-band and is generally marked as A, H, V, and D domain according to their frequency characteristic. Because the four sub-bands are down-sampled in the row and column directions, the total size of the four sub-bands is equal to the size of the original image.

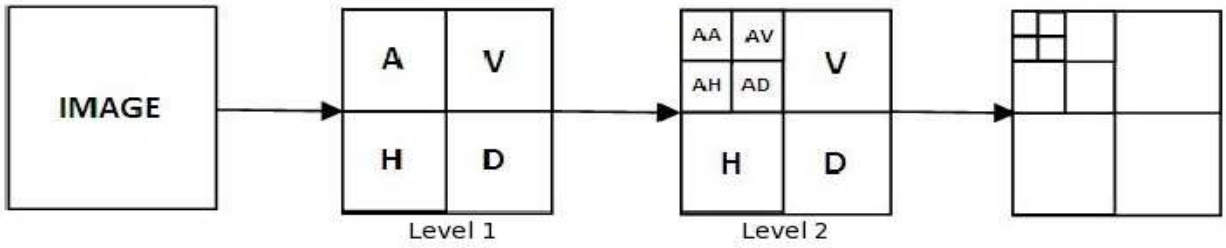

Fig. 2: Classification of Wavelet decomposition at different levels.

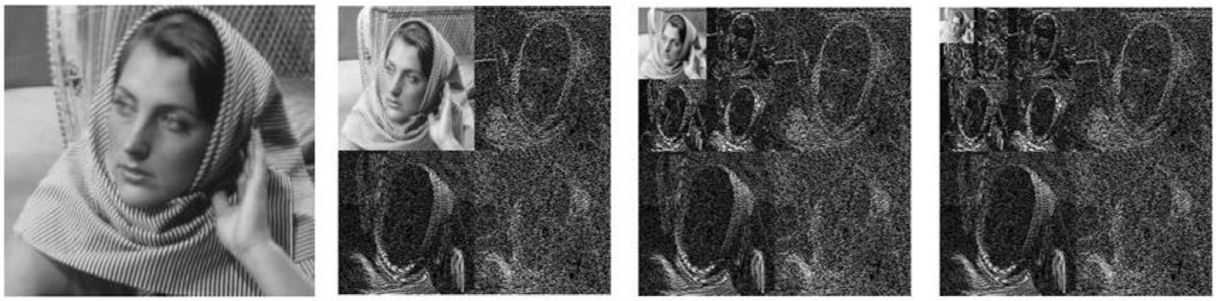

Fig. 3: Wavelet decomposition: (a) Original Barbara image; (b) Barbara image at fist level wavelet; (c) Barbara image at second level wavelet; (d) Barbara image at third level wavelet.

DWT (Gonzalez and Woods, 2008) of an image $f(x,y)$ of size $N \times M$ is defined as follows:

$$W_{\varphi}(j_0,n,m) = \frac{1}{\sqrt{NM}} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y)\varphi_{j_0,n,m}(x,y), \tag{4}$$

$$W_{\psi}^{i}(j,n,m) = \frac{1}{\sqrt{NM}} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y)\psi_{j,n,m}^{i}(x,y), i = \{H,V,D\} \tag{5}$$

for $j \geq j_0$ and

$$\begin{aligned} f(x,y) = & \frac{1}{\sqrt{NM}} \sum_{n} \sum_{m} W_{\varphi}(j_0,n,m)\varphi_{j_0,n,m}(x,y) \\ & + \frac{1}{\sqrt{NM}} \sum_{i=H,V,D} \sum_{j=j_0} \sum_{n} \sum_{m} W_{\psi}^{i}(j,n,m)\psi_{j,n,m}^{i}(x,y), \end{aligned} \tag{6}$$

where, j_0 is an arbitrary starting scale and

$$\varphi_{j,n,m}(x,y) = 2^{j/2}\varphi(2^j x - n, 2^j y - m), \tag{7}$$

$$\psi_{j,n,m}^{i}(x,y) = 2^{j/2}\psi^{i}(2^j x - n, 2^j y - m), \quad i = \{H,V,D\}, \tag{8}$$

here, index i identifies the directional wavelets that assumes values of H, V, and D. Equations (7)–(8) defines the scaled and translated basis functions. $f(x,y)$, $\varphi_{j,n,m}(x,y)$, and $\varphi_{j,n,m}^{i}(x,y)$

are functions of the discrete variables $x = 0, 1, 2, 3, \ldots, N-1$ and $y = 0, 1, 2, 3, \ldots, M-1$. The coefficients defined in Equations (4) and (5) are usually called approximation and detail coefficients, respectively. $W_\varphi(j_0, n, m)$ coefficients define an approximation of $f(x, y)$ at scale j_0. $W_\psi^i(j, n, m)$ coefficients add horizontal, vertical, and diagonal details for scales $j \geq j_0$. We normally let $j_0 = 0$ and select $M = N = 2^j$ such that $j = 0, 1, 2, 3, \ldots, J-1$ and $n, m = 0, 1, 2, 3, \ldots, 2^j - 1$. Equation (6) shows that $f(x, y)$ is obtained via the inverse DWT for given W_φ and W_ψ^i of Equations (4) and (5).

3. Procedure of encryption and decryption using TSRHC associated with DWT

Two Stage Random Hill Cipher associated with DWT is applied on grayscale-image. The encryption and decryption processes are illustrated in Figure 4 and Figure 5, respectively. In the first stage we have entire one option for random hill cipher which is applied over grayscale-image, Similarly, in the next stage one option is also available for random hill cipher for image. Therefore, the total number of choices of random hill cipher applied on grayscale-image in combining both stages is $2!$ options. These stage options mentioned here is also called arrangement of random hill cipher.

The procedure of encryption for grayscale-image is given in Figure 4. In the first stage, we applied K_1 key for RHC, then DWT is applied over partially encoded image. Finally, K_2 key is applied for second stage RHC. The same procedure is applied for decryption process which is illustrated in Figure 5. In the first stage, we choose key for inverse Random Hill Cipher (iRHC) denoted as K_2^{-1} (inverse of K_2 key), thereafter, inverse Discrete Wavelet Transformation (iDWT) is applied on the partially decoded image. We applied in second stage iRHC with K_1^{-1} key (inverse of K_1) on the partially decoded image. Then, finally original image is recovered. This approach uses only three keys - two key for random hill cipher, and one key for discrete wavelet. In our approach, the size of hill cipher key depends on the size of the block matrix (sub images) of the original image which ultimately depends on the choice of encoder (here, encoder is free to choose any size of sub image). But some earlier approaches such as (Samson and Sastry, 2012; Muttoo et al., 2012; Panduranga and Naveen, 2012) uses fixed size of hill cipher key. In our approach, even though, decoder have the correct keys, but does not have the information about the correct arrangement of RHC, decoder cannot recover the original image (Figure 6(f)), so our proposed approach not only depends on keys, but also depends on arrangement of random hill cipher with wavelet.

4. Demonstration of the procedure

The procedure is applied on grayscale-image of size 256×256 pixels shown in Figure 6(a). Figure 6(b) shows encrypted grayscale-image with the following keys, the RHC key in the first

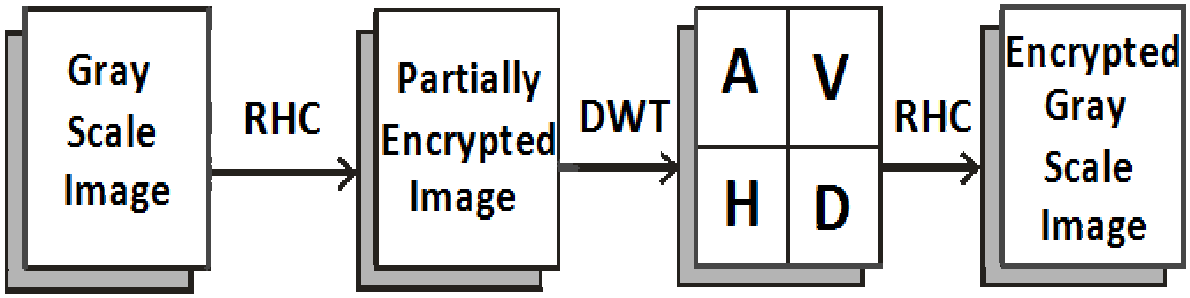

Fig. 4: Encryption process for grayscale-image.

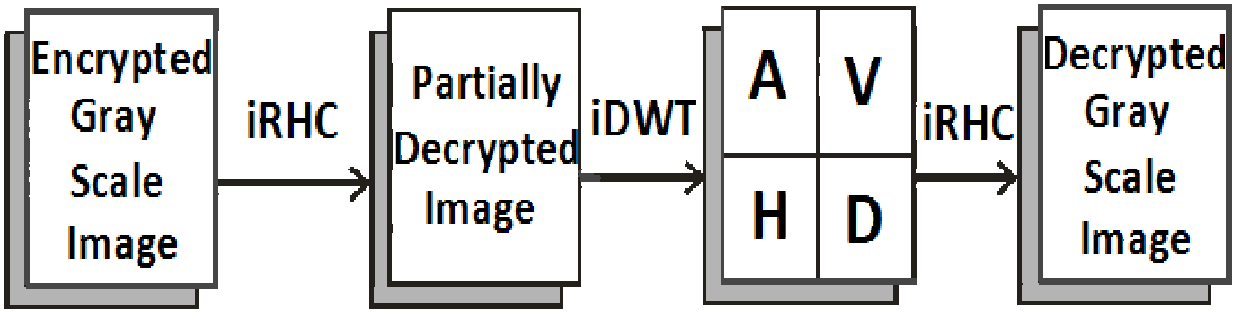

Fig. 5: Decryption process for grayscale-image.

stage are (before applying DWT):

$$K_1 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 0 & 1 & 7 & 4 \\ 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and RHC key for partially decrypted grayscale-image in second stage is (after applying DWT):

$$K_2 = \begin{bmatrix} 11 & 7 \\ 3 & 2 \end{bmatrix},$$

with 'db4' wavelet.

Figure 6(c) represent correctly decrypted grayscale-image with exact keys and correct arrangement. The inverse RHC key in the first stage is (before applying DWT):

$$K_2^{-1} = \begin{bmatrix} 2 & -7 \\ -3 & 11 \end{bmatrix},$$

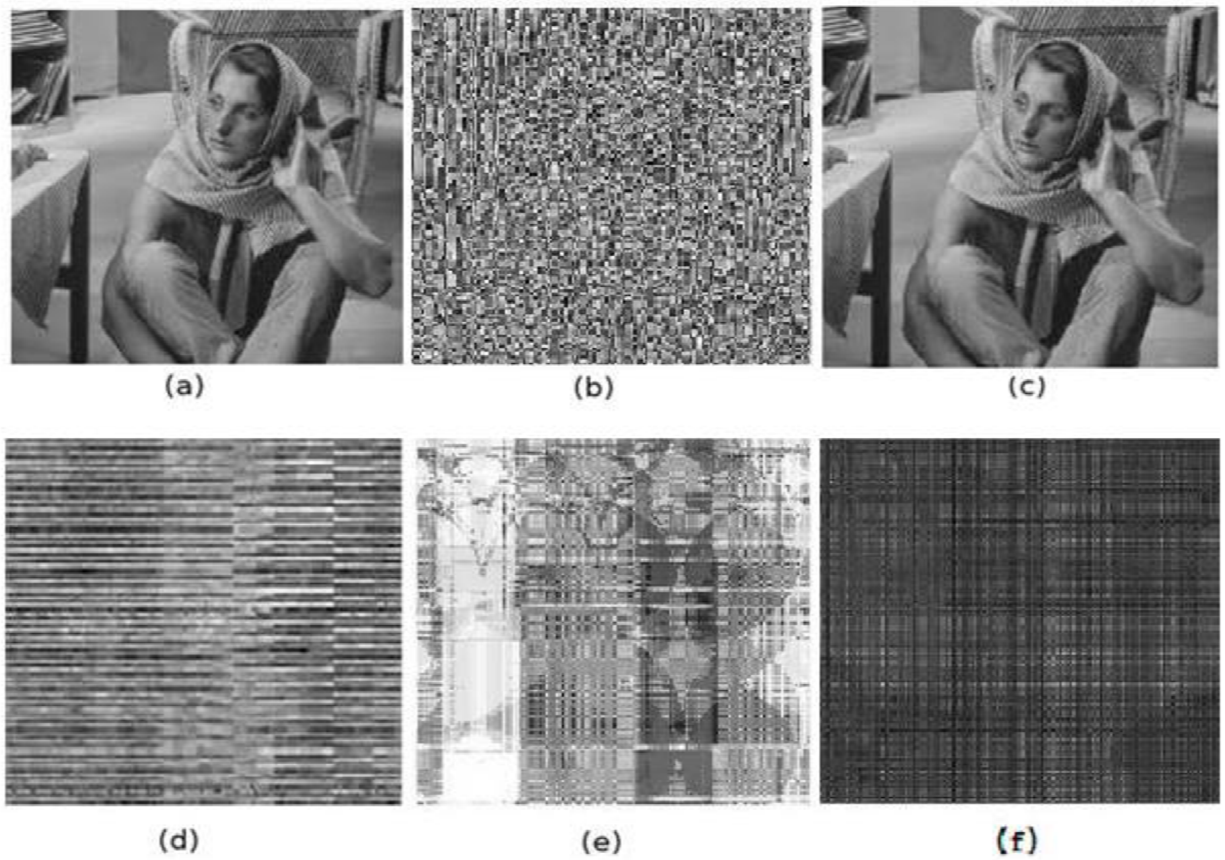

Fig. 6: Encryption and Decryption results: (a) Original image of size 256×256 pixels; (b) Encrypted image; (c) Correctly decrypted image with correct keys and correct arrangement; (d) Incorrectly decrypted image with correct wavelet and arrangement but approximated RHC; (e) Incorrectly decrypted image with correct RHC but wrong wavelet and arrangement of RHC keys; (f) Incorrectly decrypted image with correct RHC keys and wavelet but without knowing the correct arrangement of RHC keys and DWT.

and inverse RHC key for the partially decrypted grayscale-image in second stage is (after applying DWT):

$$K_1^{-1} = \begin{bmatrix} 1 & -3 & 16 & -123 \\ 0 & 1 & -7 & 52 \\ 0 & 0 & 1 & -8 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

with ‘db4’ wavelet.

Figure 6(d) represent incorrectly decrypted grayscale-image with approximated RHC key, wavelet as well as arrangement is same as in the correct decryption process (Figure 6(c)).

Figure 6(e) represent incorrectly decrypted grayscale-image with wrong WT and incorrectly

arrangement of RHC keys. The RHC key in the first stage is (before applying DWT):

$$K_1^{-1} = \begin{bmatrix} 1 & -3 & 16 & -123 \\ 0 & 1 & -7 & 52 \\ 0 & 0 & 1 & -8 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and RHC keys for the partially decrypted grayscale-image in second stage is (after applying DWT):

$$K_2^{-1} = \begin{bmatrix} 2 & -7 \\ -3 & 11 \end{bmatrix}.$$

Figure 6(f) represent incorrectly decrypted grayscale-image with correct random hill cipher keys, and wavelet but without knowing the correct arrangement of random hill cipher keys, and DWT.

5. Security analysis

5.1. Sensitivity analysis of the proposed approach

The proposed technique for image encryption and decryption should be sensitive with respect to all parameters, which is used for security. High sensitivity is required for unbreakable cryptosystems, i.e., the encrypted image data cannot be decrypted correctly (recover original image data) even though the exact parameters are slightly changed. In this technique we have used keys, arrangement of RHC, and position (pre or post) of keys multiplication with image data for secure cryptosystem, which are highly sensitive. Figure 7(a) represents the encrypted image. Figure 7(b) shows that, if a more change in any one of the keys with no information about position of keys multiplication then still attackers can not recover the original image data. The slight difference in only one key and all others parameters are same as correct decryption process, which is presented in Figure 7(c). Figure 7(d) is decrypted image using wrong DWT. Now, Figure 7(e) represents incorrectly decrypted image with no information about correct arrangement of RHC as well as position of keys multiplication with image data, while Figure 7(f) obtained by incorrect arrangement of RHC and remaining parameters are as usual. Therefore, Figure 7 represents that, the keys, arrangement of RHC, and pre or post multiplication side of keys are highly sensitive.

5.2. Key's space analysis of the proposed cryptosystem

In cryptography, an algorithm's key space refers to the set of all possible keys that can be used to generate a key, and is one of the most important attributes that determines the strength of a cryptosystem. A secure encryption algorithm should have a large key space to make it resist exhaustively against attacks, effectively. In proposed cryptosystem, we have used six random hill cipher keys, which are chosen from $SL_n(\mathbb{F})$; and $SL_n(\mathbb{F})$ contains those elements of $GL_n(\mathbb{F})$ whose determinant is 1. Thus, the order of $SL_n(\mathbb{F})$ is very large. So the key space of the whole cryptosystem is also large. In the case when finite field containing q elements the cardinality of

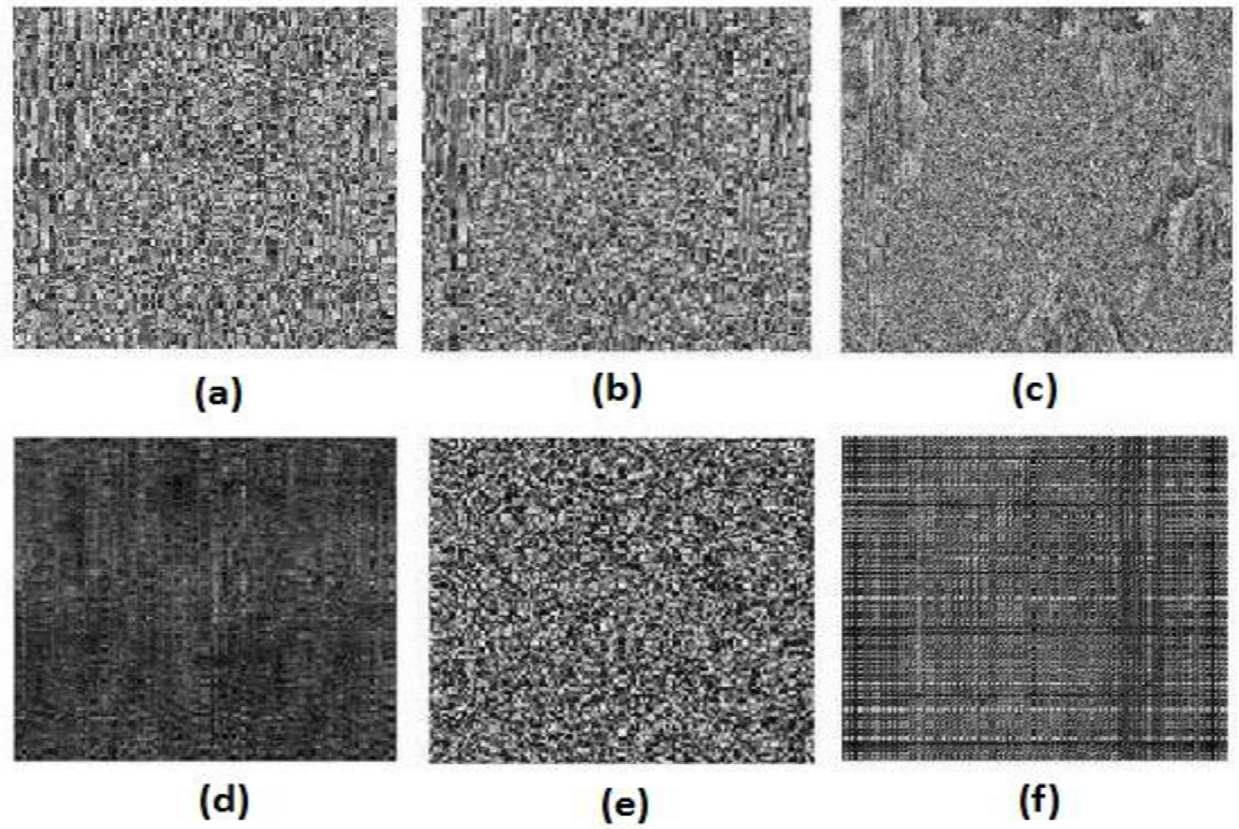

Fig. 7: Sensitivity analysis: (a) Encrypted image; (b) Decrypted image with all exact keys except one of them is slightly different from exact key and without knowing the correct multiplication side (pre or post); (c) Decrypted image data with all exact keys except one of them is slightly different from exact keys; (d) Incorrectly decrypted image with correct RHC but incorrect wavelet; (e) Incorrectly decrypted image with correct wavelet, wrong arrangement of RHC and no information of multiplication side; (f) Decrypted image with all exact parameters without knowing the correct arrangement of RHC.

the key space for each phase of hill cipher keys are

$$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{|GL_n(\mathbb{F}_q)|/|SL_n(\mathbb{F}_q)|} = \frac{|GL_n(\mathbb{F}_q)|}{|GL_n(\mathbb{F}_q) : SL_n(\mathbb{F}_q)|}$$
$$= \frac{|GL_n(\mathbb{F}_q)|}{q-1} = \frac{q^H}{q-1}\prod_{j=1}^{n}(q^j-1),$$

where $H = \sum_{j=1}^{n-1} j = \begin{pmatrix} n \\ 2 \end{pmatrix}$. For this approach, we have considered two random hill cipher keys for security of a grayscale-image data. In each phase a user may choose different order of random hill cipher keys. For large size of n and q, the key space of the whole cryptosystem is exorbitant. Moreover, in this approach arrangement of RHC and position of keys multiplication are also considered for secure cryptosystem.

5.3. Robustness of the approach for sparse image

In this section, we have discussed about robustness of the proposed technique. The robustness of proposed approach for sparse image shown in Figure 8. Figure 8(a) is original sparse image, Figure 8(b) be encrypted sparse image, the pixels of encrypted image are equally distributed and mean square error value is given in Table I, which represent the encrypted sparse image data is also more secure. The correctly decrypted image is given in Figure 8(a) and mean square error analysis is also provided in same Table I. This value is very closed to zero, which indicate that the image data is completely recover without loss of any information and intensity. Finally, we can conclude that the proposed approach is also suitable for secure transmission of spare image without loss of any information.

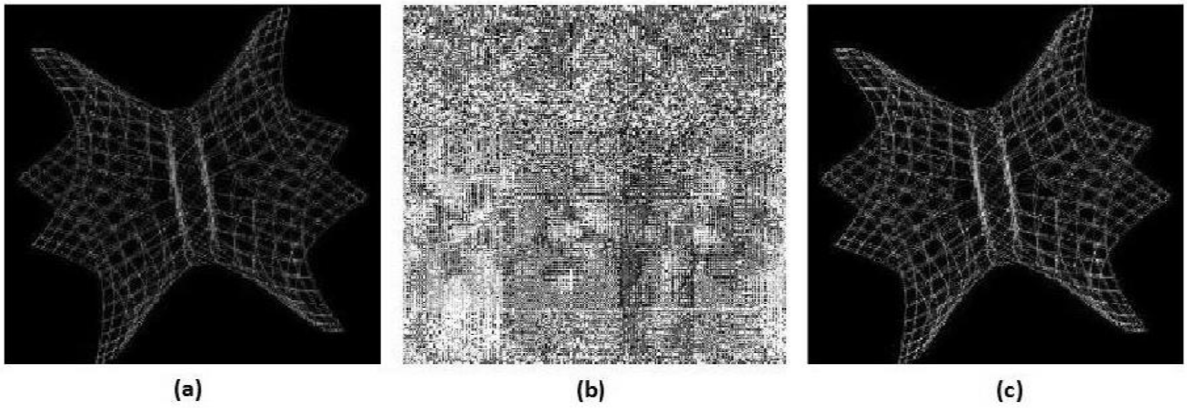

Fig. 8: Robustness for sparse image: (a) Original sparse image; (b) Encrypted sparse image; (c) Correctly decrypted sparse image with exact keys and correct arrangement.

5.4. Histogram analysis

In this section, we have presented histogram analysis of the proposed approach. Histogram of the image data represents how pixels in grayscale-image are spread by marking out the number of pixels at each intensity level. Histogram of 256×256 pixels Barbara.jpg image (Figure 6(a)) is given in Figure 9. The histogram of encrypted image illustrated in Figure 10, and histogram of decrypted image is given in Figure 11. The encrypted image (Figure 6(b)) histogram is totally different from the original image (Figure 6(a)) histogram and it is peculiar in statistical similarity, which represent that no information about original image can be obtained by encrypted image data. While correctly decrypted image (Figure 6(c)) histogram is similar in visual effect. This shows that the no information loss by encryption and decryption process.

5.5. Mean Square Error analysis

The Mean Square Error (MSE) between the reconstructed grayscale-image data and original

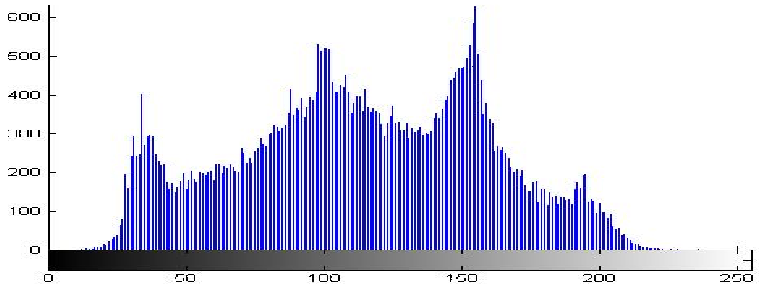

Fig. 9: Histogram of an original image (Figure 6 (a)).

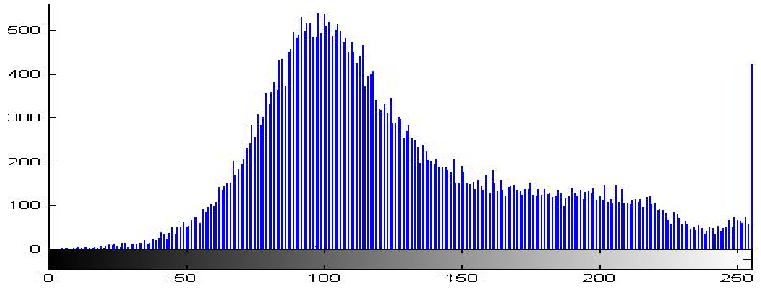

Fig. 10: Histogram of an encrypted image (Figure 6 (b)).

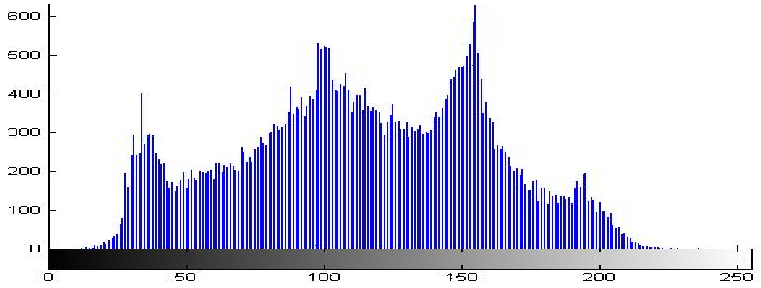

Fig. 11: Histogram of a decrypted image (Figure 6 (c)).

graycsale-image data is obtained by the formula

$$MSE = \frac{1}{X \times Y} \sum_{n=1}^{X} \sum_{m=1}^{Y} \left[|f(n\Delta x, m\Delta y) - f_0(n\Delta x, m\Delta y)|^2 \right],$$

where X and Y are the pixels of an image, Δx and Δy are the pixel sizes. The mean square error of images are given in tables I, II, III, and IV.

The mean square error value of encrypted grayscale-image (Figure 6(b)) is given in Table II. This value is very large, which represents that no information about the original image can be obtained from encrypted image without knowing of the exact keys and correct arrangement of RHC. The MSE value of correctly decrypted grayscale-image (Figure 6(c)) is given in Table III. This value is tends to zero, which indicate that the original image has been recovered exactly

TABLE I: Mean square error of Figure 8(b) and Figure 8(c).

S.No.	Sparse grayscale-image of size 256×256	MSE Figure 8(b)	MSE of Figure 8(c)
1.	Sparse grayscale-image	4.110×10^3	8.7820×10^{-27}

TABLE II: Mean square error of encrypted Image (Figure 6(b)).

S.No.	Grayscale-image of size 256×256	MSE of encrypted image (Figure 6(b))
1.	Barbara grayscale-image	11.3011×10^3

TABLE III: Mean square error of decrypted image (Figure 6(c)).

S.No.	Grayscale-image of size 256×256	MSE of decrypted image (Figure 6(c))
1.	Barbara grayscale-image	9.1140×10^{-27}

TABLE IV: Mean square error of incorrectly decrypted image (Figure 6(f)).

S.No.	Grayscale-image of size 256×256	Mean square error of Figure 6(f)
1.	Barbara grayscale-image	3.0133×10^3

after applying exact keys and correct arrangements of RHC. Now MSE value of Figure 6(f) is given in Table IV. This value is also very large, which represents if attackers know all exact keys, but not able to know about the correct arrangements of RHC with DWT, attacker cannot recover the original image. So our approach depends not only on the possible correct keys, but also on the correct arrangement of RHC.

6. Comparison of the proposed technique with existing methods

The proposed approach compares with Samson et al. (Samson and Sastry, 2012; Panduranga and Naveen, 2012) Samson et al. (Samson and Sastry, 2012) has taken hill cipher key as a involutory matrix (A^2=I). In (Samson and Sastry, 2012), no information about block matrix (sub images) is given, therefore for large size of image the hill cipher key size will also be large, and in the worst case the number of inputs for hill cipher key can be up to the image size for instance, a grayscale-image of size 512×512, the total number of inputs required for hill cipher key are 262144), so it is cumbersome for the encoder to perform encryption and decryption process, also no information is provided about mean square error analysis, histogram analysis, and robustness analysis of the approach. In addition to this, it is also time consuming to give enormous amount of inputs for large size images (as mentioned above). Panduranga H T et al. (Panduranga and Naveen, 2012) considered self invertible matrix (A^{-1}=A) for hill cipher key, which is also involutory matrix (A^2=I). In (Samson and Sastry, 2012; Panduranga and Naveen, 2012) decryption process depends only on key, if attacker knows the exact key then the image can be decrypted easily, while in our proposed approach hill cipher keys are chosen from special linear group over field

$\mathbb{F}$ ($SL_n(\mathbb{F})$) and the size of hill cipher keys depends on the choice of encoder. In this approach, if attacker knows about the all exact keys but no information about the correct arrangement of RHC then original image can not be recovered. Moreover, exact information of position (pre or post) of keys multiplication with image data are mandatory. Furthermore, arrangement of RHC and DWT are also prerequisite (for instance Figure 6(f)) for correct decryption.

Finally, after analyzing all the above mentioned ideas such as: key sensitivity analysis, key's space analysis of the proposed cryptosystem, robustness analysis, histogram analysis, mean square error analysis, and comparison of proposed approach with existing methods, we can conclude that proposed approach is more accurate and robust. So proposed approach can be used for secure transmission of grayscale-image data through insecure network.

7. Conclusion

We have proposed in this paper a novel approach for grayscale-image encryption and decryption using random hill cipher over $SL_n(\mathbb{F})$ associated with discrete wavelet transformation. In this technique, encryption process is elementary but decryption process is more unmanageable, especially in the case when there is no further information about the correct keys and the possible correct arrangement of RHC and DWT. Additionally, although, attacker knows about the all possible correct keys, but not able to know about the correct arrangement of RHC, attacker cannot decrypt the image correctly. As our basis of the approach depends not only on the possible correct keys, but also on the correct arrangement of RHC and DWT. Another advantage of this technique is, in hill cipher matrix multiplication is used and matrix multiplication is noncommutative so decryption process depends on pre or post multiplication of inverse hill cipher keys with encrypted image on the same position (pre or post) of hill cipher keys used in encryption process, if no information about the position is known, then attacker cannot recover the original image. We have also given comparison between proposed approach with other approaches. our correctly decrypted grayscale-image has a very low mean square error, this signifies that the method provides decryption with no information loss. So this approach can be used for transmission of grayscale-image data efficiently and securely through unsecured channels without loss of any information and intensity.

Acknowledgment

This work has been supported by Council of Scientific and Industrial Research (CSIR), New Delhi, Govt. of India, Under Grant no. F. No. 09/086(1068)/2010-EMR-I. The authors are very much thankful to the handling editor and reviewers for their true insightful comments and suggestions.

References

Abuturab, M. R. (2012a). Color image security system using double random-structured phase encoding in gyrator trans-form domain. *Appl. Opt.*, 51:3006–3016.

Abuturab, M. R. (2012b). Securing color image using discrete cosine transform in gyrator transform domain structured-phase encoding. *Opt Lasers Eng.*, 50:1383–1390.

Abuturab, M. R. (2012c). Securing color information using arnold transform in gyrator transform domain. *Opt Lasers Eng.*, 50:772–779.

Almedia, L. B. (1994). The fractional fourier transform and time-frequency representation. *IEEE Transaction on Signal Processing*, 42:3084–3091.

Antonini, M., Barlaud, M., Mathieu, P., and Daubechies, I. (1992). Image coding using wavelet transform. *IEEE Transaction on Image Processing*, 1:205–220.

Chen, H., Du, X., Liu, Z., and Yang, C. (2013). Color image encryption based on the affine transform and gyrator transform. *Opt Lasers Eng.*, 51:768775.

Chen, L. and Zhao, D. (2006). Optical image encryption with hartley transforms. *Opt Lett.*, 31:3438–3440.

Chen, L. and Zhao, D. (2008). Image encryption with fractional wavelet packet method. *Optik*, 119:286–291.

Daubechies, I. (1992). *Ten Lectures on Wavelets*. SIAM, Philadelphia, Pennsylvania, USA.

Gonzalez, R. C. and Woods, R. E. (2008). *Digital Image Processing*. Prentice Hall, Upper Saddle River, NJ.

Green, S. M. (1977). Generators and relations for the special linear group over a division ring. *Proceedings of the American Mathematical Society*, 62:229–232.

Hahn, J., Kim, H., and Lee, B. (2006). Optical implementation of iterative fractional fourier transform algorithm. *Opt Express*, 14:11103–11112.

Hennelly, B. and Sheridan, J. T. (2003). Optical image encryption by random shifting in fractional fourier domains. *Opt Lett.*, 28:269–271.

Liu, S., Mi, Q., and Zhu, B. (2001). Optical image encryption with multistage and multichannel fractional fourier domain filtering. *Opt Lett.*, 26:1242–1244.

Mallat, S. (1999). *A wavelet tour of signal processing*. Academic Press.

Muttoo, S. K., Aggarwal, D., and Ahuja, B. (2012). A secure image encryption algorithm based on hill cipher system. *Buletin Teknik Elektro dan Informatika*, 1:51–60.

Panduranga, H. T. and Naveen, K. S. K. (2012). Advanced partial image encryption using two-stage hill cipher technique. *International Journal of Computer Applications*, 60:14–19.

Pathak, R. S. (2009). *The Wavelet Transform*. Atlantis Press, World Scientific, Amsterdam, Paris.

Rosen, K. H. (1984). *Elementary Number Theory and Its Applications*. Pearson, New York.

Samson, C. and Sastry, V. U. K. (2012). An rgb image encryption supported by wavelet-based lossless compression. *IJACSA*, 3:36–41.

Singh, M., Kumar, A., and Singh, K. (2009). Encryption by using matrix-added, or matrixmultiplied input images placed in the input plane of a double random phase encoding geometry. *Opt Laser Eng.*, 47:1293–1300.

Stallings, W. (2006). *Cryptography and Network Security*. Prentice Hall, New Jersey.

Zhang, Y., Zheng, C. H., and Tanno, N. (2002). Optical encryption based on iterative fractional fourier transform. *Opt Commun.*, 202:277–285.