IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 3, 2021, accepted May 10, 2021, date of publication May 19, 2021, date of current version June 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3081792

Improved Twofish Algorithm: A Digital Image Enciphering Application

TANVEER UL HAQ[1], TARIQ SHAH[1], GHAZANFAR FAROOQ SIDDIQUI[2], MUHAMMAD ZAFAR IQBAL[2], IBRAHIM A. HAMEED[3], (Senior Member, IEEE), AND HUMA JAMIL[1]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Department of Computer Science, Quaid-i-Azam University, Islamabad 45320, Pakistan
[3]Department of ICT and Natural Sciences, Norwegian University of Science and Technology, 6009 Ålesund, Norway

Corresponding authors: Ghazanfar Farooq Siddiqui (ghazanfar@qau.edu.pk) and Ibrahim A. Hameed (ibib@ntnu.no)

ABSTRACT With the growth of networks, the Internet of Things (IoT) and new cyber attacks pose threats to privacy and security, secure communication is therefore becoming one of the most crucial concerns. For this purpose, symmetric algorithms namel; The Rijndael algorithm, the Serpent algorithm, and the TWOFISH algorithm pay equal attention. In this paper, the TWOFISH algorithm's mathematical complexity is improved by using substitution boxes (S-boxes) drawn from a multiplicative group of units of chain ring $\sum_{i=0}^{7} u^i F_2$. As these S-boxes have the property of having copious generators, they, therefore, produce a rich algebraic complexity. Moreover, the time complexity of the proposed work is modified by processing the 64-bit block throughout the process and reducing the number of subkeys. To measure the strength of the proposed algorithm, various standard color digital images, with a size of 256×256, are encrypted and tested. The computation speed of the encryption is compared to the standard TWOFISH algorithm's speed and found that the newly designed algorithm is quite fast. For security analysis and quality assessment, various statistical tests are performed on the standard encrypted images. The results recommend that the proposed algorithm is a strong candidate for digital image encryption.

INDEX TERMS Chain ring, color image encryption, substitution box, TWOFISH algorithm.

I. INTRODUCTION

With the increasing use of the Internet and online communications, data security has become a matter of great concern. The risk of data being stolen, hacked, altered, and damaged in one form or another compel the need to protect it before sending. Encryption is done by combining a plain text with a secret set of characters called the key. The key resists adversaries to find a correlation between the original message and the encrypted message [1], [30].

A sound encryption algorithm minimizes the chance of third-unauthorized-party interference. Based on their structures, these algorithms can be classified into two main categories; the symmetric algorithms [1]; which requires only one key for encryption and decryption purpose and asymmetric algorithm [2]; in which one key is required to encrypt the plain text while another key is required to decrypt the cipher text. An additional classification distinguishes stream ciphers from block ciphers. However, this study mainly focus on block cipher. The block ciphers operates on a bunch of bits at a time. The famous block ciphers include the Data Encryption Standard (DES) [3], the Advanced Encryption Standard (AES) [3] Serpent algorithm and Twofish aoglrithm. The algorithms provide information security services such as confidentiality, data integrity, authentication, and non-repudiation [4]. Other sources that provide these services are hashing algorithms, password authentication protocols, and digital signatures.

In cryptography, a substitution box (S-box) is the main nonlinear component of a symmetric key cipher that performs the substitution and creates a layer of confusion in the encrypted data. This was first proposed by Shannon [5] and clarified more completely in [6] and [7]. These S-boxes provides the robustness in substitution-permutation networks; a weak S-boxes can be routed to a weak crypto systems (e.g., see [8] and [9]). In block ciphers, S-boxes are commonly used to conceal the relevance between the key and the ciphered text. Properties such as bijection, non-linearity,

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

strict avalanche effect, and independence of output bits are judged in an S-box to categorize it. So far, many successful attempts have been made to construct strong S-boxes by randomly generating them and testing them on these properties [10]. However, some S-boxes do not meet the evaluation criteria and are rejected [11].

In many cases, S-boxes are carefully chosen to resist cryptanalysis. Many encryption algorithms use a variety of differently structured S-boxes. AES, for example, has S-boxes which are designed on the finite field GF(2^8) [3]. But study shows that the implication of only nine terms in the algebraic expression of the S-box created a low complexity. And therefore, these S-boxes are suspected to be vulnerable to interpolation attacks [12]. To avoid such weaknesses, we took a different approach using the S-boxes obtained from the chain ring R_8 [13]. The ring $R_8 = \frac{F_2[u]}{<u^8>} = F_2+uF_2+u^2F_2+u^3F_2+u^4F_2+u^5F_2+u^6F_2+u^7F_2$ is a commutative chain ring having cardinality 2^8. Moreover, $\frac{R_8}{uR_8} \cong F_2$ is the residue field of R_8. So, the multiplicative and the additive binary operation coincides with that of $\mathbb{Z}_{2^8}$ and F_{2^8} respectively. The achieved S-boxes can be arranged in the form of 4×4 lookup tables and are used inside the newly designed TWOFISH algorithm.

The classic TWOFISH algorithm [14] is one of the finalists for the call of AES. In this article, the TWOFISH algorithm is modified using various strategies. A 128-bit block is encrypted using a variable-length key of size 128, 192, or 256 bits in the modified TWOFISH algorithm. Initially, the 128-bit input block is divided into two sub-blocks, the right 64-bit block and the left 64-bit block, each of 64-bit (In classic Twofish algorithm 32-bit blocks were considered for encryption). This helps the newly designed algorithm in speed performance. After this, regular whitening is carried out through the key. Then, an F-function is operated on the 64-bit word. In the F-function; the 64-bit word is rotated, molded according to the function g, the pseudo hadamard transformed (PHT), and then exclusive-ored with the round key. Inside the g function, S-boxes obtained from the commutative chain ring are used. These S-boxes have multiple generators (instead of 1 generator) that improve the algebraic complexity of the g-fuction and hence the algebraic complexity of the improved Twofish algorithm. The output of F is then XORed with the right block of 64-bit obtained after whitening. To complete this process, an exchange of the outcome is performed with the right 64-bit block and the process continues for a total of 16 rounds. The output of the last round undergoes a final exchange and is exclusive-ORed with key material in the output whitening step to produce ciphered text.

The article is assembled as follows: In section II, we explain the chain rings and substitution boxes designed on the units of the structure. The modified TWOFISH algorithm on chain ring operations and its application to color images are given in section III. The security analysis of the proposed encryption scheme is given in section IV. Sections V and VI include experimental analyzes, including comparison, for the encrypted color images. Comparing the time execution of the proposed scheme with other established schemes is given in Section VII. Section VIII provides the randomness with a test on the encrypted images. In the last section IX, the concluding remarks are included.

II. ALGEBRA UNDER CONSIDERATION

Consider that R is a ring with identity and Commutativity.

A. LOCAL RING

For any $u \in R$ if there exist $v \in R$ such that $uv = 1$ then u is unit. The ring R is a local ring if the set of non-unit vectors in R form an abelian group. Also, if R has a unique maximal ideal we call it a local ring. For example, the integer modulo ring $\mathbb{Z}_{p^k}$, is a local ring.

Let the pair (R, M) represent a local ring R having maximal ideal M. Then $\frac{R}{M} = K$ form residue field. Also, there presents a canonical epimorphism $\theta : R \to \frac{R}{M}$ defined as $\theta(a) = \hat{a} = a + M, a \in R$. Let the polynomial $f(y) = a_0 + a_1 y + a_2 y^2 + \ldots + a_m y^m \in R[y]$ and $\overline{f(y)} = \hat{a_0} + \hat{a_1} y +, \hat{a_2} y^2 + \ldots + \hat{a_m} y^m \in K[y]$, if $\overline{f(y)}$ is irreducible over K, then $f(y)$ is called a basic irreducible polynomial.

III. CHAIN RING

Let $\mathcal{R}$ be a ring. Then $x \in \mathcal{R}$ is a unit in $\mathcal{R}$ if there exists some $y \in \mathcal{R}$ such that $xy = 1$, where 1 the multiplicative identity of $\mathcal{R}$. Set of all unit elements of $\mathcal{R}$ forms a multiplicative group. If $0 \neq a \in \mathcal{R}$, then a is called the zero-divisors if there exists some nonzero element $b \in \mathcal{R}$ such that $ab = 0$. Also, $0 \neq a \in \mathcal{R}$ is nilpotent if there exists a least positive integer n such that $a^n = 0$, n is called as the multiplicative index of a.

A ring with only one maximal ideal M is a local ring and the quotient ring $\frac{\mathcal{R}}{M}$ is its residue field. A local finite ring R is a chain ring iff the radical M of $\mathcal{R}$ is a principal ideal, and therefore the quotient ring $\frac{\mathcal{R}}{M}$ is a field. Thus, the ideals of a chain ring form a chain.

Let $\mathcal{R}_n$ be a representation of a finite chain ring $\frac{\mathrm{F}_2[v]}{<v^n>} = \mathrm{F}_2 + v\mathrm{F}_2 + v^2\mathrm{F}_2 + \ldots + v^{n-1}\mathrm{F}_2$. The ring $\mathcal{R}_n$ has 2^n elements. The element v is the nilpotent element with nilpotency index n, i.e. $v^n = 0$. Thus, it follows that $< 0 >= v^n\mathcal{R}_n \subset v^{n-1}\mathcal{R}_n \subset \ldots \subset v\mathcal{R}_n \subset \mathcal{R}_n$ is the ascending chain of ideals in $\mathcal{R}_n$ and therefore $\mathcal{R}_n$ is a local ring with only one maximal ideal $v\mathcal{R}_n$, whereas $\frac{\mathcal{R}_n}{v\mathcal{R}_n} \cong \mathrm{F}_2$ is the residue field of the chain ring $\mathcal{R}_n$. This ring $\mathcal{R}_n$ shares some properties of the local ring $\mathbb{Z}_{2^n}$ and the Galois field F_{2^n}. More explicitly the multiplicative binary operation of $\mathcal{R}_n$ coincides with of $\mathbb{Z}_{2^n}$ whereas the additional binary operation is similar to that of F_{2^n}.

In algebraic coding theory, the most frequently used rings of cardinality four are Galois field F_2 and the modular ring of integers $\mathbb{Z}_4$.

The cyclic codes (see [15]) are constructed over the rings $\mathrm{F}_2 + v\mathrm{F}_2 = \{0, 1, v, \bar{v}\}$ with $v^2 = 0$ and $\mathrm{F}_2 + v\mathrm{F}_2 + v^2\mathrm{F}_2 = \{0, 1, v, v^2, 1+v, 1+v^2, v+v^2, 1+v+v^2\}$ with $v^3 = 0$. These codes are further extended to $\mathcal{R}_k = \mathrm{F}_2 + v\mathrm{F}_2 + v^2\mathrm{F}_2 + \ldots + v^{k-1}\mathrm{F}_2$ with $v^k = 0$ [16]. The elements in the ring $F_2 + vF_2$ corresponds to the binomial polynomial in variable v with the degree at most 1. These elements satisfy the closure property of polynomial addition and polynomial multiplication modulo v^2. Table 1 and Table 2 states the multiplication and addition for this ring. Careful observation of these tables reveals the similarity of operations with that of $\mathbb{Z}_4$ and $_4$. More explicitly the multiplication table coincides with $\mathbb{Z}_4$ with v and $\bar{v}$ replacing 2 and 3. And the addition table coincides with the Galois field $F_4 = \{0, 1, \gamma, \gamma^2 = 1 + \gamma\}$ where $\bar{v}$ and v are replaced by γ and γ^2.

TABLE 1. Addition table for $F_2 + vF_2$.

$\times$	0	1	v	$\bar{v}$
0	0	0	0	0
1	0	1	v	$\bar{v}$
v	0	v	1	v
$\bar{v}$	0	$\bar{v}$	v	0

TABLE 2. Multiplication table of $F_2 + vF_2$.

$+$	0	1	$\bar{v}$	v
0	0	1	$\bar{v}$	v
1	1	0	v	$\bar{v}$
$\bar{v}$	$\bar{v}$	v	0	1
v	v	$\bar{v}$	1	0

The ring $\mathcal{R}_8 = \frac{F_2[v]}{<v^8>} = F_2 + vF_2 + \ldots + v^7F_2$ is a commutative chain ring of 2^8 elements since v are nilpotent with nilpotency index 8, it follows that $< 0 >= v^8\mathcal{R}_8 \subset v^7\mathcal{R}_8 \subset \ldots \subset v\mathcal{R}_8 \subset \mathcal{R}_8$. The multiplicative group $\mathcal{M}_{G^8}$ contains 128 elements. To get a subgroup of cardinality 16, the subgroup $\mathcal{H}_{G^8} =< v^6 + v^3 + 1, v^7 + v^5 + v^4 + v^2 + 1 >$ is chosen. And by defining the maps $f : \mathcal{H}_{G^8} \longrightarrow \mathcal{H}_{G^8}$ by $f(a) = a^{-1}$ and $g : \mathcal{H}_{G^8} \longrightarrow \mathcal{H}_{G^8}$ by $g(a) = a'a$ where we take $a' = v^6 + v^4 + 1$. Thus $gof(a) = (a'a)^{-1}$.

The following table of $fog(\mathcal{H}_{G^8})$ is the S-box designed over the chain ring $\mathcal{R}_8$. Table 3 is represented in the binary and corresponding hexadecimal form of the polynomial $\mathcal{R}_8 = v^7F_2 + v^6F_2 + \ldots + F_2$.

TABLE 3. The binary and hexadecimal representation of $\mathcal{R}_8 = v^7F_2 + v^6F_2 + \ldots + F_2$.

01010001 81	10011001 99	01000001 41	00010001 11
11011001 D9	11110101 F5	10100101 A5	01011101 5D
01001001 49	10001101 8D	00000001 01	01011101 5D
11100101 E5	00011101 1D	00001001 09	11001101 CD

IV. MODIFIED TWOFISH ALGORITHM

Figure 1 explains the structure of the modified TWOFISH. In this algorithm, the 128-bit plaintext is divided into two 64 bits' words. The two words are first passed through the process of input whitening, in which these are XORed with the subkeys K_0 and K_1. After this, the resultant left word is passed through the Feistel Function F. The output of the F function is XORed with the resultant right word. And then the resultant word swaps its position with the left word. These new 64-bits words are then the input of the second round. The same process continues till 16 rounds and then the output of the last round is XORed with subkeys K_2 and K_3.

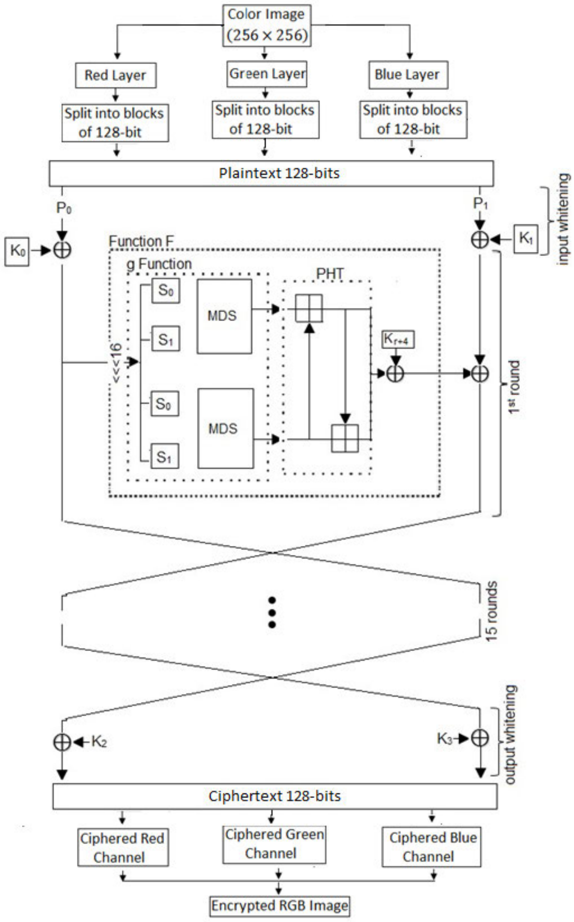

FIGURE 1. Image enciphering technique based on Improved TWOFISH algorithm.

A. THE FUNCTION F

The Function F takes two inputs, a 64-bit word R_0 and the round number to get the round key. R_0 is left rotated by 16 bits and passed through g-function. Function g yields two outputs G_0 and G_1 of 32 bits each. These two outputs undergo pseudo Hadamard transform to yield P_0 and P_1. These words are combined and XORed with the round key K_{r+4}.

$$\begin{aligned}(G_0, G_1) &= g(ROL(R_0, 16)) \\ P_0 &= (G_0 + G_1) \bmod 2^{32} \\ P_1 &= (G_0 + 2G_1) \bmod 2^{32} \\ F_0 &= ((P_0, P_1) + K_{r+4}) \bmod 2^{64}\end{aligned}$$

B. THE FUNCTION G

The g function takes a 64-bits word as an input, split it into four vectors of 16 bits, and then pass these vectors through key-dependent S-boxes. The result is then considered as two vectors of length four and is individually multiplied by the MDS matrix. The matrix multiplication is defined over Finite Field GF 2^8, with primitive polynomial $\omega(x) = x^8 + x^6 + x^5 + x^3 + 1$.

The MDS matrix is given below:

$$\begin{bmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{bmatrix}$$

C. S-BOX UNDER CONSIDERATION

The S-boxes we have used are key-dependent and take 16 bits of input. Inside these S-boxes are the two permutation q_0 and q_1 and the list S of k number of keywords are used.

These keywords are generated once and are kept fixed throughout the process. As TWOFISH supports key of variable length. The list S contains two, three, and four keywords for 128, 192- and 256-bits' key lengths respectively.

If $k = 2$, then

$$\begin{aligned}
(y_{0,0}, y_{0,1}) &= q_0\left[q_o[x_0] \oplus (s_{1,0}, s_{1,1})\right]\\
(y_{0,2}, y_{0,3}) &= q_1\left[q_1[x_1] \oplus (s_{0,0}, s_{0,1})\right]\\
(y_{1,0}, y_{1,1}) &= q_0\left[q_o[x_2] \oplus (s_{1,2}, s_{1,3})\right]\\
(y_{1,2}, y_{1,3}) &= q_1\left[q_1[x_3] \oplus (s_{0,2}, s_{0,3})\right]
\end{aligned}$$

If $k = 3$, then

$$\begin{aligned}
(y_{0,0}, y_{0,1}) &= q_0\left[q_0\left[q_o[x_0] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,0}, s_{2,1})\right]\\
(y_{0,2}, y_{0,3}) &= q_1\left[q_1\left[q_1[x_1] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,0}, s_{2,1})\right]\\
(y_{1,0}, y_{1,1}) &= q_0\left[q_0\left[q_o[x_2] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,2}, s_{2,3})\right]\\
(y_{1,2}, y_{1,3}) &= q_1\left[q_1\left[q_1[x_0] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,2}, s_{2,3})\right]
\end{aligned}$$

If $k = 4$, then

$$\begin{aligned}
(y_{0,0}, y_{0,1}) &= q_0\left[q_0\left[q_o[x_0] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,0}, s_{2,1})\right]\\
(y_{0,2}, y_{0,3}) &= q_1\left[q_1\left[q_1[x_1] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{3,0}, s_{3,1})\right]\\
(y_{1,0}, y_{1,1}) &= q_0\left[q_0\left[q_o[x_2] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{2,2}, s_{2,3})\right]\\
(y_{1,2}, y_{1,3}) &= q_1\left[q_1\left[q_1[x_0] \oplus (s_{1,0}, s_{1,1})\right)\right.\\
&\qquad \left.\oplus(s_{3,2}, s_{3,3})\right]
\end{aligned}$$

D. THE PERMUTATIONS q_0 AND q_1

The permutations used in s-boxes are made of the two fixed look-up tables whose entries are the elements of the multiplicative group of chain ring. Both permutations take input of 16 bits split into two bytes and the proceeds as explained by the equations below.

Let x be input to q_0 then:

$$\begin{aligned}
a_o, b_0 &= \lceil x/256 \rceil, (x \bmod 256)\\
a_1 &= (a_0) \oplus (b_0)\\
b_1 &= a_0 \oplus \mathrm{ROR}(b_0, 1) \oplus 16a_0 \bmod 256\\
a_2 &= t_0[a_1]\\
b_2 &= t_1[b_1]\\
y &= 256b_2 + a_2
\end{aligned}$$

The lookup tables for permutation q_0 and q_1 are given in Table 4 and Table 5 respectively.

TABLE 4. (a) T_0. (b) T_1.

(a)

51	99	41	11	D9	F5	A5	5D
49	8D	01	B5	E5	1D	09	CD

(b)

51	99	41	11	5D	D9	F5	A5
01	B5	49	8D	1D	09	CD	E5

TABLE 5. (a) T_0. (b) T_1.

(a)

51	99	41	11	5D	D9	CD	8D
01	D9	91	E5	1D	B5	F5	11

(b)

51	09	49	A5	5D	99	CD	8D
01	D9	91	E5	1D	B5	F5	11

The step $= t_0[a_1]$ works as follows:

$$\begin{aligned}
n &= a_1 \bmod 16\\
m &= t_0[n]\\
a_2 &= a_1 \times m
\end{aligned}$$

Here multiplication × is defined over chain ring $\mathcal{R}_8$. The values from other lookup tables are also fetched similarly.

E. THE KEY SCHEDULE

TWOFISH supports the key lengths of $N = 128$, $N = 192$, and $N = 256$. The key Schedule has to provide 20 subkeys, four of which are used for whitening and the other sixteen in the rounds. And the fixed keys $[S_0, S_1, \ldots, S_k]$ for S-boxes are produced separately. Where $k = N/64$.

If the original key is $M = [m_0, m_1, \ldots, m_{8k}]$, where m_i represents the byte. Then the keys S_i are produced as follows:

$$\begin{bmatrix} S_{i,0} \\ S_{i,1} \\ S_{i,2} \\ S_{i,3} \end{bmatrix} = \begin{bmatrix} . & \cdots & . \\ \vdots & RS & \vdots \\ . & \cdots & . \end{bmatrix} \begin{bmatrix} m_{8i} \\ m_{8i+1} \\ m_{8i+2} \\ m_{8i+3} \\ m_{8i+4} \\ m_{8i+5} \\ m_{8i+6} \\ m_{8i+7} \end{bmatrix}$$

The multiplication with Reed Solomon (RS) matrix is carried out in finite field $GF(2^8)$ with primitive polynomial $\omega(x) = x^8 + x^6 + x^5 + x^3 + 1$. The RS matrix is given as follows:

$$\begin{bmatrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{bmatrix}$$

To produce the subkeys K_i, the same S-boxes are used as in function g. The input is $(2i)!$ and is of 64 bits, where i is the number of rounds.

F. THE ALGORITHM

In this section, the algorithm for the proposed chain ring cryptosystem is stated. The Encryption scheme is as follows:

Input: Plain text P, User key K, Block Size B
Output: Cipher Text C
Algorithm Body:
Begin

G. BEGIN KEY SCHEDULE

1. Read user key K
2. Generate Sub keys S_0, S_1 by calling the subkey generation function.
3. Generate round keys K by calling encryption function F and using the initial agreed-upon values as the random input to the function.
4. Repeat step 3 to generate all the round keys.

End Key Schedule;

H. BEGIN ENCRYPTION

5. Read a block B from the Message P into the message cache.
6. Divide the block into Left and Right sub-blocks.
7. Encrypt the Left block by calling encryption function F.
8. Perform XOR of the right block with the resulting block of step 7.
9. Swap the result of step 8 with the input block of step 7.
10. Repeat step 7 and step 8 for 16 rounds.
11. Combine the resulting blocks in one block.
12. If message P is not finished
13. Load the next block into the message cache.
14. Go to step 6.

Else if the message is finished then Halt.
End Encryption;
End;

I. FUNCTION F ENCRYPTION

Begin

1. Read the Left Block.
2. Read the round key.
3. Perform rotation, Q-permutation, MDS matrix multiplication, PHT, and subkey XOR.
4. Store the resulting block.

End;

Flow chart for enciphering scheme using improved TWOFISH algorithm is given in Figure 1.

V. CORRECTNESS PROOF USING TEST VECTOR

The modified TWOFISH algorithm takes an input of size 128 and a key of variable length 128 or 192 or 256. The original explicit pseudo-code for defining the algorithm was transformed to a strictly functional form in the formalization, which served as both an executable model and the code tested in the correctness proof. Using function composition, we can describe the encryption (TWOFISH) and decryption (TWOFISH_INV) functions as follows:

```
TWOFISH keys = from_state_vector ∘
Round 16 ∘ AddRoundKey ∘
to_state_vector
TWOFISH _INV-keys =
from_state_vector ∘ InvRound 16 ∘
AddRoundKey ∘ to_state_vector
```

TWOFISH takes a key schedule (a list of keys), while TWOFISH_INV takes the key schedule in reverse. The encrypted copies the input vector, 'xors' with the first key, and then processes it for 16 rounds. Each round consumes one key from the key plan. Onward the F-function is applied.

A. ENCRYPTION OF A ROUND

Divide the 128-bit plaintext to two 64-bit blocks and process the left 64-bit as follows:

```
F-function (64-bit vector) =
PHT(left_rotate (g-function(64-bit
vector))) ⊕ key

g-function(64-bit vector) =
MDS(Subbytes_state(64-bit vector))
```

B. DECRYPTION OF A ROUND

```
INV_F-function (64-bit vector) =
INV_PHT(Right_rotate (INV_g-
function(64-bit vector))) ⊕ (key in
reverse order)

INV_g-function(64_bit vector) =
INV_MDS(INV_Subbytes_state)
```

C. BYTE SUBSTITUTION AND ITS INVERSE SUBSTITUTION

As the S-box consists of units elements therefore, they have inverse for each element. The S-box on a single byteis applied in the following manner:

$$\begin{aligned} Let\ plaintext &= 114\,(dec) = 1110010\,(bin) \\ &= x + x^4 + x^5 + x^6 \\ S - box &= 81 = 1010001 = 1 + x^4 + x^6 \\ C &= S - box(plaintext) \\ &= (1 + x^4 + x^6)(x + x^4 + x^5 + x^6) \\ &= x + x^4 + x^5 + x^6 + x^5 + x^8 + x^9 \\ &\quad + x^{10} + x^7 + x^{10} + x^{11} + x^{12} \end{aligned}$$

Now delete higher terms than degree 7 and take mode 2 we get:

$$C = x + x^4 + x^6 + x^7$$

This is the output of the proposed Subbyte step.

Now let apply the inverse S-box on this C.

$$\begin{aligned} INV\_S - box\,(C) &= \left(1 + x^4 + x^6\right)\left(x + x^4 + x^6 + x^7\right) \\ &= x + x^4 + x^6 + x^7 + x^5 + x^8 + x^{10} \\ &\quad + x^{11} + x^7 + x^{10} + x^{12} + x^{13} \end{aligned}$$

Now delete higher terms than degree 7 and take mode 2 we get:

$$INV\_S - box\,(C) = x + x^4 + x^6 + x^5 = plaintext$$

VI. SECURITY ANALYSIS

We have performed analysis on various digital images to approve the certainty and execution of the designed algorithm of TWOFISH. These analyses consist of authentic testing and exploration with subtleness and raggedness tests for the enciphered images. The analysis techniques are explained in the accompanying subsections.

A. ANALYSIS OF CONSISTENCY OF IMAGE PIXELS

The image histogram defines the tonal distribution of pixels of an image. A secured encryption structure creates the enciphered digital images with undifferentiated histograms that have the power to cope with statistical strikes and thrashes. The histograms for the various standard original and encrypted images are displayed in Figures 2, 3, and 4. In the 1st row of each of these Figures, the sharp peaks and un-balanced data show the uneven pixel distribution of the original images. Whereas, the histograms in the 2nd row of each figure reveals uniform pixel distribution. The value for each pixel is turned out to be approximately equal. These results guarantee the difficulty an intruder can face to obtain the original image by statistically analyzing pixels approximation of encrypted image.

The histogram pins of R, G, and B components of enciphered and ciphered images in Figures (2-4) indicate the resistivity of the proposed cipher against the brute force attack.

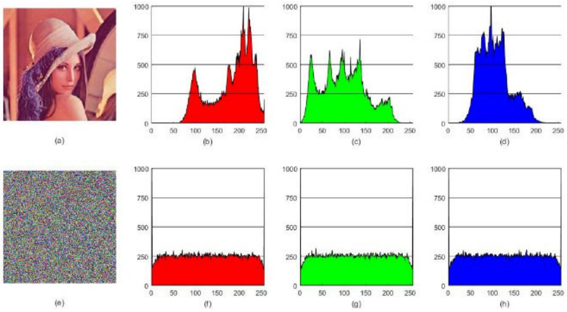

FIGURE 2. The 1st row represents Lena original image with its corresponding R, G, B layers histogram, denoted by (a), (b), (c) and, (d) respectively. The 2nd row represents Lena ciphered image with its corresponding R, G, B layers histogram, denoted by (e), (f), (g) and, (h) respectively.

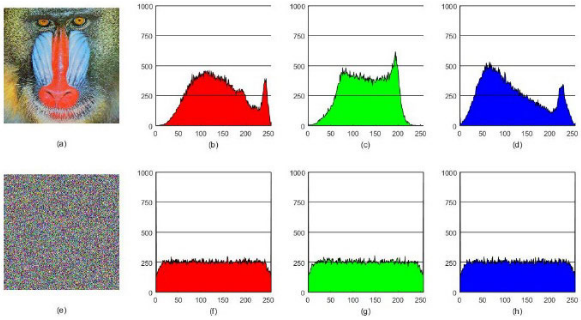

FIGURE 3. The 1st row represent Baboon original image with its corresponding R, G, B layers histogram, denoted by (a), (b), (c) and (d) respectively. The 2nd row represent Baboon ciphered image with its corresponding R, G, B layers histogram, denoted by (e), (f), (g) and (h) respectively.

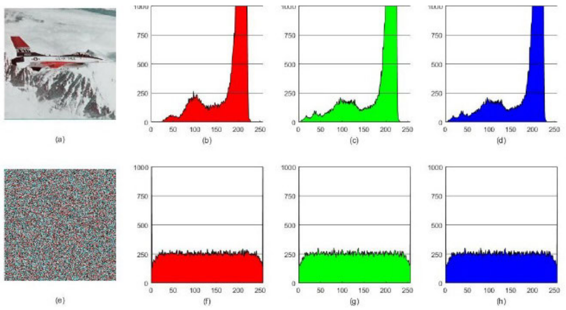

FIGURE 4. The 1st row represents Aeroplane original image with its corresponding R, G, B layers histogram, denoted by (a), (b), (c), and (d) respectively. The 2nd row represent the Aeroplane ciphered image with its corresponding R, G, B layers histogram, denoted by (e), (f), (g), and (h) respectively.

B. CORRELATION ANALYSIS FOR NEIGHBORING PIXELS

In the correlational analysis, we examine the interdependence of adjacent pixels of original and enciphered combined images. The correlation coefficients $\sigma_{X,Y}$ of two bordering pixels can be deduced by:

$$\sigma_{X,Y} = \frac{Cov(X,Y)}{\sqrt{Var\,(X)\,.Var(Y)}}$$

where X and Y are the assessments of two bordering pixels at grayscale in the image, $Cov(X,Y)$ defines the value of

TABLE 6. Lena's correlation.

(a): Horizontal Correlation				
		Red	**Green**	**Blue**
Original Image, I	**R**	0. 9577	0. 8596	0. 6632
	G	0. 6631	0. 9578	0. 9214
	B	0. 6534	0. 8701	0. 9080
Encrypted Image, E	**R**	0.0073	-0.0305	0.0743
	G	-0.0417	-0.023	0.0017
	B	-0.0338	-0.0323	-0.0321
(b): Vertical Correlation				
		Red	**Green**	**Blue**
I	**R**	0. 9828	0. 8654	0. 7116
	G	0. 7189	0. 9762	0. 9679
	B	0. 7071	0. 8907	0. 9540
E	**R**	-0. 0156	0. 0744	0. 0031
	G	0. 0230	0. 0075	-0. 0165
	B	0. 0372	0. 0468	0. 0303
(c): Diagonal Correlation				
		Red	**Green**	**Blue**
I	**R**	0. 9375	0. 8246	0. 6267
	G	0. 6500	0. 9192	0. 8897
	B	0. 6426	0. 8534	0. 9010
E	**R**	0. 0275	-0. 0039	-0. 0160
	G	0. 0152	-0. 0712	-0. 0223
	B	-0. 0363	-0. 0043	-0. 0243

TABLE 7. Baboon's correlation.

(a): Horizontal Correlation				
		Red	**Green**	**Blue**
Original Image, I	**R**	0.8543	0.2107	0. 0983
	G	0. 0219	0. 7058	0. 7691
	B	0. 0292	0. 5686	0. 8097
Encrypted Image, E	**R**	-0.0097	-0.0066	0.0585
	G	-0.0275	-0.007	-0.015
	B	-0.0305	-0.0181	-0.0319
(b): Vertical Correlation of Multiple Original and Encrypted Image				
		Red	**Green**	**Blue**
I	**R**	0. 7915	0. 1036	0. 0038
	G	0. 0277	0. 6663	0. 7868
	B	0. 0457	0. 5370	0. 7737
E	**R**	-0. 0246	-0. 0078	-0. 0286
	G	-0. 0264	0.0538	-. 0.0504
	B	-0. 0110	0. 0017	-0. 0059
(c): Diagonal Correlation				
		Red	**Green**	**Blue**
I	**R**	0. 7918	0. 1754	-0. 0022
	G	-0. 0340	0. 6502	0. 7614
	B	-0.0132	0. 5373	0. 7650
E	**R**	-0.0118	-0.041	0.0131
	G	0.0147	0.0175	0.0073
	B	0.0331	0.0027	0.0114

TABLE 8. Aeroplan's correlation.

(a): Horizontal Correlation				
		Red	**Green**	**Blue**
Original Image, I	**R**	0.9199	0. 8537	0. 8916
	G	0. 8861	0. 9297	0. 9184
	B	0. 8568	0. 9126	0. 9261
Encrypted Image, E	**R**	0. 0063	0.0012	-0.0073
	G	-0.0038	0. 0023	0. 0009
	B	0.0025	-0.0091	0. 0069
(b): Vertical Correlation				
		Red	**Green**	**Blue**
I	**R**	0. 8978	0. 8652	0. 8527
	G	0. 8451	0. 9027	0. 9149
	B	0. 8349	0. 9105	0. 8994
E	**R**	-0.0103	-0.0003	-0.0011
	G	-0.0009	-0.0032	-0.0013
	B	0. 0066	-0.01	0. 0002
(c): Diagonal Correlation				
		Red	**Green**	**Blue**
I	**R**	0. 7984	0. 8180	0. 8150
	G	0. 7918	0. 8799	0. 8432
	B	0. 7801	0. 8760	0. 8484
E	**R**	0.0095	0. 0011	-0.0054
	G	0.0099	-0.0015	-0.0038
	B	-0.01	-0.0047	-0.0007

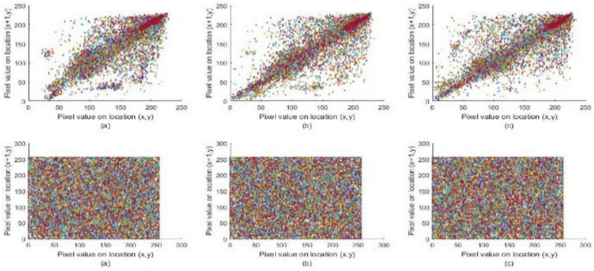

FIGURE 5. (a), (b), and (c) shows Original image horizontal correlation for R, G, and B layer, respectively. Whereas, there corresponding encrypted channels are shown in the 2nd row respectively.

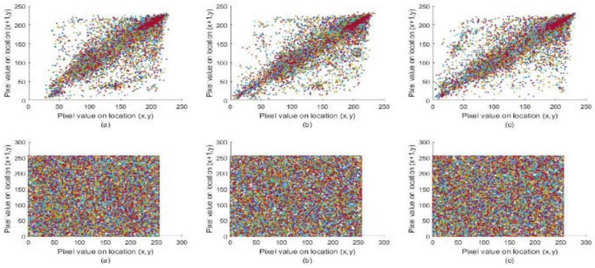

FIGURE 6. (a), (b), and (c) shows Original image vertical correlation for R, G and B layer, respectively. Whereas, there corresponding encrypted channel are shown in the 2nd row respectively.

covariance, $Var\ (X)$ and $Var(Y)$ is the measure of distinctness of components X and Y separately. The coefficients of correlation for the original and ciphered images corresponding to figures (5-7) are displayed in Table (6-8). The high correlation of the neighboring pixels of original images is turned into a very weak correlation after being encrypted.

The correlation distribution of sample images, Lena, Baboon, and Airplane's original and encrypted images are shown in Figure (5-7). The analyses of these correlations from the given figures and stated tables (6-8) reveals the ability of the proposed algorithm to discard the correlation between the neighboring pixels. The alignment of dots along the diagonal lines indicates the strong correlation between the neighboring pixels, while for the encrypted images these dots are scattered, showing the reduced correlation between these pixels.

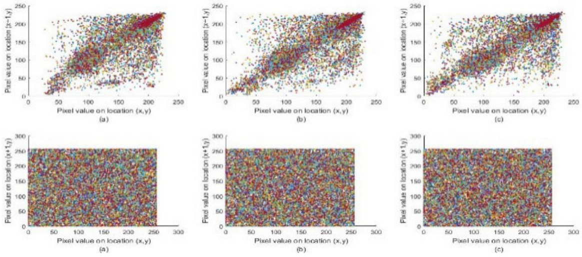

FIGURE 7. (a), (b), and (c) shows Original image diagonal correlation for R, G, and B layer, respectively. Whereas, there corresponding encrypted channels are shown in the 2nd row respectively.

C. MAXIMUM DEVIATION

The statistical security of the encryption scheme can be measured using Maximum Deviation. It measures the deviation of the values of pixels of the ciphered image from the pixel values of the original image. The larger value of maximum deviation indicates the greater deviation and hence stronger security. The formula to calculate the maximum deviation is given as follows:

$$\mathcal{M}_d = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i$$

where h_i denotes the difference between the count value of the histogram of an original and ciphered image.

Table 9 shows the results of Maximum deviation for the images of Lena, Baboon, and Airplane.

TABLE 9. Maximum Deviation of different RGB 256 × 256 images and their corresponding layers.

Images		Maximum Deviation			
	Ref. [17]	Color Image	Red Channel	Green Channel	Blue Channel
Lena	14390	83452	50661	38175	61339
Baboon	18265	85385	31418	43424	28537
Airplane	18774	199792	68009	67215	67215

The large values of maximum deviation in Table 9 indicate the greater difference between the corresponding pixels of an original and ciphered image. Hence showing the proficiency of the proposed algorithm.

D. IRREGULAR DEVIATION

A strong cipher should be capable of changing the pixel's values randomly. The cipher that lacks this property, that is, for some pixel values the change is large while for others it is insignificant, is not considered as secure. The strength of statistical robustness can be measured by calculating irregular deviation using the following formula:

$$I_d = \sum_{i=0}^{255} |h_i - M_h|$$

where h_i denotes the difference between the count value of histogram of original and ciphered image. M_h denotes the mean value of h_i. Smaller value of I_d is an indication that the encryption is uniform and hence the cipher possesses the statistical strength.

Table 10 shows the results of Irregular deviation for the images of Lena, Baboon and Airplane.

TABLE 10. Irregular deviation of different RGB 256 × 256 images and their corresponding layers.

Images	Irregular Deviation			
	Color Image	Red Channel	Green Channel	Blue Channel
Lena	56152	29502	21405	30372
Baboon	38304	15693	13674	16500
Airplane	150140	51185	51762	51762

The values stated in Table 10 indicates the small randomness in deviation. Hence showing the proficiency of the proposed algorithm.

E. INTENSITY HISTOGRAM

The pixel appearance of an image is controlled by the intensity of R, G, and B components of the image. This value of intensity decides the amount of information stored in the pixel. The color depth deals with the pixel colors. Figure 8, 9, and 10 gives the count of pixel satisfying the intensity level over the image. For the sample images of 'Lena', 'Baboon' and 'Airplane' the 3-D intensity histograms of original and ciphered images elucidates the uniformity of color intensities of encrypted images in comparison with the non-uniform 3-D color intensities of the original image. Thus, guarantying the robustness of cipher against adversaries.

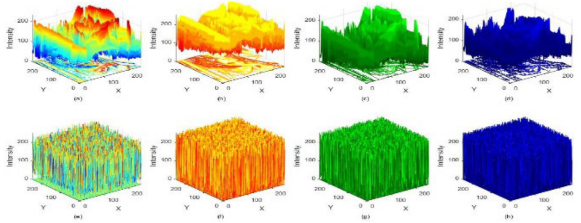

FIGURE 8. (a) is Lena Intensity histogram whereas, (b), (c), and (d) represents intensity histogram of R, G and B layers respectively. (e) is Lena encrypted image intensity histogram whereas, (f), (g) and (h) represents intensity histogram of R, G, and B layers respectively.

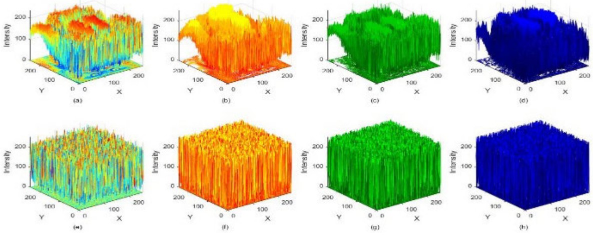

FIGURE 9. (a) is Baboon Intensity histogram whereas, (b), (c), and (d) represents intensity histogram of R, G, and B layers respectively. (e) is Baboon encrypted image intensity histogram whereas, (f), (g) and (h) represents intensity histogram of R, G, and B layers respectively.

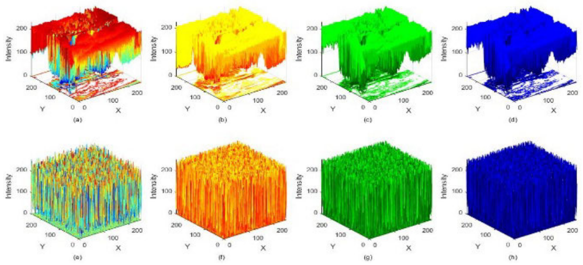

FIGURE 10. (a) is Airplane Intensity histogram whereas, (b), (c), and (d) represents intensity histogram of R, G, and B layers respectively. (e) is Aeroplane encrypted image intensity histogram whereas, (f), (g) and (h) represents intensity histogram of R, G and B layers respectively.

The histogram pins of encrypted images in Figures (8-10) show the uniformity in intensity, hereby revealing very little information stored at every pixel. Thus proving the robustness of the cipher.

VII. MEASUREMENTS BASED ON PIXEL MODIFICATION

The assessment for the quality of the image is dependent on the pixel difference technique that has been performed by calculating MSE, MD, AD, SC, NAE, NCC, PSNR, AD, and MSE values. This provides error benchmarks used to connect different images.

A. MSE AND PSNR ANALYSIS

The encryption scheme must create heterogeneity between the original and encrypted digital image by appending noise to the accurate content. Mean square error has been carried out between original and encrypted image to check the quality of encryption. MSE is given as follows:

$$MSE = \frac{\sum_{i=1}^{O} \sum_{j=1}^{P} (P_{ij} - C_{ij})2}{O \times P}$$

where P_{ij} and C_{ij} are the position of pixels situated in the ith row and jth column of the original and encrypted image respectively. The large value of MSE implies strong encryption security. The distinctiveness of encrypted image is evaluated by exploiting PSNR (peak signal to noise ratio) which is given by the following expression:

$$PSNR = 20log_{10}[\frac{I_{max}}{\sqrt{MSE}}]$$

whereas I_{max} is the largest value for pixel estimation of the image. A strongly encrypted image must have a low PSNR.

Table 11 shows the PSNR and MSE values of the original and enciphered Lena images.

B. NORMALIZED ABSOLUTE ERROR

Normalized absolute error (NAE) is expressed as follows:

$$NAE = \frac{\sum_{m=1}^{O} \sum_{n=1}^{P} |P_{mn} - C_{mn}|}{\sum_{m=1}^{O} \sum_{n=1}^{P} |C_{mn}|}$$

This distribution reveals how digitally isolated an encrypted image is from the original one.

C. MAXIMUM DIFFERENCE

MD (Maximum Difference) provides the between original and encrypted image. A higher MD value implies stronger encryption. It is given as follows:

$$MD = \max |P_{ij} - C_{ij}| \quad \text{Whereas,} \quad i = 1, 2, \ldots, m \text{ and } \quad j = 1, 2, \ldots, n.$$

D. AVERAGE DIFFERENCE

The average difference can be defined as the pixel dissimilarities between the original and its corresponding encrypted image. A large value of the AD indicates the significant strength of the image encryption scheme (see Table 11). AD can be expressed as follows:

$$AD = \frac{1}{O \times P} \sum_{i=1}^{O} \sum_{j=1}^{P} (P_{ij} - C_{ij})$$

The average difference for two similar images is ideally zero.

E. SIMILARITY MEASURES

To assess the affinity between two signals, the criteria like structural content, structural similarity, and cross-correlation are used. For the assessment of signals from the perspective of comparison and divergence, other methods exist. Recognition is used to match the corresponding pixels of two images. But this method is limited due to some conditions. So, to illustrate the differences between original and encrypted images, standardized correlation and structural correlations are used.

F. NORMALIZED CROSS CORRELATION

To check the similarity between two images the criteria of normalized correlation is used. The little sensitivity towards the linear changes gives normalized cross-correlation as well as common correlation an upper hand among other criteria. NCC takes the values between −1 and 1. The allocation of position bounds is comparatively easier in NCC as compared to cross-correlation. The main aim of NCC is to analyze the interdependence of color between two images, be it the plain and encrypted images. The correlated measures are assigned the value of 1 and the dissimilar ones are assigned zero. For every image, the resemblance count is dependent on the varieties of utilizing cross-correlation, hence is computed accordingly. The mathematical expression that defines the normalized correlation is given as follows

$$NCC = \frac{\sum_{i=1}^{O} \sum_{j=1}^{P} |P_{ij} - C_{ij}|}{\sum_{j=1}^{P} P_{ij}^2}$$

where O × P denotes the size for plain (P) and encrypted image (C). The deviation of the NCC value from unity indicates the strong dissimilarities present between the pixels of the original and the encrypted image. (See Table 11).

G. STRUCTURAL CONTENT

Structural content is an important criterion that is used to get the statistics of weights of the original image against

TABLE 11. Quality measure analysis of improved TWOFISH algorithm based encrypted Lena image 36.

No.	Quality measure	Encryption based on improved TWOFISH algorithm			Optimal values		
		Red	Green	Blue	Red	Green	Blue
5.1	**MSE**	10654.2	8915.75	7129.88	10680.6	9047.11	7311.82
5.1	**PSNR**	7.8556	8.62922	9.59998	7.84485	8.56571	9.49055
5.2	**NAE**	0.469382	0.78452	0.669749	0.470065	0.79014	0.678703
5.3	**MD**	255	230	212	255	219	224
5.4	**AD**	52.0839	-28.4671	-21.9503	52.081	-28.9503	-22.4915
5.5	**SSIM**	0.00596501	0.0100766	0.0114185	0.00764174	0.00761283	0.00849676
5.6	**NCC**	0.66129	1.01568	1.09357	0.659053	1.00999	1.08712
5.7	**SC**	1.58737	0.571316	0.565316	1.59765	0.572897	0.56569

the encrypted one. The better-quality encryption gives the encrypted, the value of 1. Whereas, the greater value of SC indicates the low quality of the image. Structural content is defined as:

$$SC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (P\,(i,j))^2}{\sum_{i=1}^{m} \sum_{j=1}^{n} (C\,(i,j))^2}$$

Due to the confusion and diffusion layer in the encryption scheme, the value of SC is not usually close to unity. If the standard color layers (red, green, and blue) in an image are cross-hatched then the value of SC is not close to one.

H. ENTROPY INVESTIGATION

Entropy is used to access the increase of grayscale estimations and assessments of the images. The sharper the image is, the greater the entropy is. Smoother areas of the image show less entropy. For an asymmetrical image having 256 gray levels, the most perfect desirable entropy is 8 [18]. However, the entropy of the encrypted image is under 8, as the regularity in the image is expected. Mathematically, entropy H can be represented for a data source z_i is delineated as:

$$H = -\sum_{i=0}^{2^N-1} p(z_i) log_2 p(z_i)$$

where z_i in this condition is called source image and 2N is the total states of information. For completely scattered source displaying signs, entropy should be N. For ideally unpredictable digital content, the estimation of perfect information entropy is 8.

For the color image of 'Lena (256 x 256)', the values for entropy are evaluated and are stated in Table-12. These values are very close to the optimal value of 8. It verifies the strength of the proposed cipher.

TABLE 12. Comparing entropy for Lena (256 × 256) image.

	Red	Green	Blue	RGB Image
Proposed	7.9575	7.9538	7.9578	7.9555
Ref. [19]	7.8693	7. 8693	7. 8693	7. 8693
Ref. [20]	7.7260	7. 7260	7. 7260	7. 7260
Ref. [21]	7.9976	7.9974	7.9977	7.9979
Ref. [22]	7.9968	7.9968	7.9968	7.9968

VIII. VITALITY AGAINST DIFFERENTIAL ATTACK

The randomization of any encryption scheme can be assessed by evaluating the value of diffusion. A good encryption algorithm satisfies the avalanche effect, which is sensitive even against the slightest change in the original image e.g. [23]–[26]. So, a good diffusion property prevents the adversary to make minor advancements by changing only a single pixel and observing the differences in the encrypted image. This property is a very vital tool to protect the image against differential cryptanalysis.

To assess the diffusion property of the encryption scheme, a single bit of plain image is changed, and the relation of difference between the encrypted images is tested. The results for MSE, PSNR, NCC, AD, SC, MD, and NAE of the resulting image are stated in Table 13.

TABLE 13. Differential analyses of the proposed scheme tested for Lena ciphered image.

Schemes	NPCR			UACI		
	R	G	B	R	G	B
Proposed	**0.9956**	**0.9960**	**0.9958**	**0.3386**	**0. 3355**	**0. 3346**
Ref. [1]	0.9962	0.9962	0.9962	0.3053	0.3053	0.3053
Ref. [21]	0.9959	0.9959	0.9959	0.3355	0.3355	0.3355
Ref. [19]	0.9963	0.9963	0.9963	0.3347	0.3347	0.3347
Ref. [27]	0.9953	0.9953	0.9953	0.3340	0.3340	0.3340

The values stated in Table 13 reflect the sound resistivity of the proposed algorithm against the differential cryptanalysis.

IX. COMPLEXITY OF ALGORITHM

In this section, we figure out the complexity of the enciphering algorithm. The algorithm has four key stages. Image splitting to blocks, F-function and PHT key whitening. Initially, we split an astronomical digital RGB image into 16 × 16 matrices. Each matrix is then partitioned to 128-bit bit blocks. After this, we apply the F-function and the PHT. In the last, we apply key whitening to get the output of the 1st round. The process is repeated for 16 rounds to get the ciphered image.

We split Lena RGB image of size $N \times N \times 3$ into blocks of 16×16 matrices that results $[\frac{N^2}{256} \times 3]$ matrices. Then we partitioned each channel in 128-bit blocks to obtain $\left[\frac{N^2}{256} \times 3 \times 128\right]$. We an exclusive or operation and then apply the F-function. The complexity of XOR operation is $O(N)$. The F-function consists of g-function (i.e. substitution using

TABLE 14. Specification of the computer system used for implantation of the proposed and classical TWOFISH algorithm.

Features	Specifications
Processor clock	Intel® Core ™ I5-5300U CPU
Memory	8.00 GB RAM
Speed	@2.29 GHz
O.S.	Windows 10 pro, C++ Compiler

TABLE 15. The execution time of the proposed and classical TWOFISH algorithm in seconds.

Packet Size	35KB	80Kb	260Kb	550Kb
Proposed Algorithm	**86.70 sec**	**206.11 sec**	**563.01 sec**	**1063 sec**
Classical TWOFISH	129.0 sec	305.27 sec	984.6 sec	2092 sec

S-box and multiplication with MDS) and PHT. As the S-box is constructed over unit element of the commutative chain ring $\frac{F_2[u]}{<u^8>}$, therefore, has complexity $O(4\,log\,4)$ and as a result, the complexity of becomes $O\,(\mathrm{N}) \times O\left(4^2 \log_2 4\right) \times \left[\frac{N^2}{256} \times 3 \times 128\right] = O(48N^2)$. Also the MDS operates over field F[x] and so has a complexity of $O(4log4)$. Also the PHT has a complexity of $4\,log\,4$. Thus the computing complexity of the proposed Twofish algorithm is: $O\left(48N^2\right) \times O\,(4\,log\,4) \times O\,(4\,log\,4) = O(768N^2)$

This indicates that the proposed Twofish algorithm is of low complexity and therefore a small encryption scheme of high-security may substitute most of the prevailing encryption schemes.

X. EXECUTION TIME OF ALGORITHM

The implementation of the algorithm is done using C++ language; a widely used language in algorithms implementation. We used a 128-bits sized key to encrypt the files of various sizes. The results of which are being compared with the classical TWOFISH presented in [28]. The specifications of the computers used for the implementation of the proposed algorithm and the Classical TWOFISH are given in Table 14.

The packet sizes of data are taken as 35kb, 80kb, 260kb, and 550kb. The speed comparison reflects the better time complexity of the proposed algorithm. Table 15 displays the comparison of speeds.

XI. RANDOMNESS TEST FOR CIPHER

Factors like period, complexity, distribution, and output data define the level of security for any cryptosystem. A secure

TABLE 16. NIST test results for improved TWOFISH algorithm based encrypted image.

Test		P – values for RGB ciphering of the encrypted image			Results
		Red	Green	Blue	
Frequency		0.049924	0.52709	0.82481	Pass
Block frequency		0.19339	0.78397	0.95035	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs (M=10,000)		0.50781	0.25755	0.39277	Pass
Long runs of ones		0.7127	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.81656	0.85988	Pass
No overlapping templates		1	0.9994	1	Pass
Spectral DFT		0.059263	0.24574	0.38399	Pass
Approximate entropy		0.19896	0.57537	0.068134	Pass
Universal		0.99561	0.9932	0.98611	Pass
Serial	p values 1	0.008021	0.12601	1.16E-05	Pass
Serial	p values 2	0.16895	0.16198	9.11E-08	Pass
Cumulative sums forward		0.11794	0.1676	0.24053	Pass
Cumulative sums reverse		1.93	1.0832	0.98972	Pass
Random excursions	X = -4	0.39711	0.053665	0.55621	Pass
	X = -3	0.64709	0.56457	0.74449	Pass
	X = -2	0.84521	0.50979	0.016796	Pass
	X = -1	0.89596	0.80131	0.68123	Pass
	X = 1	0.78446	0.4257	0.89843	Pass
	X = 2	0.55653	0.66347	0.58613	Pass
	X = 3	0.19305	0.73121	0.67613	Pass
	X = 4	0.55765	0.96861	0.70378	Pass
Random excursions variants	X = -5	0.52652	0.004606	1.70E-05	Pass
	X = -4	0.38467	0.037635	0.001341	Pass
	X = -3	0.28313	0.37109	0.048107	Pass
	X = -2	0.2987	0.5637	0.35833	Pass
	X = -1	0.27133	0.45325	0.85968	Pass
	X = 1	0.84148	1	0.59588	Pass
	X = 2	0.84148	0.77283	0.30743	Pass
	X = 3	0.59151	0.43385	0.30407	Pass
	X = 4	0.85011	0.44969	0.59298	Pass
	X = 5	0.94685	0.50499	0.90619	Pass

cryptosystem has high value for complexity, a long period and it distributes the input data uniformly. We have measured these parameters by using NIST.SP 800-22 [29] test. The test is applied to the colored image of Specimen Lena. The results indicate that the chain-ring based TWOFISH algorithm passes all the security threats. The result of this test is stated in Table 16.

Table 16 confirms that the presented scheme for encryption qualifies the entire NIST tests and therefore guarantees the safety of the modified TWOFISH algorithm.

XII. CONCLUSION

In this paper, the mathematical complexity of the proposed TWOFISH algorithm is improved by using substitution boxes drawn from a multiplicative group of chain ring $\frac{F_2[u]}{<u^8>}$. As these S-boxes have the property of having copious generators, they, therefore, produce a strong algebraic complexity. Additionally, we have changed the time complexity of the TWOFISH algorithm by processing a 64-bit block and reducing the total number of subkeys. Moreover, the proposed cipher is tested on various standard color digital images of size 256 × 256.

The Cipher computation speed is compared with the speed of the standard TWOFISH algorithm and found that the newly designed algorithm is quite fast. The multiple generators for S-box add to the confusion in different layers of digital images. For security analysis and quality assessment, various statistical tests are performed on the standard encrypted images. The results recommend that the proposed algorithm is a strong candidate for digital image encryption.

REFERENCES

[1] T. Shah, T. U. Haq, and G. Farooq, "Improved SERPENT algorithm: Design to RGB image encryption implementation," *IEEE Access*, vol. 8, pp. 52609–52621, 2020.

[2] H. S. Mondal, M. T. Hasan, M. M. Hossain, M. M. Arifin, and R. Saha, "A RSA-based efficient dynamic secure algorithm for ensuring data security," in *Proc. Int. Joint Conf. Comput. Intell.*, 2020, pp. 643–653.

[3] M. M. R. Kishore, M. T. S. Anudeep, M. K. S. Patel, and M. A. R. Reddy, "Secure communication for messaging using AES or DES," *Purakala UGC CARE J.*, vol. 31, no. 27, pp. 124–130, May 2020.

[4] A. A. Thinn and M. M. S. Thwin, "A hybrid solution for confidential data transfer using PKI, modified AES algorithm and image as a secret key," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, Feb. 2020, pp. 1–4.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[6] H. Feistel, "Cryptography and computer privacy," *Sci. Amer.*, vol. 228, no. 5, pp. 15–23, May 1973.

[7] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proc. IEEE*, vol. 63, no. 11, pp. 1545–1554, Nov. 1975.

[8] W. Fumy, "On the F-function of FEAL," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1987, pp. 434–437.

[9] B. Den Boer, "Cryptanalysis of FEAL," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, 1988, pp. 293–299.

[10] T. ul Haq and T. Shah, "12×12 S-box design and its application to RGB image encryption," *Optik*, vol. 217, Sep. 2020, Art. no. 164922.

[11] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Appl. Cryptograph. Techn.*, 1985, pp. 523–534.

[12] L. Jing-Mei, W. Bao-Dian, C. Xiang-Guo, and W. Xin-Mei, "Cryptanalysis of rijndael S-box and improvement," *Appl. Math. Comput.*, vol. 170, no. 2, pp. 958–975, Nov. 2005.

[13] T. Shah, S. Jahangir, and A. A. de Andrade, "Design of new 4 × 4 S-box from finite commutative chain rings," *Comput. Appl. Math.*, vol. 36, no. 2, pp. 843–857, Jun. 2017, doi: 10.1007/s40314-015-0265-9.

[14] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, and M. Stay, "The Twofish team's final comments on AES selection," *AES Round*, vol. 2, pp. 1–13, May 2000.

[15] T. Abualrub and I. Siap, "Cyclic codes over the rings Z_2+ uZ_2 and Z_2+ uZ_2+ u^2 Z_2," *Des., Codes Cryptogr.*, vol. 42, pp. 273–287, Feb. 2007.

[16] M. M. Al-Ashker and J. Chen, "Cyclic codes of arbitrary length over F_q+ uF_q+ u^2F_q+...+u^{k-1}F_q," *Palest. J. Math*, vol. 2, no. 1, pp. 72–80, 2013.

[17] C. B. B. Aguila, A. M. Sison, and R. P. Medina, "Performance evaluation of enhanced RC6 permutation-diffusion operation in securing images," in *Proc. 2nd Int. Conf. Softw. Eng. Inf. Manage.*, 2019, pp. 180–184.

[18] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

[19] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019.

[20] A. H. Jassem, A. T. Hashim, and S. A. Ali, "Enhanced Blowfish algorithm for image encryption based on chaotic map," in *Proc. 1st Int. Conf. Comput. Appl. Sci. (CAS)*, Dec. 2019, pp. 232–237.

[21] X. Zhang, L. Wang, G. Cui, and Y. Niu, "Entropy-based block scrambling image encryption using DES structure and chaotic systems," *Int. J. Opt.*, vol. 2019, pp. 1–13, Aug. 2019.

[22] A. H. Jassem, A. T. Hashim, and S. A. Ali, "Enhanced blowfish algorithm for image encryption based on chaotic map," in *Proc. 1st Int. Conf. Comput. Appl. Sci. (CAS)*, Dec. 2019, pp. 232–237.

[23] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," *Inf. Sci.*, vol. 520, pp. 177–194, May 2020.

[24] D. Shah, T. Shah, and S. S. Jamal, "A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation," *Multidimensional Syst. Signal Process.*, vol. 31, no. 3, pp. 1–21, Jul. 2020, doi: 10.1007/s11045-019-00689-w.
RP-5: Ref. [24] Volume 31, issue 3, July 2020 DOI: https://doi.org/

[25] T. ul Haq and T. Shah, "Algebra-chaos amalgam and DNA transform based multiple digital image encryption," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102592.

[26] W. Song, Y. Zheng, C. Fu, and P. Shan, "A novel batch image encryption algorithm using parallel computing," *Inf. Sci.*, vol. 518, pp. 211–224, May 2020.

[27] R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali, and J. J. P. C. Rodrigues, "Chaos based enhanced RC5 algorithm for security and integrity of clinical images in remote health monitoring," *IEEE Access*, vol. 7, pp. 52858–52870, 2019.

[28] H. Harahsheh and M. Qatawneh, "Performance evaluation of Twofish algorithm on IMAN1 supercomputer," *Int. J. Comput. Appl.*, vol. 179, no. 50, pp. 1–7, Jun. 2018.

[29] F. Pareschi, R. Rovatti, and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 491–505, Apr. 2012.

[30] G. F. Siddiqui, M. Z. Iqbal, K. Saleem, Z. Saeed, A. Ahmed, I. A. Hameed, and M. F. Khan, "A dynamic three-bit image steganography algorithm for medical and e-healthcare systems," *IEEE Access*, vol. 8, pp. 181893–181903, 2020.

TANVEER UL HAQ is currently pursuing the Ph.D. degree with the Mathematics Department, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include steganography, watermarking, and algebraic cryptography.

TARIQ SHAH received the degree from the University of Karachi, in 1986, the M.Sc. and M.Phil. degrees in mathematics from Quaid-i-Azam University (QAU), Islamabad, Pakistan, in 1989 and 1991, respectively, and the Ph.D. degree in mathematics from the University of Bucharest, Romania, in 2000. He is currently working as a Tenured Professor with the Department of Mathematics, QAU. His research interests include commutative algebra, non-associative algebra, error correcting codes, cryptography, and computational economics. He is a member of different academic bodies of the QAU and the HEC approved Ph.D. Supervisor.

GHAZANFAR FAROOQ SIDDIQUI received the Ph.D. degree from Vrije Universiteit Amsterdam, The Netherlands, in 2010. He was a Research Scholar with the Department of Computer Science, Vrije Universiteit Amsterdam. He is currently an Assistant Professor with the Department of Computer Science, Quaid-i-Azam University, Islamabad. His Ph.D. scholarship was funded by the Higher Education Commission, Pakistan. He published numerous research articles in reputed conferences and Journals. He is a member of the Federal Public Service Commission, the Khyber Pakhtunkhwa Public Service Commission, the Board of Studies of Quaid-i-Azam University, Islamabad, and National Textile University, Faisalabad. He is also serving as an Evaluator for scientific projects of Directorate of Science and Technology (DoST)—Khyber Pakhtunkhwa. He is also a reviewer of a number of peer reviewed conferences and journals.

MUHAMMAD ZAFAR IQBAL is currently a Ph.D. Scholar with the Department of Computer Science, Quaid-i-Azam University, Islamabad. He is also a Faculty Member of computer science with The Islamia University of Bahawalpur. His research interests include image analysis and processing, computer vision, artificial intelligence, and machine learning.

IBRAHIM A. HAMEED (Senior Member, IEEE) received the Ph.D. degree in industrial systems and information engineering from Korea University, Seoul, South Korea, and the Ph.D. degree in mechanical engineering from Aarhus University, Aarhus, Denmark. He is currently a Professor with the Department of ICT and Natural Sciences, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology (NTNU), Norway, where he is the Deputy Head of research and innovation. He is the author of more than 120 journal articles and conference papers. His current research interests include artificial intelligence, machine learning, optimization, and robotics. He is also the program coordinator of the department's at international master program in simulation and visualization. He is also the Elected Chair of the IEEE Computational Intelligence Society (CIS), Norway section.

HUMA JAMIL is an M. Phil. research student in the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. Cryptography is her research area in her master's degree.