Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 1912603, 9 pages
https://doi.org/10.1155/2022/1912603

Research Article

A Novel Image Encryption Technique Based on Cyclic Codes over Galois Field

Muhammad Asif[1], **Joshua Kiddy K. Asamoah**[2], **Mohammad Mazyad Hazzazi**[3], **Adel R. Alharbi**[4], **Muhammad Usman Ashraf**[5] and **Ahmed M. Alghamdi**[6]

[1]*Department of Mathematics, University of Management and Technology, Sialkot Campus, Sialkot, Pakistan*
[2]*Department of Mathematics, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana*
[3]*Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia*
[4]*College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia*
[5]*Department of Computer Science, GC Women University, Sialkot, Pakistan*
[6]*Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*

Correspondence should be addressed to Joshua Kiddy K. Asamoah; jkkasamoah@knust.edu.gh

Received 10 December 2021; Revised 25 December 2021; Accepted 28 December 2021; Published 8 February 2022

Academic Editor: Ahmed Mostafa Khalil

In the modern world, the security of the digital image is vital due to the frequent communication of digital products over the open network. Accelerated advancement of digital data exchange, the importance of information security in the transmission of data, and its storage has emerged. Multiple uses of the images in the security agencies and the industries and the security of the confidential image data from unauthorized access are emergent and vital. In this paper, Bose Chaudhary Hocquenghem (BCH) codes over the Galois field are used for image encryption. The BCH codes over the Galois field construct MDS (maximum distance separable) matrices and secret keys for image encryption techniques. The encrypted image is calculated, by contrast, correlation, energy, homogeneity, and entropy. Histogram analysis of the encrypted image is also assured in this paper. The proposed image encryption scheme's security analysis results are improved compared to the original AES algorithm. Further, security agencies can utilize this work for their confidential image data.

1. Introduction

Nowadays, cryptography plays a primary role in information security and embedded system design. The use of mobile communication and the Internet rapidly increases and occupies wide-ranging areas in daily life. There is an increase in the number of users and unauthorized users who try to fetch data illegally, causing data security issues. To solve this problem, encrypted data is generated, unreadable for unauthorized users. Cryptography is the science of information security which secures the data while it is stored or transmitted. Claude Shannon [1] describes the two basic properties, diffusion and confusion for the design of block ciphers in a communication theory of secrecy systems. Substitution boxes are the block ciphers' only nonlinear component that confuses the ciphertext. Many researchers have created highly nonlinear and influential S-boxes to provide secure communication. The diffusion layer has been neglected in cryptographic research, juxtaposed to confusion layers for a long time. The replacement of the permutation layer of substitution-permutation networks (SPNs) by a diffusion layer enhances the avalanche property of the block cipher. It makes the cipher's resistance to linear and differential cryptanalysis explained by Heys and Tavare in [2–4]. Thus, MDS (maximum distance separable) matrices provide diffusion in cryptographic algorithms and are the main component in the architecture of block ciphers to make resistance against the linear and differential cryptanalysis. The keystream generator is added to the AES algorithm to improve encryption performance [5]. The modified AES

algorithm is explained in [6]. The image and video encryption based on chaos with security analyses are presented in [7]. The existing image encryption techniques are reviewed in [8]. The article explains the simulation of image encryption using the AES algorithm [9]. Using Gaussian Distribution Cryptographic Substitution Box is designed in [10]. The present age ciphers SHARK [11], Advanced Encryption Standard (AES) [12], and Twofish [13,1 4] have a diffusion layer that depends on the mix column operation step. The least weight maximum distance separable (MDS) matrices constructed by comprehensive search from the companion matrices are given in [11]. Zhang et al. [15] presented chaotic research encryption, combining the image and DES encryption algorithm. Logistic chaos sequencer is used in the new encryption scheme to create the pseudorandom sequence and then makes double-time encryption with improvements in DES. Their results show high security and encryption speed and high starting value sensitivity. Shah et al. [16] propose a criterion to examine the prevalent S-boxes and study their strength and weaknesses to define their correctness in image encryption applications. The bases of the AES key expansion image encryption scheme are explained in [17]. Error-correcting codes, particularly BCH codes, are helpful to reduce the rate of decryption failure [18]. Walter et al. [18] analyze the decoding algorithm of the BCH code and design a constant-time version of the BCH decoding algorithm. Asif et al. [19] constructed BCH codes with a computational approach and applied those codes in data security. Different image encryption techniques are utilized by various authors [20–24].

The modified AES algorithm for image and text encryption based on bit permutation instead of mixed column operation is presented in [25]. But we used BCH codes to construct MDS matrices and private keys to secure image data. The proposed criteria use correlation analysis, entropy analysis, homogeneity analysis, contrast analysis, energy analysis, and histogram analysis. This paper presents a new symmetric algorithm based on BCH codes over the Galois field. MDS matrices and secrete keys of the proposed algorithm are derived from the generator polynomials of the respecting BCH codes over the Galois field. We furnished a novel technique for constructing the building components of the block cipher. The rest of the paper is organized as follows: some basic concepts of coding theory and cryptography are presented in Section 2. Section 3 contains the proposed algorithm and its components with an example. Section 4 has statistical analyses of the encrypted image by the proposed algorithm. Conclusion and future application are discussed in Section 5.

2. Preliminaries

2.1. Cyclic Codes. The linear mapping $\rho: \mathcal{F}^n \longrightarrow \mathcal{F}^n$ is defined by

$$\rho(b_1, b_2, b_3, \ldots, b_n) = (b_n, b_1, b_2, b_3, \ldots, b_{n-1}). \tag{1}$$

It is called a cyclic shift. A linear code $C \subset \mathcal{F}^n$ is called cyclic code if

$$\rho(b) \in C, \quad \forall b \in C. \tag{2}$$

2.2. Irreducible Polynomial. A polynomial is called irreducible if it cannot be written as the product of two polynomials. For example, $P(x) = x^3 + x + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}_2$.

2.3. Primitive Polynomial. An irreducible polynomial $P(x)$ is primitive polynomial if α is a primitive root of $P(x)$, that is,

$$\begin{aligned} P(\alpha) &= 0, \\ \alpha^{p^m - 1} &= 1, \end{aligned} \tag{3}$$

where p is prime and m is the degree of the irreducible polynomial. For example, $P(x) = x^4 + x + 1$ is a primitive, irreducible polynomial over $\mathbb{Z}_2$.

2.4. Theorem [26]. Let $\alpha \epsilon \mathcal{F}_{q^m}$. Then, $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ have the same minimal polynomial over $\mathcal{F}_q$.

2.5. BCH Code. BCH codes are cyclic linear codes. Let c, d, q, n be positive integers such that $2 \le d \le n$, q is a power of some prime number, and $(n, q) = 1$. Let m be the least positive integer such that

$$q^m \equiv 1 \,(\mathrm{mod} n). \tag{4}$$

Thus, $n | q^m - 1$. Let α be a primitive nth root of unity in F_{q^m}. Let $m_i(x) \in F_q[x]$ denote the minimal polynomial of α^i. Let $g(x)$ be the product of distinct minimal polynomials among $m_i(x)$, $i = c, c+1, \ldots, c+d-2$, that is,

$$g(x) = l \cdot c \cdot m\{m_i(x) | i = c, c+1, \ldots, c+d-2\}. \tag{5}$$

Since $m_i(x)$ divides $y^n - 1$ for each i, it follows that $g(x)$ divides $x^n - 1$. Let C be a cyclic code with generator polynomial $g(x)$ in the ring $F_q[x]_n$. Then, C is called a BCH code of length n over F_q with designed distance d.

Nowadays, BCH codes have many applications; BCH codes are used in satellite communication, hard disc, compact disc, storage systems, and data security.

2.6. Theorem [26]. Let C be BCH code of length n over $\mathcal{F}_q$ with designed distance d. Then

$$C = \left\{c(x) \in \mathcal{F}_q[x]_n : c\left(\alpha^j\right) = 0, \quad \forall j = c, c+1, c+2, \ldots, c+d-2\right\}. \tag{6}$$

2.7. Theorem [26]. Let C be a BCH code of designed distance d. Then,

$$d(c) \ge d, \tag{7}$$

where $d(c)$ is the minimum distance and d is designed to distance.

2.8. Galois Field. A finite field is called Galois field. Galois field extension of the polynomial ring $\mathbb{Z}_p[x]$ is

$$\mathrm{GF}(p^m) = \frac{\mathbb{Z}_p[x]}{\langle P(x)\rangle}, \tag{8}$$

where p is prime and $P(x)$ is a primitive, irreducible polynomial of degree m over $\mathbb{Z}_p$. Therefore,

$$\mathrm{GF}(p^m) = \left\{a_0 + \cdots + a_{m-1}x^{m-1} : a_i \in \mathbb{Z}_{p^i}, \quad \forall i = 0, 1, \ldots m-1\right\}. \tag{9}$$

2.9. MDS (Maximum Distance Separable) Matrices. MDS (Maximum Distance Separable) matrices have many applications in data security and channel coding. They create diffusion in block cipher data. These matrices are constructed by using the elements of a finite field. MDS matrices are invertible because the inverse of the MDS matrix is used for the decryption of data. Nowadays, Reed Solomon codes and BCH codes construct MDS matrices.

2.10. Proposition. If $l \times l$ MDS matrices can be generated from BCH code $[n, k, d]$ over Galois field $\mathrm{GF}(2^m)$ then m, l, and d must satisfy

$$\begin{aligned} m &\geq \log_2 2l + 1, \\ l + 1 \leq d &\leq 2^m - l. \end{aligned} \tag{10}$$

2.11. Proposition. Let $g(x)$ be the generator polynomial of $[n, k]$ cyclic code over the field $\mathcal{F}$. Let H be the $k \times n - k$ matrix whose jth row is $\mathrm{rem}_{g(x)}(x^{n-k+j-1})$, $j = 1, 2, 3 \ldots, k$. Then, the canonical parity check and generator matrices of the code are

$$\begin{aligned} H &= \left[A^t : I_{n-k}\right], \\ G &= \left[I_k : -A\right]. \end{aligned} \tag{11}$$

2.12. Example. Suppose that $p(x) = x^7 + x + 1$ is a primitive, irreducible polynomial of degree 8 and α is the primitive root of $p(x)$ over $\mathbb{Z}_2[x]$. Then the elements of Galois field $\mathrm{GF}(2^7)$ are shown in Table 1.

We want to construct the BCH code of length 127 with designed distance $d = 60$. Then find minimal polynomials corresponding to each α^i where $i = 1, 2, 3, \ldots, 59$. By using Theorem 2.4. and elements of the Galois field from Table 1, we get the following distinct minimal polynomials.

Now, by taking the LCM of all minimal polynomials from Table 2, we get generator polynomial of degree 119 for 127 length BCH code.

$$\begin{aligned} g(x) = {} & X^{119} + X^{117} + X^{115} + X^{113} + X^{112} + X^{109} + X^{108} + X^{104} + X^{100} + X^{98} \\ & + X^{97} + X^{95} + X^{92} + X^{91} + X^{90} + X^{87} + X^{82} + X^{79} + X^{77} + X^{74} + X^{71} + X^{70} \\ & + X^{68} + X^{67} + X^{65} + X^{64} + X^{63} + X^{59} + X^{58} + X^{57} + X^{56} + X^{54} + X^{48} + X^{47} \\ & + X^{45} + X^{43} + X^{39} + X^{38} + X^{35} + X^{33} + X^{32} + X^{31} + X^{29} + X^{28} + X^{23} + X^{22} \\ & + X^{21} + X^{19} + X^{17} + X^{16} + X^{15} + X^{14} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^4 \\ & + X^3 + X^2 + X + 1. \end{aligned} \tag{12}$$

3. Proposed Algorithm

In this algorithm, the key and block size are 128 bits. Simple logical and arithmetic operations are like shifting and logical XOR. Mainly, 2 steps are repeated 10 times for encrypting plain image data. These two steps are not constant for each round. Perhaps these steps introduced new entry in the next round, making the cryptanalysis more difficult.

3.1. Steps of Encryption

(i) Step 1: convert 128 bits of data into 16 data bytes and write these 16 bytes into a 4∗4 state matrix.

(ii) Step 2: construct keys using the BCH codes of length 128 by taking different designed distances over the Galois field, used as round keys. Key 0 is used in round 0; key 1 is used in round 1. Apply all 10 different keys in 10 rounds.

(iii) Step 3: ten different MDS matrices are constructed for each round using the BCH codes over the Galois field. Then the current state matrix is multiplied with the different MDS matrix in each round. The multiplication is modulo multiplication over the Galois field $\mathrm{GF}(2^8)$.

(iv) Step 4: then, take the analyses of the encrypted image and compare it with the original image.

3.2. Construction of Round Keys. The construction technique of round keys is followed by the binary representation of the generator polynomials of BCH codes over $\mathrm{GF}(2^7)$ for different designed distances. Convert each generator polynomial to its binary representation form of length 128 bits. If it

Table 1: Elements of Galois field GF(2^7).

α	$\alpha 2$	$\alpha 3$	$\alpha 4$
$\alpha 5$	$\alpha 6$	$\alpha 7 = \alpha + 1$	$\alpha 8 = \alpha^2 + \alpha$
$\alpha 9 = \alpha^3 + \alpha^2$	$\alpha 10 = \alpha^4 + \alpha^3$	$\alpha 11 = \alpha^5 + \alpha^4$	$\alpha 12 = \alpha^6 + \alpha^5$
$\alpha 13 = \alpha^6 + \alpha + 1$	$\alpha 14 = \alpha^2 + 1$	$\alpha 15 = \alpha^3 + \alpha$	$\alpha 16 = \alpha^4 + \alpha^2$
$\alpha 17 = \alpha^5 + \alpha^3$	$\alpha 18 = \alpha^6 + \alpha^4$	$\alpha 19 = \alpha^5 + \alpha + 1$	$\alpha 20 = \alpha^6 + \alpha^2 + \alpha$
$\alpha 21 = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 22 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	$\alpha 23 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	$\alpha 24 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha 3$
$\alpha 25 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	$\alpha 26 = \alpha^6 + \alpha^5 + \alpha^2 + 1$	$\alpha 27 = \alpha^6 + \alpha^3 + 1$	$\alpha 28 = \alpha^4 + 1$
$\alpha 29 = \alpha^5 + \alpha$	$\alpha 30 = \alpha^6 + \alpha^2$	$\alpha 31 = \alpha^3 + \alpha + 1$	$\alpha 32 = \alpha^4 + \alpha^2 + \alpha$
$\alpha 33 = \alpha^5 + \alpha^3 + \alpha^2$	$\alpha 34 = \alpha^6 + \alpha^4 + \alpha^3$	$\alpha 35 = \alpha^5 + \alpha^4 + \alpha + 1$	$\alpha 36 = \alpha^6 + \alpha^5 + \alpha^2 + \alpha$
$\alpha 37 = \alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 38 = \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha 39 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	$\alpha 40 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$
$\alpha 41 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$	$\alpha 42 = \alpha^6 + \alpha^4 + \alpha^2 + 1$	$\alpha 43 = \alpha^5 + \alpha^3 + 1$	$\alpha 44 = \alpha^6 + \alpha^4 + \alpha$
$\alpha 45 = \alpha^5 + \alpha^2 + \alpha + 1$	$\alpha 46 = \alpha^6 + \alpha^3 + \alpha^2 + \alpha$	$\alpha 47 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 48 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
$\alpha 49 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	$\alpha 50 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$	$\alpha 51 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	$\alpha 52 = \alpha^6 + \alpha^5 + \alpha^3 + 1$
$\alpha 53 = \alpha^6 + \alpha^4 + 1$	$\alpha 54 = \alpha^5 + 1$	$\alpha 55 = \alpha^6 + \alpha$	$\alpha 56 = \alpha^2 + \alpha + 1$
$\alpha 57 = \alpha^3 + \alpha^2 + \alpha$	$\alpha 58 = \alpha^4 + \alpha^3 + \alpha^2$	$\alpha 59 = \alpha^5 + \alpha^4 + \alpha^3$	$\alpha 60 = \alpha^6 + \alpha^5 + \alpha 4$
$\alpha 61 = \alpha^6 + \alpha^5 + \alpha + 1$	$\alpha 62 = \alpha^6 + \alpha^2 + 1$	$\alpha 63 = \alpha^3 + 1$	$\alpha 64 = \alpha^4 + \alpha$
$\alpha 65 = \alpha^5 + \alpha^2$	$\alpha 66 = \alpha^6 + \alpha^3$	$\alpha 67 = \alpha^4 + \alpha + 1$	$\alpha 68 = \alpha^5 + \alpha^2 + \alpha$
$\alpha 69 = \alpha^6 + \alpha^3 + \alpha^2$	$\alpha 70 = \alpha^4 + \alpha^3 + \alpha + 1$	$\alpha 71 = \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	$\alpha 72 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$
$\alpha 73 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	$\alpha 74 = \alpha^5 + \alpha^4 + \alpha^2 + 1$	$\alpha 75 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha$	$\alpha 76 = \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$
$\alpha 77 = \alpha^5 + \alpha^3 + \alpha^2 + 1$	$\alpha 78 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha$	$\alpha 79 = \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	$\alpha 80 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$
$\alpha 81 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 82 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha 83 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	$\alpha 84 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$
$\alpha 85 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	$\alpha 86 = \alpha^6 + \alpha^4 + \alpha^3 + 1$	$\alpha 87 = \alpha^5 + \alpha^4 + 1$	$\alpha 88 = \alpha^6 + \alpha^5 + \alpha$
$\alpha 89 = \alpha^6 + \alpha^2 + \alpha + 1$	$\alpha 90 = \alpha^3 + \alpha^2 + 1$	$\alpha 91 = \alpha^4 + \alpha^3 + \alpha$	$\alpha 92 = \alpha^5 + \alpha^4 + \alpha^2$
$\alpha 93 = \alpha^6 + \alpha^5 + \alpha^3$	$\alpha 94 = \alpha^6 + \alpha^4 + \alpha + 1$	$\alpha 95 = \alpha^5 + \alpha^2 + 1$	$\alpha 96 = \alpha^6 + \alpha^3 + \alpha$
$\alpha 97 = \alpha^4 + \alpha^2 + \alpha + 1$	$\alpha 98 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha$	$\alpha 99 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2$	$\alpha 100 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$
$\alpha 101 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$	$\alpha 102 = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 103 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha 104 = \alpha^5 + \alpha^4 + \alpha^3 + 1$
$\alpha 105 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha$	$\alpha 106 = \alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1$	$\alpha 107 = \alpha^6 + \alpha^3 + \alpha^2 + 1$	$\alpha 108 = \alpha^4 + \alpha^3 + 1$
$\alpha 109 = \alpha^5 + \alpha^4 + \alpha$	$\alpha 110 = \alpha^6 + \alpha^5 + \alpha^2$	$\alpha 111 = \alpha^6 + \alpha^3 + \alpha + 1$	$\alpha 112 = \alpha^4 + \alpha^2 + 1$
$\alpha 113 = \alpha^5 + \alpha^3 + \alpha$	$\alpha 114 = \alpha^6 + \alpha^4 + \alpha^2$	$\alpha 115 = \alpha^5 + \alpha^3 + \alpha + 1$	$\alpha 116 = \alpha^6 + \alpha^4 + \alpha^2 + \alpha$
$\alpha 117 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 118 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	$\alpha 119 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 120 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
$\alpha 121 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha 122 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha 123 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 1$	$\alpha 124 = \alpha^6 + \alpha^5 + \alpha^4 + 1$
$\alpha 125 = \alpha^6 + \alpha^5 + 1$	$\alpha 126 = \alpha^6 + 1$	$\alpha 127 = 1$	0

Table 2: Minimal polynomials.

$M(1) = x^7 + x + 1$
$M(2) = x^7 + x^5 + x^3 + x + 1$
$M(3) = x^7 + x^3 + x^2 + x + 1$
$M(4) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
$M(5) = x^7 + x^5 + x^4 + x^3 + 1$
$M(6) = x^7 + x^3 + 1$
$M(7) = x^7 + x^6 + x^5 + x^2 + 1$
$M(8) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
$M(9) = x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
$M(10) = x^7 + x^6 + x^3 + x + 1$
$M(11) = x^7 + x^5 + x^2 + x + 1$
$M(12) = x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$
$M(13) = x^7 + x^4 + 1$
$M(14) = x^7 + x^6 + x^4 + x^2 + 1$
$M(15) = x^7 + x^6 + x^4 + x + 1$
$M(16) = x^7 + x^6 + x^5 + x^4 + 1$
$M(17) = x^7 + x^4 + x^3 + x^2 + 1$

is not 128 bits, add check bits on the left-hand side to make 128 bits long. Then convert the BCH of length 128 into 16 bytes. This 16-byte string serves as a round key. Key 1 is derived from the generator polynomial of BCH code $[n = 127, k = 1]$ with designed distance 65. By using the proposed technique, we get Key 1 as follows:

(i) Key 1: 127 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255

(i) Now we construct the next key by using BCH code of length 127 over Galois field GF(2^7) with a designed distance of 60. Then convert the coefficients of generator polynomial $g(x)$ which are in descending order into the block of 8 bits.

(ii) 00000000 10101011 00110001 00010110 10011100 10000100 10100100 11011011 10001111 01000001 10101000 11001011 10110000 11101011 11001111 10111111

(iii) Convert each byte into the decimal form so that key 2 is as follows:

(ii) Key 2: 0 171 49 22 156 132 164 219 143 65 168 203 176 235 207 191

(i) Similarly, we construct all keys using BCH codes over the Galois field by changing the designed distance.

(iii) Key 3: 0 1 101 123 192 163 7 249 56 40 16 229 154 109 22 187

(iv) Key 4: 0 0 3 146 27 208 157 120 3 122 83 250 137 174 174 43

(v) Key 5: 0 0 0 5 16 109 174 23 166 30 82 12 96 106 78 41

(vi) Key 6: 0 0 0 0 13 83 6 214 191 219 200 87 71 25 231 13

(vii) Key 7: 0 0 0 0 0 25 161 99 10 46 46 13 22 111 12 93

(viii) Key 8: 0 0 0 0 0 0 41 19 31 9 172 122 28 6 238 111

(ix) Key 9: 0 0 0 0 0 0 0 65 218 145 157 158 251 54 166 153

(x) Key 10: 0 0 0 0 0 0 0 0 244 132 85 24 185 88 42 31

3.3. Construction of Mixed Column Matrix. This is a significant step in the proposed algorithm which creates confusion and diffusion. We construct a mixed column matrix by following steps:

(i) Step 1: construct a generator polynomial of BCH code of length n with designed distance δ where $n = 2^m - 1$ and m is the degree of the primitive, irreducible polynomial.

(ii) Step 2: select a value δ satisfying $l + 1 \le \delta \le 2^m - l$.

(iii) Step 3: calculate the dimension of the code, $k = n - r$, where r is the degree of the generator polynomial of BCH code.

(iv) Step 4: divide the $x^{n-k+i-1}$ where $i = 1, 2, \ldots k$ by generator polynomial and get remainder polynomial.

(v) Step 5: convert each remainder polynomial into binary form, make a block of 8 bits, and convert each block into decimal form.

(vi) Step 6: write coefficients of the remainder polynomial, which are in decimal form, into $l \times l$ matrix such that matrix is nonsingular.

3.4. Demonstration. Suppose that we want to construct the MDS matrices with the help of BCH code of length 255 with designed distance $\delta = 119$. Here we take $l = 4$, so that δ satisfies the inequality $5 \le \delta \le 252$. Generator polynomial is for BCH code with $[n = 255, k = 13, \delta = 119]$. The coefficients of generator polynomial in descending form are as follows:

1011010100110011100000101000101111111111001010111
0111111001011001100001001111111011011100000011101101
0111111010001101110001000010111010000101100111001000
0110000100000100100001001001011110011000011101000011
1000100010001001010010111111010100010010111.

We find the $\text{remg}_{BCH}(x)(x^{n-k+i-1})$, $i = 1, \ldots, 13$, that is, $\text{remg}_{BCH}(x)(x^{i+241})$. Coefficients of the polynomial $\text{remg}_{BCH}(x)(x^{242})$ are into the block of 8 bits. Here $\text{remg}_{BCH}(x)(x^{242})$ is the remainder polynomial after dividing x^{242} by generator polynomial of BCH code. The coefficients of remainder polynomial are as follows.

11101001 00010101 11110100 10100100 01000100 01100001 01110000 11001111 01001001 00001001 00000100 00110001 00111001 10100001 01110100 00100011 10110001 01111110 10110111 00000011 10110111 11100100 00110011 01001111 11011101 01001111 11111010 00101000 00111001 10010101 110100100

$$A = \begin{bmatrix} 11101001 & 01000100 & 01001001 & 00111001 \\ 00010101 & 01100001 & 00001001 & 10100001 \\ 11110100 & 01110000 & 00000100 & 01110100 \\ 10100100 & 11001111 & 00110001 & 00100011 \end{bmatrix}. \quad (13)$$

Now, converting each block into decimal form

$$A = \begin{bmatrix} 233 & 68 & 73 & 57 \\ 21 & 97 & 9 & 161 \\ 244 & 112 & 4 & 116 \\ 164 & 207 & 49 & 35 \end{bmatrix}. \quad (14)$$

Similarly, we construct 9 more MDS matrices for each round using BCH codes of length 127 corresponding to different designed distances for the image encryption scheme.

$$A_1 = \begin{bmatrix} 221 & 104 & 182 & 89 \\ 110 & 180 & 91 & 44 \\ 234 & 50 & 155 & 207 \\ 168 & 113 & 251 & 190 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 212 & 117 & 117 & 145 \\ 190 & 79 & 207 & 89 \\ 95 & 39 & 231 & 172 \\ 251 & 230 & 134 & 71 \end{bmatrix},$$

$$A_3 \begin{bmatrix} 148 & 114 & 86 & 6 \\ 74 & 57 & 43 & 3 \\ 177 & 110 & 195 & 135 \\ 88 & 183 & 87 & 195 \end{bmatrix},$$

$$A_4 = \begin{bmatrix} 176 & 231 & 152 & 226 \\ 232 & 148 & 84 & 147 \\ 196 & 173 & 178 & 171 \\ 98 & 86 & 217 & 85 \end{bmatrix},$$

$$A_5 = \begin{bmatrix} 186 & 48 & 246 & 104 \\ 231 & 40 & 141 & 92 \\ 201 & 164 & 11 & 198 \\ 222 & 226 & 174 & 11 \end{bmatrix}, \quad (15)$$

$$A_6 = \begin{bmatrix} 246 & 119 & 96 & 56 \\ 123 & 59 & 176 & 28 \\ 203 & 234 & 184 & 54 \\ 101 & 245 & 92 & 27 \end{bmatrix},$$

$$A_7 = \begin{bmatrix} 153 & 101 & 108 & 223 \\ 76 & 178 & 182 & 111 \\ 38 & 89 & 91 & 55 \\ 19 & 45 & 173 & 155 \end{bmatrix},$$

$$A_8 = \begin{bmatrix} 248 & 84 & 26 & 157 \\ 132 & 126 & 23 & 83 \\ 66 & 63 & 11 & 233 \\ 33 & 31 & 133 & 244 \end{bmatrix},$$

$$A_9 = \begin{bmatrix} 136 & 52 & 201 & 200 \\ 68 & 26 & 100 & 228 \\ 34 & 13 & 50 & 114 \\ 153 & 50 & 80 & 241 \end{bmatrix}.$$

These are the required matrices used in the proposed algorithm in the mixed column transformation step for image data security.

4. Analysis

4.1. Key Space Analysis. The asset of an algorithm of cryptography depends on the space of the key, so the length of the key must be large for a brute force attack. The proposed algorithm has 2^{128} possible keys, which are very large. Suppose any unauthorized person tries for a brute force attack. In that case, the acute sensitivity is very high for this algorithm, so he has to try all possibilities of keys for the decryption of the image, which is very difficult to do computationally.

4.2. Key Sensitivity Analysis. High key sensitivity is vital for image security, which means that the encrypted image cannot be converted into a plain image correctly even if there is a small change between decryption or encryption keys. The proposed algorithm is tested for different keys with a minimal difference. This is the same as an avalanche effect in text encryption, where a minimal change in the key gives a major difference in the encrypted text. The strength of an algorithm is that if a key is changed by a single bit, then the original image cannot be obtained.

4.3. Statistical Analysis for Image Encryption. Statistical analyses are used to determine the statistical features of the encryption technique. These analyses include correlation, information entropy, contrast, homogeneity, and energy. These analyses determine the strength of the encryption scheme. Statistical analyses decide whether the encryption scheme is secure for image encryption or not. The details of statistical analyses are briefly discussed as follows.

4.3.1. Histogram Analysis. Histogram analysis is used to see how much encryption procedure is needed to change test image compared to the encrypted image. For good encryption, the histogram of the ciphered image should have a uniform distribution that indicates that the anticipated scheme can resist statistical attacks. Figure 1–6 shows the histogram analysis of test images and encrypted images. Figure 1 shows original image histogram and Figure 4 shows the histogram of encrypted image through blue channel. Figure 2 shows histogram of original image and Figure 5 shows histogram of encrypted image through green channel. Figure 3 is showing histogram of plain image and Figure 6 shows histogram of encrypted image through red channel.

The histograms of the ciphered images are appreciably uniform and are quite dissimilar from the test images. The suggested encryption technique has fulfilled all the test image features and has convoluted the statistical bond between the test image and its cipher image.

4.3.2. Contrast. Contrast analysis organizes the objects in an image. A secure encryption technique has high contrast values. It measures the color difference, which identifies the distinctive in an object. More briefly, it measures the change in brightness, color, and other objects within a similar frame

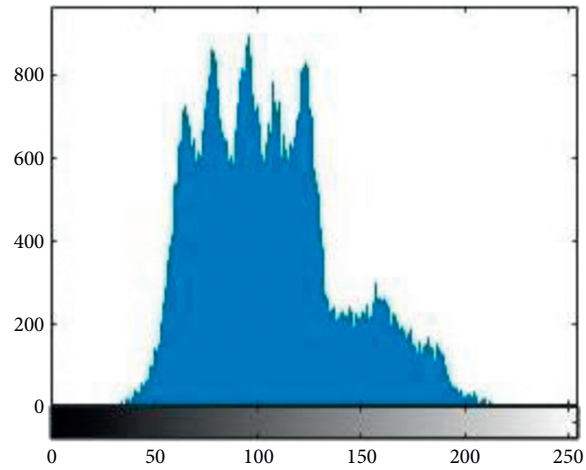

Figure 1: Original blue.

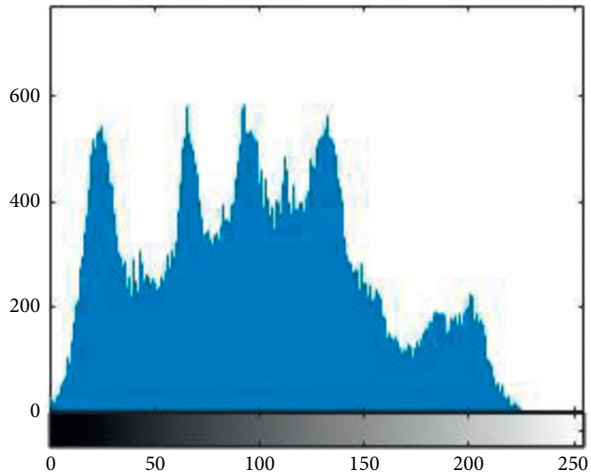

Figure 2: Original green.

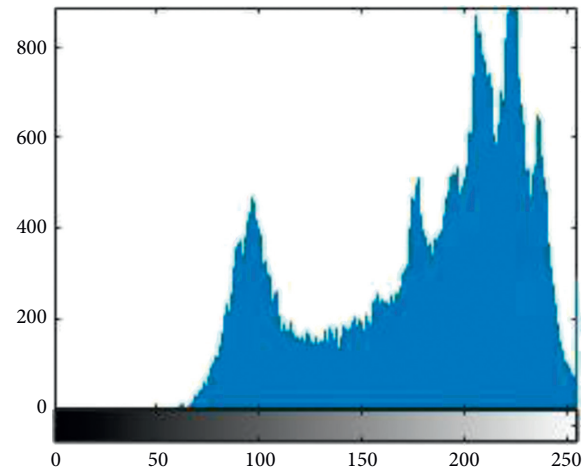

Figure 3: Original red.

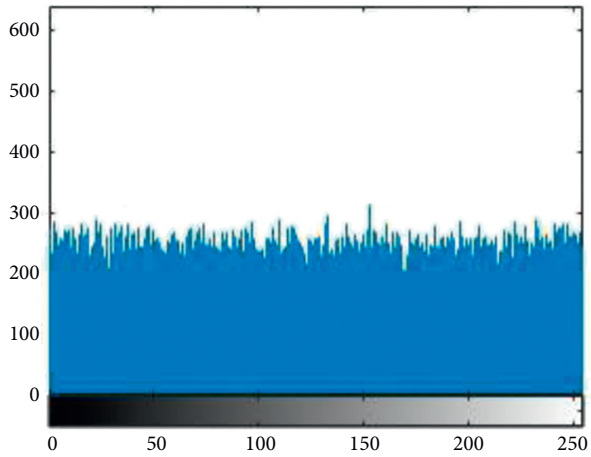

Figure 4: Encrypted blue.

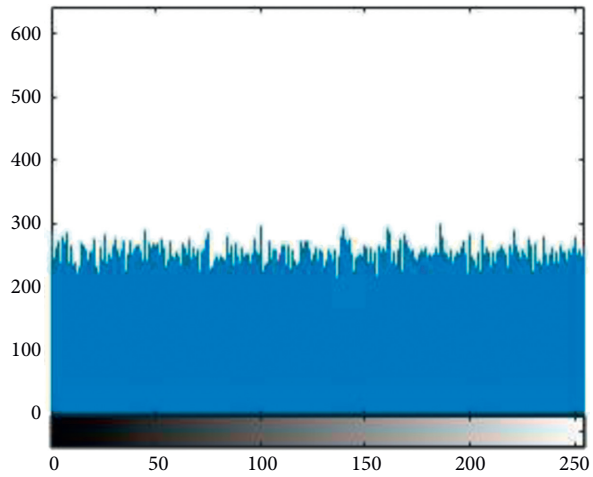

Figure 5: Encrypted green.

of view. Contrast can be measured mathematically by the equation

$$C = \sum_{g,h} |g - h|^2 n(g,h). \tag{16}$$

$n(g,h)$ denotes the number of grey-level cooccurrence matrices and g, m are the pixels of an image. The strength of contrast between the pixels and their adjacent pixels is compared in the full image.

4.3.3. Correlation. The correlation analysis is used to break the relationship between the neighboring pixels. The test image correlation is approaching one. The encrypted image should correlate coming zero for better encryption. To determine the encryption effect of the proposed technique, perform correlation analysis on the plain and encrypted image. The correlation coefficient is calculated by formula

$$r_{xy} = \frac{E\left(\left(x - \mu_x\right)\left(y - \mu_y\right)\right)}{\sqrt{\delta x \delta y}}. \tag{17}$$

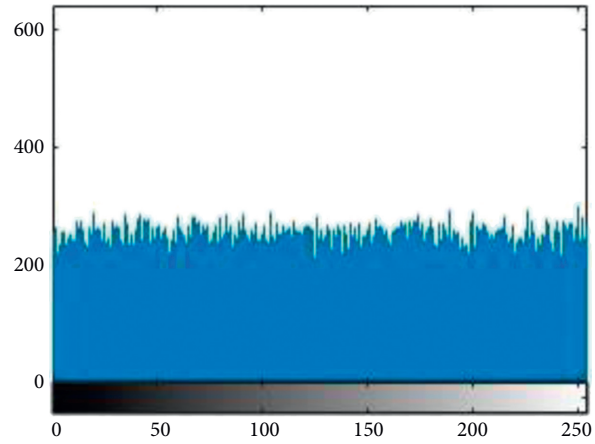

Figure 6: Encrypted red.

δ and μ and denote the variance and expected value.

4.3.4. Energy. In this analysis, we compute the energy of the encrypted images by applying S-boxes. This measure gives the sum of squared elements in the grey-level cooccurrence matrix

$$e = \sum_{l,m} p(l,m)^2, \tag{18}$$

where $p(l,m)$ is the number of grey-level cooccurrence matrices.

4.3.5. Homogeneity. In homogeneity, the grey-level cooccurrence matrix explains the proficiency of arrangements of pixel brightness results in tabular form. The closeness of the distribution in the grey-level cooccurrence matrix to its diagonal is measured through the homogeneity analysis. If the homogeneity is as small as possible, then encryption is better. The following formula measures homogeneity:

$$H = \sum_{l,m} \frac{n(l,m)}{1 + |l - m|}. \tag{19}$$

4.3.6. Entropy. Information entropy measures the disorder which is created by the encryption process. Entropy measures the strength of the encryption technique. An encryption technique is good if it has more disorder and randomness. Entropy is defined as

$$e = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i), \tag{20}$$

where $P(x_i)$ contains the histogram counts. Entropy must be close to 8 for better image quality.

4.3.7. Image Encryption. The image is encrypted using the proposed scheme. Figure 7 shows the original Lena image, and Figure 8 shows the encrypted Lena image. The

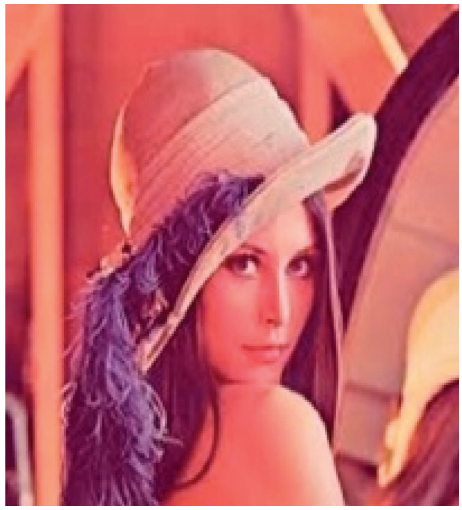

Figure 7: Original image.

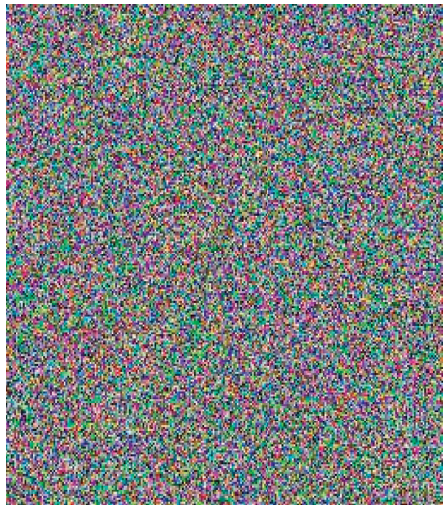

Figure 8: Encrypted image.

Table 3: Analyses of original and encrypted image

Channel	Contrast	Correlation	Energy	Homogeneity	Entropy
Original AES red	5.1454	0.0742	0.0254	0.4701	7.7337
Proposed AES red	5.2462	0.0731	0.0256	0.4661	7.7959
Original AES green	5.3501	0.0804	0.0250	0.4621	7.7337
Proposed AES green	5.3557	0.0800	0.0250	0.4620	7.7959
Original AES blue	5.0947	0.0721	0.0270	0.4666	7.7337
Proposed AES blue	5.1995	0.0716	0.0271	0.4602	7.7959

comparison results of the original AES algorithm and proposed encryption technique are shown in Table 3.

Table 3 shows results of the encryption technique using the original AES algorithm and proposed AES algorithm through the red, green, and blue channels. The contrast of the proposed AES is better than the original AES. Correlation and energy are also close to zero. Proposed homogeneity is also good as compared to the original AES. Entropy is close to 8, which shows that our image encryption technique is good.

5. Conclusion

This paper encrypts the image using the novel technique based on BCH codes over the Galois field. We introduce a new method for image encryption using Bose Chaudhary Hocquenghem codes which secures our data. We constructed the secret keys and MDS matrices using the BCH codes of length 127 over the Galois field (2^7). Then encrypt the image using the proposed modified AES algorithm. Table 3 concludes that the proposed image encryption technique is better than the original AES algorithm. Correlation, homogeneity, and energy of encrypted image also show promising results for image data security. Our histogram analysis shows that the proposed encryption scheme is improved. We can conclude that the proposed algorithm gives a high-security level to image data using different tests and studies. The unauthorized user cannot access the data without permission. This algorithm can be used in various intelligence agencies, Forensics, and Military Communication in the future. Further, this work can be extended to apply text, audio, video encryption.

Data Availability

No such type of data were used in this manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through the research groups program under Grant no. R. G. P. 2/150/42.

References

[1] C. E. Shannon, "Communication theory of secrecy systems ∗," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] H. M. Heys and S. E. Tavares, "The design of substitution-permutation networks resistant to differential and linear cryptanalysis," in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 148–155, ACM, Fairfax, VI, USA, November 1994.

[3] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *Journal of Cryptology*, vol. 9, no. 1, pp. 1–19, 1996.

[4] H. M. Heys and S. E. Tavares, "Avalanche characteristics of substitution-permutation encryption networks," *IEEE Transactions on Computers*, vol. 44, no. 9, pp. 1131–1139, 1995.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," *International Journal of Computer Science and Engineering*, vol. 1, no. 1, pp. 70–75, 2007.

[6] P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, "Modified advanced encryption standard," *International Journal of Soft Computing and Engineering*, vol. 4, p. 1, 2014.

[7] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137–2150, 2018.

[8] K. D. Patel and S. Belani, "Image encryption using different techniques: a review," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 1, pp. 30–34, 2011.

[9] P. Karthigaikumar and S. Rasheed, "Simulation of image encryption using aes algorithm. Ijca special issue on "computational science-new dimensions & perspectives"," *International Journal of Computer Applications*, vol. 4, pp. 166–172, 2011.

[10] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, pp. 15999–16007, 2019.

[11] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. Win, "The cipher SHARK," in *Proceedings of the International Workshop on Fast Software Encryption*, pp. 99–111, Springer, Cambridge, UK, February 1996.

[12] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *aes Algorithm Submission*, pp. 37-38, 1999, http://www.nist.gov/CryptoToolKit.

[13] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: a 128-bit block cipher," *NIST AES Proposal*, vol. 15, p. 23, 1998.

[14] B. Schneier, J. Kelsey, D. Whiting et al., "The Twofish team's final comments on AES Selection," *AES round*, vol. 2, p. 7, 2000.

[15] Z. Yun-Peng, L. Wei, C. Shui-Ping, Z. Zheng-Jun, N. Xuan, and D. Wei-di, "Digital image encryption algorithm based on chaos and improved DES," in *Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics*, pp. 474–479, IEEE, San Antonio, TX, USA, October 2009.

[16] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion," *International Journal of the Physical Sciences*, vol. 6, no. 16, pp. 4110–4127, 2011.

[17] B. Subramanyan, V. M. Chhabria, and T. S. Babu, "Image encryption based on AES key expansion," in *Proceedings of the 2011 2nd International Conference on Emerging Applications of Information Technology*, pp. 217–220, IEEE, Kolkata, India, February 2011.

[18] M. Walters and S. S. Roy, "Constant-time BCH error-correcting code," in *Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, Seville, Spain, October 2020.

[19] M. Asif and T. Shah, "BCH Codes with computational approach and its applications in image encryption," *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 3, pp. 3925–3939, 2019.

[20] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain, and M. Asif, "An efficient image encryption scheme based on double affine substitution box and chaotic system," *Integration*, vol. 81, pp. 108–122, 2021.

[21] A. S. Alanazi, N. Munir, M. Khan, M. Asif, and I. Hussain, "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes," *IEEE Access*, vol. 9, pp. 93795–93802, 2021.

[22] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, pp. 123492–123506, 2020.

[23] Y. Naseer, T. Shah, and D. Shah, "A novel hybrid permutation substitution base colored image encryption scheme for multimedia data," *Journal of Information Security and Applications*, vol. 59, pp. 102829–102833, 2021.

[24] N. Munir, M. Khan, T. Shah, A. S. Alanazi, and I. Hussain, "Cryptanalysis of nonlinear confusion component based encryption algorithm," *Integration*, vol. 79, pp. 41–47, 2021.

[25] H. V. Gamido, A. M. Sison, and R. P. Medina, "Implementation of modified AES as image encryption scheme," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 6, no. 3, pp. 301–308, 2018.

[26] S. R. Nagpaul, *Topics in Applied Abstract Algebra*, Vol. 15, American Mathematical Society, , Providence, RI, USA, 2005.