Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 1, pp. 161–183
DOI : 10.47974/JDMSC-2118

Association schemes in encrypting two dimensional data

Anuradha Sabharwal *
Department of Mathematics
University of Delhi
Delhi 110007
India

Pooja Yadav †
Department of Mathematics
Kamala Nehru College
University of Delhi
New Delhi 110049
India

R. K. Sharma §
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016
India

Abstract

A new Crypto-Stegano system is proposed using Random Matrix Transformation on relations of association schemes based on finite abelian groups associated with Arnold tranform and concealing the encrypted data within a randomly selected cover image. The proposed technique has been evaluated through comprehensive experimental results. Additionally, statistical tools are used to assess its performance. Furthermore, error analysis and key analysis have been carried out to ensure the technique's accuracy and reliability. Comparison results between existing schemes and the proposed techniques to validate the robustness have also been provided.

Subject Classification: *(2020) 05E30, 11T71.*

Keywords: *Association scheme, Arnold transform, Cryptography, Steganography.*

* *E-mail:* **anuradha.sabharwal@gmail.com (Corresponding Author)**
† *E-mail:* **iitd.pooja@gmail.com**
§ *E-mail:* **rksharmaiitd@gmail.com**

1. Introduction

With the quick advancement of networks and information technology, digital images are now being widely used and, serve as a vital source of information. Consequently, image data security and storage become crucial. Hence we propose a crypto-stegano system for encrypting both image and text data using random matrix transformation on the relations of association schemes based on finite abelian groups associated with the Arnold transform. The encrypted data is then hidden behind a cover image which is randomly selected. In the literature, various techniques have been studied to ensure the security of the data using different transformations such as [4, 6, 15, 18–21, 24].

Steganography allows us to conceal the secret data in a multimedia file for evading detection by an intruder. While various file formats are available, digital images are favored because of their prevalence on the Internet. Various embedding techniques for hiding the data have also been studied, such as [1–3, 11, 16, 30].

Using both steganography and cryptography techniques together enhances the security of the data [8, 23]. Hiding the original data in the edges of the cover image provides better imperceptibility [7, 29]. The papers [17, 23, 27, 28] proposed techniques for steganography and cryptography-based two-dimensional data security using some classical ciphers and transforms with LSBMR techniques. In the paper [22], a novel, simpler construction of a secret sharing scheme with a tree-like access structure was proposed. The paper focused on hierarchical secret sharing.

In the proposed method, multiple protection layers have been applied on the secret information by first encrypting it and then concealing the encrypted data. Two-dimensional data, such as an image or text file, are first converted into a cipher text using Random Matrix Transform (RMT) on relations of the association scheme, which in return is then scrambled using the Arnold transform. Finally, The encrypted data is then hidden in the LSB of the cover image, rendering it invisible to the human eye due to the minimal pixel value distortion and negligible impact on the image's histogram. As a result, we transmit sensitive information without the intruder noticing. However if they get suspicious from the cover image, the data is hard to decipher due to being doubly encrypted by association scheme cipher and the Arnold transform. Furthermore, the proposed crypto-stegano method can be employed as an imperceptible digital watermark, serving as a powerful tool for verifying and protecting copyright of data in the form of an image or .txt file format. It is

imperceptible, more secure, and robust than other methods. When data is inserted into the middle bits, authorized individuals can extract or retrieve it and decrypt it to verify the authenticity of the copyright symbol or text. We gain the benefit of data not being easily degraded or lost by many actions such as noise orÂ compressionÂ in the dataÂ by hiding itÂ in this way at middle bits rather than LSB. The data is thus constantly accessible but permanently labeled due to watermarking. There are various useful applications for digital watermarking such as image databases, medical imaging, digital cameras among others. The proposed cryptosystem enables secure transmission through an unsafe or unsecured network for two-dimensional data (colored images or any text file) of any dimensions.

2. Preliminary

Association schemes (AS), as initially proposed by Bose and Shimamoto [10], play a vital role in algebraic combinatorics. They find applications across multiple domains, including network analysis, error-correcting codes, algebraic structures, and combinatorial designs. Information security is a major concern these days. So we find applications of association schemes in cryptography. Below is a summary of the essential foundational literature and preliminaries on association schemes.

2.1 *Association Scheme*

Definition 1: Let Y be a finite set and $\mathcal{P}$ be a partition of the Cartesian product $Y \times Y$. Consider binary relations $S_0, S_1, \ldots, S_n$ defined on $\mathcal{P}$. The structure $\mathcal{A} = (Y, \mathcal{P})$ is called an association scheme with n-classes if it meets the following criteria:

(1) $S_0 = \{(a,b) : a,b \in Y\} \in \mathcal{P}$.

(2) For each relation $S \in \mathcal{P}$, the relation $S^* = \{(a,b) \mid (b,a) \in S\} \in \mathcal{P}$.

(3) If $(a,b) \in S_k$, then for any $c \in Y$, the number of elements c such that $(a,c) \in S_l$ and $(c,b) \in S_m$ is a constant denoted by p_{lm}^k, which does not depend on the specific choices of a and b for all integers $0 \le k,l,m \le n$.

The integers $\{p_{lm}^k\}_{0 \le k,l,m \le n}$ are known as the *parameters* or *intersection numbers* of the association scheme $\mathcal{A}$. If every relation S in $\mathcal{P}$ is symmetric $(S = S^*)$, then $\mathcal{A}$ is symmetric. Furthermore, if $p_{lm}^k = p_{ml}^k$ holds for all integers $0 \le k,l,m \le n$, it is termed a commutative association scheme. Define the set $aS = \{b \in Y \mid (a,b) \in S\}$ for any $a \in Y$ and $S \in \mathcal{P}$. The elements a and b in Y are called *kth associates* if $(a,b) \in S_k$ with the condition

that $a \neq b$. Notably, any symmetric association scheme inherently exhibits commutativity. For more fundamental results on association schemes, please refer to [32].

Sabharwal et al. [25, 26] have constructed non symmetric commutative association schemes for several groups and group rings. In [26], a non-symmetric association scheme has, in particular, been developed for the group $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$.

Theorem 2.1: *Let* $Y = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$, *where* $n_1 \leq n_2 \leq \ldots \leq n_r$ *and* $\gcd(n_1, n_2, \ldots, n_r) \neq 1$. *The relations* S_k *in* $\mathcal{P}$ *defined by*

$$S_k = \{(a,b) \mid b_r \equiv (k + a_r) \bmod n_r, b_s \equiv (k + t_s^{(k)} + a_s) \bmod n_s$$
$$\forall\, 1 \leq s \leq r-1 \mid a = (a_1, a_2, \ldots, a_r), b = (b_1, b_2, \ldots, b_r) \in Y\}$$

is a commutative association scheme that is non-symmetric and has parameters.

$$p_{lm}^k = \begin{cases} 1 & \text{if } k \equiv (l+m) \bmod n_r, \text{ and} \\ & \quad k + t_s^{(k)} \equiv (l + m + t_s^{(l)} + t_s^{(m)}) \bmod n_s \ \forall 1 \leq s \leq r-1 \\ 0 & \text{otherwise} \end{cases}$$

where $k = n_2 n_3 \cdots n_r t_1^{(k)} + n_3 n_4 \cdots n_r t_2^{(k)} + \cdots + n_r d_{r-1}^{(k)} + t_r^{(k)}$; $l = n_2 n_3 \cdots n_r t_1^{(l)} + n_3 n_4 \cdots n_r t_2^{(l)} + \cdots + n_r t_{r-1}^{(l)} + t_r^{(l)}$; $m = n_2 n_3 \cdots n_r t_1^{(m)} + n_3 n_4 \cdots n_r t_2^{(m)} + \cdots + n_r t_{r-1}^{(m)} + t_r^{(m)}$;

and $t_s^{(k)}, t_s^{(l)}, t_s^{(m)} \in \mathbb{Z}_{n_s} \ \forall\, 1 \leq s \leq r$.

For each $0 \leq k < n_1 n_2 \ldots n_r$, the relation $S_k^* = S_K$ can be established by analyzing the equations presented below:

$$\begin{aligned} K + k &\equiv 0 \bmod n_r \\ K + k + T_s + t_s &\equiv 0 \bmod n_s \qquad \forall 1 \leq s \leq r-1 \end{aligned}$$

where $k = n_2 n_3 \cdots n_r t_1 + n_3 n_4 \cdots n_r t_2 + \cdots + n_r t_{r-1} + t_r$ *and* $K = n_2 n_3 \cdots n_r T_1 + n_3 n_4 \cdots n_r T_2 + \cdots + n_r T_{r-1} + T_r$.

Proof: Refer [26].

In our proposed technique, we first encrypt two dimensional original data which is in the form of an image or a text data file by using association schemes over $\mathbb{Z}_n^r = \underbrace{\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n}_{r \text{ times}}$. In Theorem 2.1, every relation S_k is regarded as a mapping from $\mathbb{Z}_n^r$ to $\mathbb{Z}_n^r$. Thus, the association schemes on $\mathbb{Z}_n^r$ represents Vigenere Cipher.

Image Encryption/Decryption: The original RGB image of size $h \times w$ is first converted into text format by storing pixels. The pixels are given in matrix form and each matrix cell consists of 3 components which denote color saturation of Red, Green and Blue. The value in each component lies between 0 and 255. Let *R*, *G* and *B* are $h \times w$ matrices over $\mathbb{Z}_{256}$ which represents pixels of the image (red, green, blue). Now consider a single matrix *M* of order $h \times w$ over $\mathbb{Z}_{256} \times \mathbb{Z}_{256} \times \mathbb{Z}_{256}$. Each element x_{ij} of matrix *M* is a 3-tuple $(x_{ij}^{(1)}, x_{ij}^{(2)}, x_{ij}^{(3)})$ in which component $x_{ij}^{(1)}$, $x_{ij}^{(2)}$ and $x_{ij}^{(3)}$ is an $(i,j)^{th}$ element of *R*, *G* and *B* respectively. Let k_1 be the RMT key and k_2 be the encryption key between 1 and $256^3 - 1$. We consider the matrix

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

for RMT which is applied k_1 times on relations of AS. Consider AS over $\mathbb{Z}_{256}^3$ discussed in Theorem 2.1. Then by applying relation S_{k_2} on (x_{ij}, y_{ij}) where $y_{ij} = (y_{ij}^{(1)}, y_{ij}^{(2)}, y_{ij}^{(3)})$, we get the value of y_{ij}, which is the $(i,j)^{th}$ element of matrix *C*. Here each element y_{ij} of *C* is encrypted pixel value, where $1 \le i \le h$, and $1 \le j \le w$. Seperate the components of each element into 3 matrices R_1, G_1 and B_1 of order $h \times w$. With the help of these matrices we convert the text format of these encrypted pixels to color image and we get an encrypted image of size $h \times w$. For decryption process, let $S_{k_2}^* = S_l$. Therefore the decryption key is *l*. By applying RMT k_1 times on the relation R_l (Theorem 2.1) on (y_{ij}, z_{ij}) where $z_{ij} = (z_{ij}^{(1)}, z_{ij}^{(2)}, z_{ij}^{(3)})$, we get the value of z_{ij}, which is the $(i,j)^{th}$ element of matrix *D* (of order $w \times h$). Finally, the original image of size $h \times w$ is recovered.

Text data Encryption/Decryption: The plaintext message from the two dimensional text data file is first converted into integers and arranged in one dimensional matrix *M*. Then the encryption and decryption process is same as in previous case.

2.2 *Arnold Transformation*

The Arnold transformation, also referred to as the cat face transformation, was introduced by V. Arnold [5]. Considering an image of size $n \times n$, it transforms the position of a pixel from (a,b) to a new position (a',b') based on the equation (Equation (1)).

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} (\text{mod } n) \tag{1}$$

This transformation is periodic in nature and the upper bound of its period is $n^2/2$ [9, 13]. The arnold transform is applied repeatedly during the encryption process to produce jumbled data, and the number of iterations used serves as the key that must be known by the recipient. In order to decrypt data, the inverse arnold transform [11, 14] given by Equation (2) is used.

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} a' \\ b' \end{bmatrix} (\text{mod } n) \tag{2}$$

3. Proposed Approach for Cryptography and Steganography

Cryptography is a process of protecting important information and communications through encryption and decryption. Encryption process converts the information into cipher text with the help of encryption key so that it cannot be understood by the intruders. Steganography is the process of hiding information in another image or audio file. In this paper, we propose a technique for securing a color image by merging cryptography and steganography. In the proposed approach, we first encrypt the original two dimensional data that is, RGB image or text file by using RMT on relations of association scheme over $\mathbb{Z}_n^r$ to get first cipher image/text. The encrypted data is then further scrambled using the arnold transform, which makes the data difficult to decrypt. Finally, the double-encrypted data that has been retrieved is combined with a cover image by embedding it in the least significant bit (LSB) of the cover image. to eliminate any possibility of suspicion regarding the data. By using this method, AS crypto-stegano images can be created; the technique for doing so is discussed in Figure 1. A similar strategy is used to recover data from an AS crypto-stegano image as given in Figure 2.

3.1 *Encryption and Decryption of RGB image/text file by Cryptography over Association Scheme and Arnold Transform*

We first encrypt our original data A which is in the form of an RGB image or text file by using RMT on association scheme over $\mathbb{Z}_n^r$. Let (k_1, k_2, k_3) be the set of three encryption keys which is to be shared at the receiver's end. Here k_1 is used as RMT key applied on relations of association scheme over $\mathbb{Z}_{256}^3$ (defined in Section 2) relative to key k_2 to get new relations. These relations are further applied on A. Thereafter, in the second step arnold transformation is applied k_3 times to scramble the encrypted data. Here the number of iterations (k_3) act as the part of the

key. The final step involves reading the intermediate data in binary form and merging it with the RGB component of the cover image by placing these at the LSB of the image. Any significant change in the cover image cannot be noticed. The procedure for creating AS crypto-stegano image by this approach is discussed in Algorithm 1.

A similar procedure is used to retrieve the information from the AS crypto-stegano image which is described in Algorithm 2. After obtaining relevant information from an image, inverse of arnold transformation is applied k_3 times to descramble the image. Now we determine the decryption key l from the shared encryption key k_2 by using the defined association scheme, which is discussed in Section 2. Then applying RMT key k_1 on the relation S_l of the defined association scheme, we get the original data.

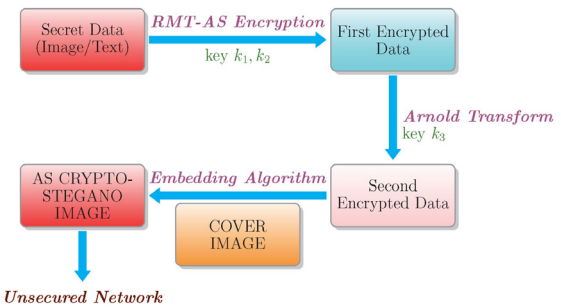


Figure 1

Block diagram for constructing AS Crypto-Stegano Image

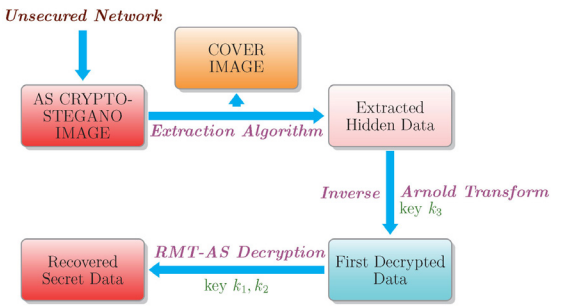


Figure 2

Block diagram for reconstructing secret data from AS Crypto-Stegano Image

Algorithm 1 Algorithm for Encryption Procedure for constructing AS Crypto-Stegano Image

1. **Input:** Secret data (Image/Text file) (A), Cover Image (C), RMT key (k_1), association scheme key (k_2), Arnold key (k_3)
2. **Output:** AS Crypto-Stegano Image
3. **procedure** Encryption
   (1) *Image:* Divide A into 3 matrices R, G, B with respect to red, green and blue components respectively.

   Text file: Convert the plaintext message from A into integers and arrange in one dimensional matrix M.

   (2) Find d_1, d_2, d_3 such that $k_2 = (256)^2 d_1 + (256) d_2 + d_3$.

   (3) Apply RMT k_1 times on relation S_{k_2} of association scheme over $\mathbb{Z}_{256}^3$ (as defined in Section 2).

   (4) *Image:* Apply new relation on R, G, B to obtain R_1, G_1, B_1 and concatenate these to get first encrypted data A_1.

   Text file: Apply new relation on M to obtain first encypted data A_1.

   (5) Scramble the above data A_1, by applying arnold transformation k_3 times (as in Equation 1) and obtain the second decrypted data E.

   (6) Store the bits of E at the least significant bits of the RGB channels of C.
4. **end procedure**

Algorithm 2 Algorithm for Retrieving Secret Data from AS Crypto-Stegano Images

1. **Input:** AS Crypto-Stegano Image (S), RMT key (k_1), association scheme key (k_2), Arnold key (k_3)
2. **Output:** Recovered secret data
3. **procedure** Decryption
   (1) Retrieve the concealed data from RGB components of S.

   (2) Descramble this data by applying inverse of arnold transformation k_3 times (as in (2)) and obtain A_1.

   (3) Obtain the decryption key l from the key k_2, as outlined in Section 2.

(4) Determine D_1, D_2, D_3 such that $l = (256)^2 D_1 + (256)D_2 + D_3$.

(5) Apply RMT k_1 times on the relation S_l of association scheme over $\mathbb{Z}_{256}^3$ (as defined in Section 2)

(6) *Image:* Divide A_1 into 3 matrices R_1, G_1, B_1 with respect to red, green and blue components respectively then apply new relation on R_1, G_1, B_1 to obtain R, G, B.

Text file: Apply new relation on A_1 to obtain M.

(7) *Image:* Concatenate R, G, B to get the correctly decrypted image.

Text file: Convert data M into text to get the correctly decrypted text data.

4. **end procedure**

4. Experimental Results

This section examines the computer simulation and experimental analysis for secure transmission of two dimensional data by statistically

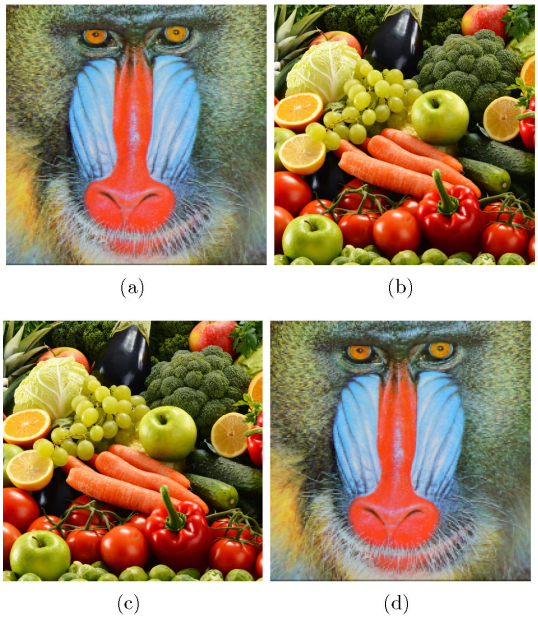


Figure 3

(a) Image of Baboon (size 204 × 204 × 3); (b) cover image; (c) AS crypto-stegano image; (d) extracted and correctly decrypted image

analysing the proposed approach. This scheme is carried out in MATLAB R2021b, which is run on a laptop with the specifications 12th Gen Intel(R) Core(TM) i7-1255U CPU @ 1.70 GHz. For analysis, we have chosen two different images, 'Lena' and 'Baboon' of size 256×256 and 204×204 respectively and one text file. The two different cover images are shown in Figure 3(b) and Figure 4(b) respectively. The secret data is encrypted by using RMT, association scheme and arnold transform. Furthermore, on hiding this data in the LSB of cover image, AS crypto-stegano image is obtained as shown in Figure 3 to 5(c). We observe that the extracted data (see Fiogure 3 to 5(d)) showed no perceptible distortion. The analysis of these images have been discussed in regards to their Peak Noise-to-Signal Ratio (PNSR), Mean Square Error (MSE), pixel intensity, histogram analysis, correlation graphs, Correlation Coefficient (CC), Unified Average Changing Intensity (UACI) and the Change Rate of Number of Pixels (NPCR), for the cryptosystem's robustness.

4.1 *Histogram Analysis*

The visual depiction of an image's frequency with its pixel intensity value is the histogram. It plays a vital role in ensuring the strength of the cryptosystem. The histograms and pixel intensity correlation graphs for

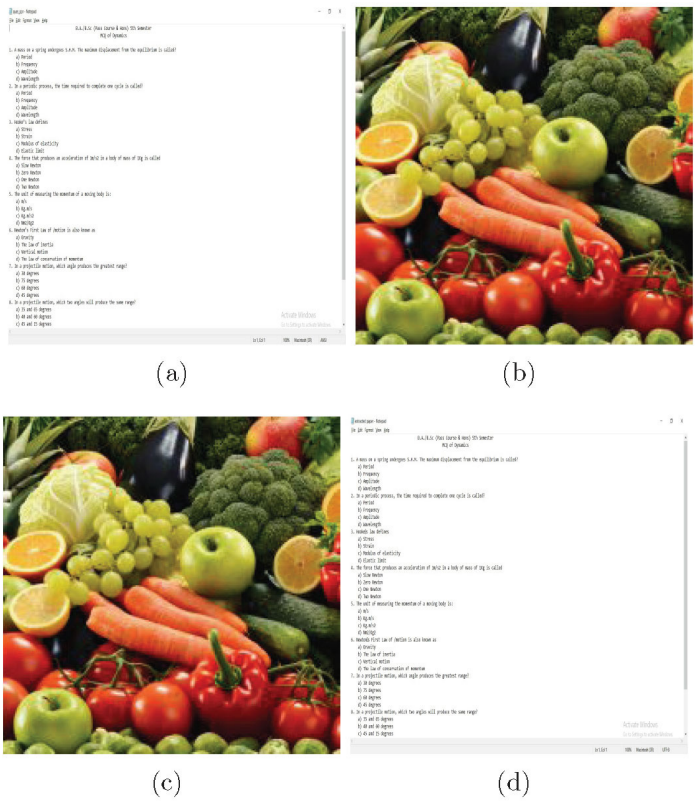
Figure 4

(a) Image of Lena (size 256 × 256 × 3); (b) cover image; (c) AS crypto-stegano image; (d) extracted and correctly decrypted image

the red, green, and blue components of the original image and extracted image for Figures 3 and 4 are given in Figures 6-8 and Figures 9-11 respectively, from which we can analyse that the histogram of original data is similar to the histogram of the recovered data. This also represents that the secret data is fully recovered after applying the correct keys.

5. Error Analysis

This section discusses the examination of the AS crypto-stegano image and the cover image for Figures 3 to 5 in regards to their PNSR, MSE, CC, UACI and NPCR values, given in Table 1 for the cryptosystem's robustness.



(a) (b)

(c) (d)

Figure 5

(a) Text document; (b) cover image; (c) AS crypto-stegano image; (d) extracted and correctly decrypted text document

5.1 *Mean Square Error*

The MSE which quantifies the maximum deviation for the red, green, blue channels of the original and reconstructed images is determined according to the formula

$$\mathrm{MSE} = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} [\,| f(i\Delta x, j\Delta y) - f_0(i\Delta x, j\Delta y)|^2].$$

Here, h and w represent the pixel count, while Δx and Δy denote the pixel dimensions in an RGB image.

The MSE between the original and the extracted image in Figures 3 and 7 for R, G, B channels are shown in table:combined_analysis. The precise retrieval of the original image without any loss or distortion of information is indicated by the fact that these values are zero. The values of MSE in the table depict that the crypto-stegano image resembles with the cover image for all the data in Figures 3 to 5.

5.2 *Peak Signal-to-Noise Ratio (PSNR)*

To assess the peak error between the original and reconstructed images, the PSNR is computed using the following formula:

$$\mathrm{PNSR} = 10 \cdot \log_{10}\left(\frac{\mathrm{MPV}_I^2}{\mathrm{MSE}}\right),$$

where MPV_I denotes the maximum pixel value that the image can attain.

Table 1 shows that the PNSR values of original image and the extracted image in Figs. 3 and 7 for R, G, B channels are infinity which indicates that correct information is retrieved without any loss or error of data. The elevated PNSR values of both the crypto-stegano image and the cover image for text data in Figures 3 to 5 as shown in the table indicate the similarity between these images.

5.3 *Correlation Coefficient*

The CC between the original and reconstructed images (encrypted and decrypted) is calculated according to the formula

$$\mathrm{CC} = \frac{\Sigma_p \Sigma_q (u_{pq} - \overline{u})(v_{pq} - \overline{v})}{\sqrt{[\Sigma_p \Sigma_q (u_{pq} - \overline{u})]^2 [\Sigma_p \Sigma_q (v_{pq} - \overline{v})]^2}}$$

where $\overline{u}$ and $\overline{v}$ are mean of original image and reconstructed image respectively. CC between two images vary from –1 to +1. The value of CC

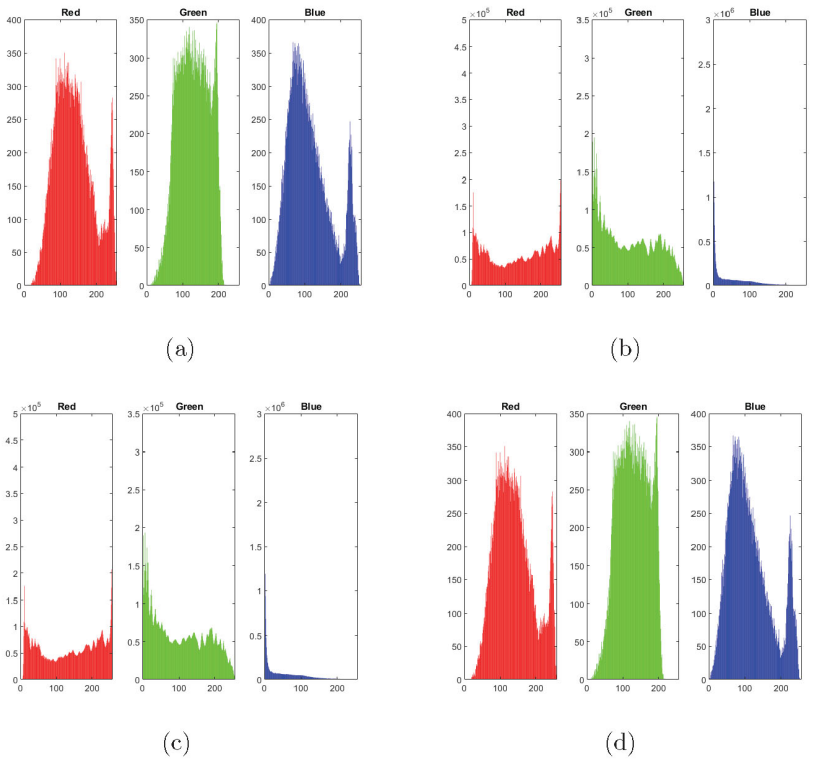


Figure 6

(a) Histogram of Baboon original image (b) Histogram of cover image (c) Histogram of cryptostegano image (d) Histogram of extracted image

+1 indicates a substantial positive linear connection between the two images and the value –1 indicates a negative relationship between the images. The value close to 0 indicates no relationship between two images.

5.4 *Number of Pixel Change Rate*

The NPCR measures the different pixel numbers between the reconstructed image and the original image. Let the original and reconstructed image be represented by $A(m,n)$ and $B(m,n)$ respectively. The formula for computing NPCR between the two images is expressed as:

$$\text{NPCR} = \frac{\Sigma_m \Sigma_n e(m,n)}{h \times w} \times 100\%$$

where

$$e(m,n)=\begin{cases}1 & \text{if } A(m,n)\neq B(m,n),\\ 0 & \text{if } A(m,n)=B(m,n)\end{cases}$$

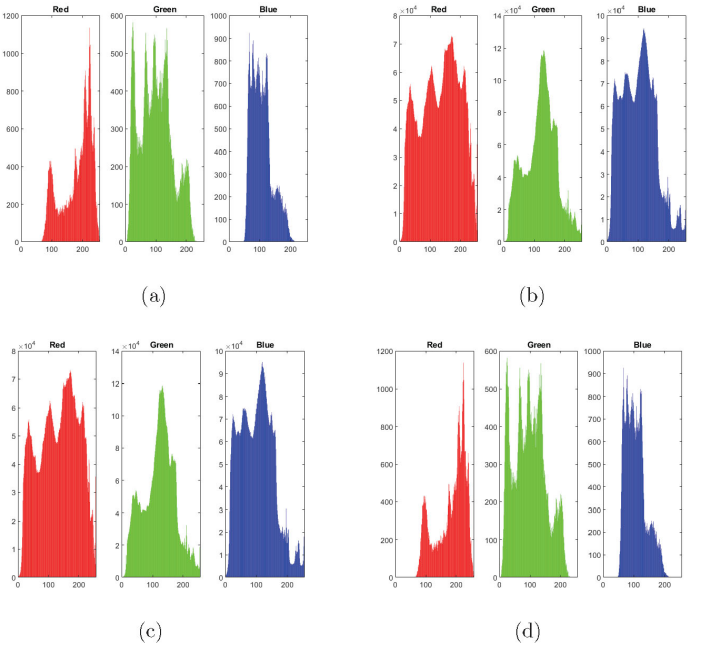


Figure 7

(a) Histogram of Fig. 4(a) (b) Histogram of Fig. 4(b) (c) Histogram of Fig. 4(c) (d) Histogram of Fig. 4(d)

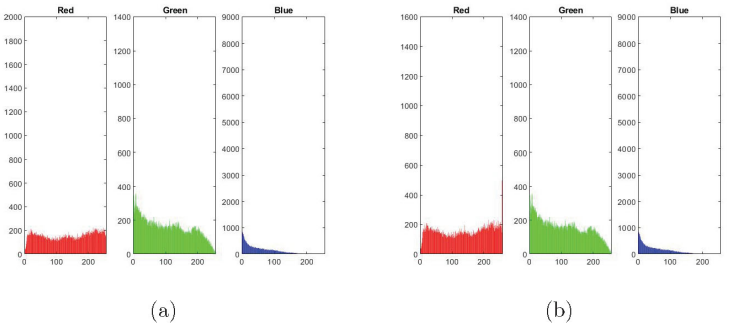


Figure 8

(a) Histogram of Fig. 5(b) (b) Histogram of Fig. 5(c)

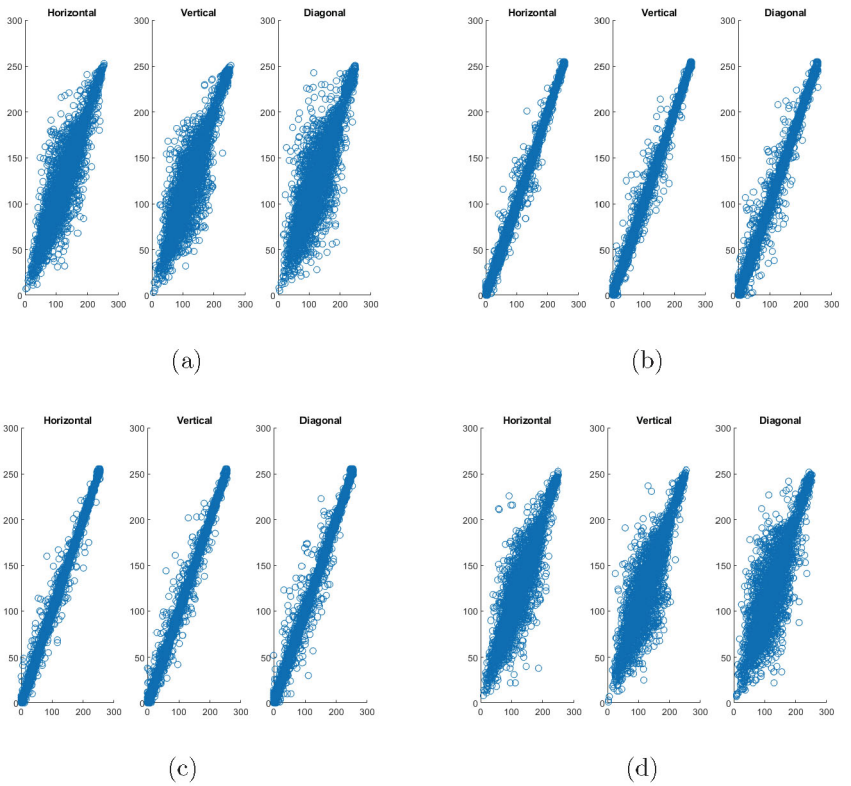


Figure 9

(a) Pixel intensity of Fig. 3(a) (b) Pixel intensity of Fig. 3(b) (c) Pixel intensity of Fig. 3(c) (d) Pixel intensity of Fig. 3(d)

5.5 *Unified Average Changing Intensity (UACI)*

To quantify the mean differences in pixel brightness between the original and reconstructed images, UACI is calculated using the following formula:

$$\mathrm{UACI} = \frac{1}{h \times w} \sum_{m} \sum_{n} \frac{|A(m,n) - B(m,n)|}{255} \times 100\%$$

5.6 *Key Space Analysis*

In cryptography, key space refers to the maximum possible size of a key; as a result, key space depends on the key length. In this paper, individual analysis have been carried out to verify the strength of the

Table 1
Statistical evaluations for various image comparisons

Channel	NPCR	UACI	MSE	PNSR	CC
Figure 3(a) and Figure 3(d)					
Red	0	0	0	∞	1
Green	0	0	0	∞	1
Blue	0	0	0	∞	1
Figure 3(b) and Figure 3(c)					
Red	1.0898	0.0043	0.0109	67.7575	1
Green	1.0826	0.0042	0.0108	67.7860	1
Blue	1.0804	0.0042	0.0108	67.7950	1
Figure 4(a) and Figure 4(d)					
Red	0	0	0	∞	1
Green	0	0	0	∞	1
Blue	0	0	0	∞	1
Figure 4(b) and Figure 4(c)					
Red	2.1473	0.0084	0.0215	64.8119	1
Green	2.1503	0.0084	0.0215	64.8059	1
Blue	2.1568	0.0085	0.0216	64.7926	1
Figure 5(b) and Figure 5(c)					
Red	13.5164	0.0530	0.1352	56.8222	1
Green	0	0	0	∞	1
Blue	0	0	0	∞	1

cryptosystem in case of an attack. Cryptography over association scheme uses encryption key to encrypt the data. Even if the attacker knows the key used for encryption, they cannot access the underlying data easily. From the encryption key, subkey is calculated using the proposed algorithm. If we take the encryption key to be 15888413, its subkey will be $[242\ 112\ 29]$. The value of subkey is in uint8, therefore key space is $(256)^3$, that is, 1.6777216×10^7.

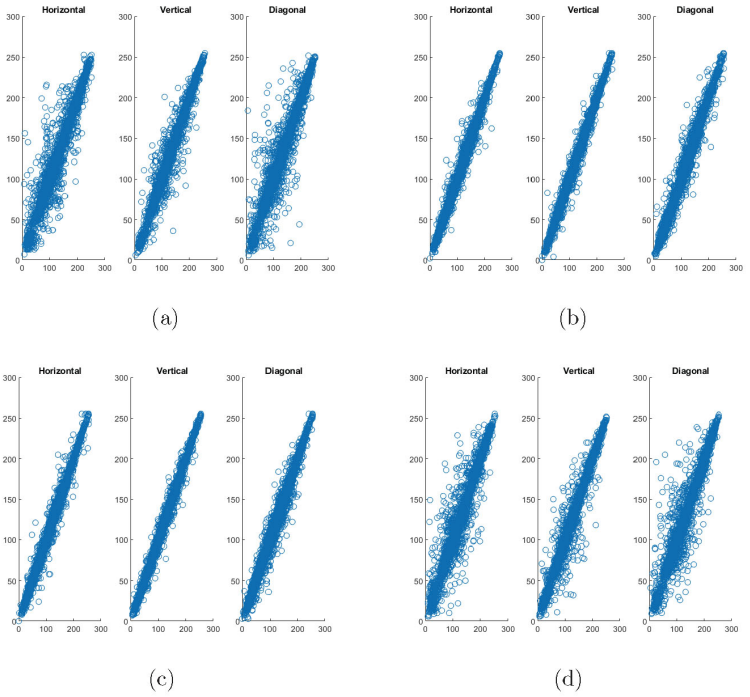


Figure 10

(a) Pixel intensity of Fig. 4(a) (b) Pixel intensity of Fig. 4(b) (c) Pixel intensity of Fig. 4(c) (d) Pixel intensity of Fig. 4(d)

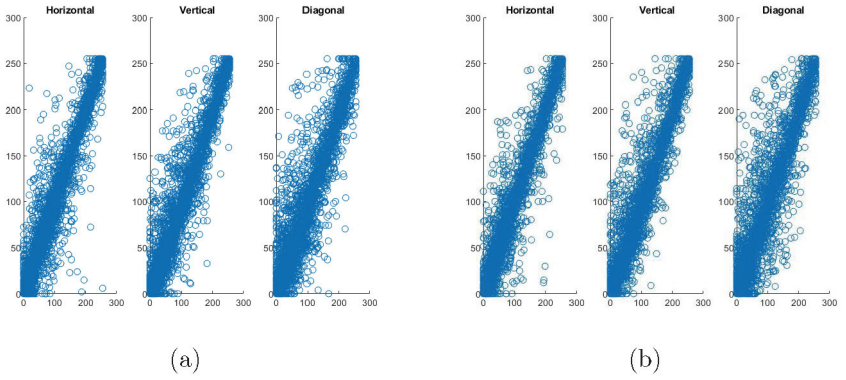


Figure 11

(a) Pixel intensity of Fig. 5(b) (b) Pixel intensity of Fig. 5(c)

5.6.1 Key Sensitivity Analysis

One of the most crucial factors that dictate the robustness of any security system is the key sensitivity. High key sensitivity ensures greater security of the cryptosystem, which means the sensitive information cannot be extracted without possession of the exact key. In the proposed method, the original data cannot be recovered in case any discrepancy is detected during the decryption stage.

Even if there is a slight change in decryption key, for example: if key is 14888413 instead of 15888413, then the changed subkey is [227 45 22] which is different from [242 112 29]. The decryption keys calculated from encryption key and subkey will be changed, which results in corrupted and damaged output. The original data can be recovered only if the key utilized during the decryption process matches the original key precisely.

6. Comparison

This section compares the security of our proposed cryptosystem with that of the existing schemes [2, 4, 6, 8, 11, 18, 24, 28, 30]. Majority of techniques proposed in the past have provided steganography [11, 30, 31] for image data. The techniques [4, 6, 12, 18, 24] render security mainly by using cryptographic methods. The AS crypto-stegano methodology, which has been proposed, uses steganographic and cryptographic methods to secure both image and text data. This method employs association schemes on the group $\mathbb{Z}_n^r$ for encryption, introducing a novel approach that has not been previously applied in cryptography.

Abdulla et al. [2], Tang et al. [30] and Chen et al. [11] developed steganographic techniques aimed at safeguarding 2D information. By disintegrating the pixel intensity value into 16 virtual bit planes suitable for embedding, Abdulla et al. [2] introduced a data hiding method with improved stego-image quality. Tang et al. [30] proposed multilayer embedding technique for hiding high capacity data and Chen et al. [11] presented a technique for hiding color image where the RGB components of the image are initially scrambled using arnold transform and then hidden in fractional fourier domain through Gerchberg-Saxton algorithm. The techniques [2, 11] are ideal for image data security whereas technique [30] is suitable for security for image as well as text data. These techniques [2, 11, 30] offer a single layer security for the secret data. The proposed AS crypto-stegano technique, however, uses steganography and cryptography

to transmit two-dimensional data securely, and it is appropriate for both image and text data files.

Abuturab [4], Kumar et al. [18], Mishra et al. [24], and Arora et al. [6] have designed algorithms for securing color images using cryptography through the processes of encoding and decoding. Abuturab[4] applied gyrator transforms and DCT with the help of arnold transform to secure the color image data. Kumar et al. [18] presented symmetric key cryptosystem that is concerned with the security of color image data using RMAC associated with discrete wavelet transform for red, green and blue components of the color image. The keys and arrangement of RMAC parameters for the security of RGB image data are also discussed in the scheme [18]. Mishra et al.[24] have designed image encryption and decryption algorithm using RSA cryptosystem with 2-D discrete wavelet transform. Arora et al. in their paper [6], have cryptanalyzed an image encryption scheme based on the arnold transformation, logistic map and word-oriented feedback shift register. These methods [4, 6, 18, 24] are appropriate solely for securing image data. Additionally, the encryption of data transmitted over an unsecure network may raise concerns, as an attacker might recognize that the data is protected by a cryptosystem [23]. Consequently, the attacker will use some cryptanalysis to decrypt the secret data. Whereas the proposed AS crypto-stegano technique uses both cryptography and steganography for secure transmission of image and text data file in an insecure network and the AS crypto-stegano Images that are transmitted are unremarkable and do not attract any unsolicited attention. The algorithm designed by Abuturab [4] for image security relies solely on keys. If an attacker discovers these keys, the secret data may be decrypted easily. The proposed AS crypto-stegano technique uses RMT on association schemes on the group $\mathbb{Z}_n^r$ for encryption followed by scrambling using arnold transform. Ultimately, the doubly encrypted data is concealed within the cover image. It is very difficult for an intruder to intercept the message without the knowledge of the exact key and algorithm used for this cryptosystem. Even if the keys are known to the intruder, the keys cannot be applied directly to decrypt without knowing which algebraic structure has been used. The AS crypto-stego images obtained by this technique are highly imperceptible.

Using steganography and cryptography, Sharma et al.[28] and Balkrishan et al.[8] have developed algorithms for the security of two-dimensi-onal data. The cryptosystem used in [8] provide a multilayer security for the secret data and the technique [28] uses affine transform and DCT for encryption and LSB method for hiding the encrypted data

Table 2
Comparison of existing schemes and proposed technique

Schemes	Technique Used	Data type	PNSR (in dB)	Embedding rate	Data retrieval
Abuturab [4]	Cryptography	Image	-	-	lossy
Tang et al. [30]	Steganography	Image and Text file	36.98	1.2	lossless
Chen et al. [11]	Steganography	Image	45.75	1	lossy
Balkrishan et al. [8]	Cryptography and Steganography	Image and Text file	42.373	-	lossless
Sharma et al. [28]	Cryptography and Steganography	Image and Text file	51.16	0.75	lossless
Proposed technique	Cryptography and Steganography	Image and Text file	51.19	0.99	lossless

behind cover image. Table 2 displays comparison of some existing schemes with our proposed AS crypto-stegano technique on the basis of results and error analysis done using image of Mandril of size 256×256 as cover image. From this table we can see that the average value of PNSR for the proposed technique is higher than for techniques [8, 28]. Table 2 compares the embedding rate of several techniques with the proposed technique and shows that the proposed AS crypto-stegano technique achieves higher embedding rate, that is, higher embedding capacity. The proposed AS crypto-stegano technique is lossless and is more robust and appropriate as compared to the above existing techniques.

7. Conclusion

In this paper, a new technique has been proposed using association scheme for secure transmission of image and text data. Experimental results have been obtained to examine statistical and error analysis which verify the appropriateness of the proposed technique for sending information securely through open network. Comparison between existing and proposed techniques is also provided in support of the robustness of this approach. It is expected that this approach will give a new direction in

this area with a different algebraic structure (association scheme). Further, this scheme can also be applied for safe and secure transmission of audio and video data.

References

[1] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, "Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 17799–17823 (2019).

[2] A. A. Abdulla, H. Sellahewa, and S. A. Jassim, "Steganography based on pixel intensity value decomposition," in *Mobile Multimedia/Image Processing, Security, and Applications 2014*, vol. 9120, pp. 19–27 (2014).

[3] A. A. Abdulla, Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography, Ph.D. dissertation (2015).

[4] M. R. Abuturab, "Securing color information using Arnold transform in gyrator transform domain," *Optics and Lasers in Engineering*, vol. 50, no. 5, pp. 772–779 (2012).

[5] V. I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics*, vol. 9, Benjamin (1968).

[6] A. Arora and R. K. Sharma, "Cryptanalysis and enhancement of image encryption scheme based on word-oriented feedback shift register," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16679–16705 (2022).

[7] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46, pp. 42–51 (2017).

[8] J. Balkrishan and A. P. Singh, "Concealing data in a digital image with multilayer security," *Multimedia Tools and Applications*, vol. 75, no. 12, pp. 7045–7063 (2016).

[9] J. Bao and Q. Yang, "Period of the discrete Arnold cat map and general cat map," *Nonlinear Dynamics*, vol. 70, no. 2, pp. 1365–1375 (2012).

[10] R. C. Bose and T. Shimamoto, "Classification and analysis of partially balanced incomplete block designs with two associate classes," *Journal of the American Statistical Association*, vol. 47, no. 258, pp. 151–184 (1952).

[11] H. Chen, X. Du, Z. Liu, and C. Yang, "Optical color image hiding scheme by using Gerchberg–Saxton algorithm in fractional Fourier domain," *Optics and Lasers in Engineering*, vol. 66, pp. 144–151 (2015).

[12] L. Chen and D. Zhao, "Color image encoding in dual fractional Fourier wavelet domain with random phases," *Optics Communications*, vol. 282, no. 17, pp. 3433–3438 (2009).

[13] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *The American Mathematical Monthly*, vol. 99, no. 7, pp. 603–614 (1992).

[14] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognition*, vol. 41, no. 12, pp. 3572–3581 (2008).

[15] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402 (2019).

[16] C. Kim, D. Shin, L. Leng, and C.-N. Yang, "Separable reversible data hiding in encrypted halftone image," *Displays*, vol. 55, pp. 71–79 (2018).

[17] C. Kim, C.-N. Yang, and L. Leng, "High-capacity data hiding for ABTC-EQ based compressed image," *Electronics*, vol. 9, no. 4, p. 644 (2020).

[18] M. Kumar, D. C. Mishra, and R. K. Sharma, "A first approach on an RGB image encryption," *Optics and Lasers in Engineering*, vol. 52, pp. 27–34 (2014).

[19] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," *Optics Express*, vol. 18, no. 11, pp. 12033–12043 (2010).

[20] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color image encryption by using Arnold transform and colorblend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128 (2011).

[21] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22023–22043 (2019).

[22] G. Meriem and S. Bouroubi, "A new ideal secret sharing scheme based on a tree," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1–18 (2021).

[23] D. C. Mishra, H. Sharma, R. K. Sharma, and N. Kumar, "A first cryptosystem for security of two-dimensional data," *Fractals*, vol. 25, no. 01, p. 1750011 (2017).

[24] D. C. Mishra, R. K. Sharma, M. Kumar, and K. Kumar, "Security of color image data designed by public-key cryptosystem associated with 2D-DWT," *Fractals*, vol. 22, no. 04, p. 1450011 (2014).

[25] A. Sabharwal and P. Yadav, "Association schemes over some finite group rings," in *Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy*, pp. 13–23 (2022).

[26] A. Sabharwal, P. Yadav, and R. K. Sharma, "Association schemes for some finite group rings II," *Communications on Applied Nonlinear Analysis* (2024).

[27] H. Sharma, D. C. Mishra, R. K. Sharma, and N. Kumar, "Multi-image steganography and authentication using crypto-stego techniques," *Multimedia Tools and Applications*, vol. 80, no. 19, pp. 29067–29093 (2021).

[28] H. Sharma, D. C. Mishra, R. K. Sharma, and N. Kumar, "Crypto-stego system for securing text and image data," *International Journal of Image and Graphics*, vol. 18, no. 04, p. 1850020 (2018).

[29] S. Sun, "A novel edge-based image steganography with 2k correction and Huffman encoding," *Information Processing Letters*, vol. 116, no. 2, pp. 93–99 (2016).

[30] M. Tang, J. Hu, and W. Song, "A high capacity image steganography using multi-layer embedding," *Optik*, vol. 125, no. 15, pp. 3972–3976 (2014).

[31] C.-N. Yang, J.-F. Ouyang, and L. Harn, "Steganography and authentication in image sharing without parity bits," *Optics Communications*, vol. 285, no. 7, pp. 1725–1735 (2012).

[32] P.-H. Zieschang, An Algebraic Approach to Association Schemes, Springer (2006).

Received January, 2024