Cryptanalysis of Novel Image Encryption Scheme Based on Multiple Chaotic Substitution Boxes

AMMAR S. ALANAZI1, (Member, IEEE), NOOR MUNIR2, MAJID KHAN2, MUHAMMAD ASIF3, AND IQTADAR HUSSAIN4

1Communication and Information Technology Research Institute, King Abdul Aziz City for Science and Technology, Riyadh 11442, Saudi Arabia
2Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad 44000, Pakistan
3Department of Mathematics, University of Management and Technology, Sialkot Campus, Sialkot, Pakistan
4Department of Mathematics, Statistics, and Physics, Qatar University, Doha, Qatar

Corresponding author: Ammar S. Alanazi (salanazi@kacst.edu.sa)

This work was supported in part by King Abdulaziz City for Science and Technology.

This work did not involve human subjects or animals in its research.

ABSTRACT In current years many chaos-based Substitution boxes (S-boxes) have been proposed. Recently, an image encryption technique based on multiple chaotic S-box was offered. This encryption method was based on the concept of confusion only produced by the implementation of the S-box. The concept of confusion utilized in the understudy technique can be smashed by using just one chosen-plaintext attack and a chosen-ciphertext attack. This article presents a detailed structure of two types of cryptographic attacks on the diffusion-based encryption scheme. The proposed attacks are successfully performed to retrieve the key with very little execution time by using just one chosen image which indicates the vulnerability of multiple chaotic S-boxes-based cryptosystems. The retrieved data is passed through some statistical analysis such as correlation, histogram, and entropy to check the correctness of recovered data.

INDEX TERMS Cryptanalysis, shuffling, image encryption, chaotic encryption, substitution box, chosen-plaintext attack.

I. INTRODUCTION

Data protection is considered to be one of the most important issues; it is an indispensable necessity, especially for data-based activities and transactions. In particular, before transmitting the data into the network, data encryption is required. Generally, cryptosystems are categorized into the two most significant classes. The first class comprises traditional and classical encryption schemes which involve Data Encryption Standard (DES), Advanced Encryption Standard (AES). These structures are theoretically easy whereas they show a robust resistance to conventional attacks. The prominent concerns with the execution of traditional systems are their reliance on numerous composite mathematical propositions which indicates having a protracted implementation period for encoding multimedia statistics. Conversely, the second class which has protected the algorithms is Shannon’s confusion and diffusion theory [1]. The confusion procedure processes that how a modification in the private key shakes the output information, and the diffusion measures how a change in the input data affects the output.

The Shannon confusion and diffusion design are further necessary for data encryption due to their strength compared to numerous assaults and being lower in execution time. The part of the nonlinear component of the block cipher (S-box) is of significance in secure communication and confusion. The design of the Substitution box was first introduced in 1949 by Shannon [1]. If the nonlinear component is not secure, it means that the encryption standard has to be compromised. The power of the S-box confirms the ability of block ciphers. To improve the quality of the S-box, many attempts have been made. Cryptographers have drained devotion to the literature to test the features of eminent Substitution boxes. The S-box is a significant nonlinear module utilized to obscure the relationship between ciphertext and private key in the block cipher structure architecture. The Substitution box can be viewed as vector Boolean functions from a mathematical perspective. Mathematical structures and random methods are generally utilized to construct S-box structures. A huge number of strong S-boxes need to be built. The protection of block ciphers is straightforwardly related to their nonlinear components, while the best example is the Data Encryption Standard (DES). In renovating a plain text or intelligible message into an encoded form, the S-box plays a
crucial role. A significant field of concern for security experts is the construction of powerful S-boxes.

The authors in [2] presented the Gray S-box for AES, which is created by adding the binary grey code conversion to the traditional AES S-box. To minimize the time complexity of AES, the authors in [3] changed the affine mapping of the AES S-box. In [4], to decrease the computational complexity of S-box design, the authors anticipated a new Substitution box design approach centered on single expression algebra. In [5], the authors suggested a new S-box based on the Galois field $GF(2^8)$ fractional linear transformation, which can generate uncertainty in the results. The authors utilized the principles of group theory in [6] to suggest a new S-box structure. A secure S-box with around optimum characteristics was developed in [7]. For this purpose, the authors applied a systematic group theoretical approach by executing chaotic maps and linear fractional mapping. Ullah et al. [8] created five powerful S-boxes. To produce 462,422,016 numbers of diverse AES-like Substitution boxes, Razaq, et al. [9] employed the behavior of symmetric groups $S_{16}$ and permutation groups of order 21,504. In [10], a novel genetic method for evolving Substitution boxes with high non-linearity was offered. They have implemented their system on various S-boxes successfully. The piecewise linear chaotic system and the traveling salesman problem were explored by Ahmad et al. [11] to construct a powerful S-box. An important algebraic procedure was suggested in [12] to build a robust Substitution box. The authors employed $S_{16}$ permutations and associative loops in their S-box design structure. Ahmad et al. [13] suggested a new methodology based on optimization of the artificial bee colony and chaotic system to construct an S-box with very efficient cryptographic features. To build an S-box with tremendous cryptographic characteristics, Javeed [14] used an innovative chaotic map and an acceptable element $S_{56}$. An innovative Substitution box structure was proposed by Khan et al. [15] using Lorenz equations. Artürger and Özkaynak [16] are developing a new framework to strengthen the skills of Chaos-based Substitution boxes. Ahmad et al. [17] used Particle Swarm Optimization for secure nonlinear component development.

The S-boxes have also been used by many researchers in image encryption applications [18]–[26]. In [27] authors presented a 2D modular chaotic system for improving the complexity of chaos. Authors in [28] designed a 2D logistic tent map-based color image encryption technique. Hua et al. suggested a new 2D chaotic system and orthogonal Latin square-based color image encryption method. Shah et al. endorsed a common norm in [30] to test the specific forms of S-boxes and assess their proficiency for applications for image encryption. Wu et al. [31] proposed an innovative image encryption procedure centered on coupled-map lattices (CML) and a chaotic method of fractional order. However, all the encryption schemes utilizing S-box are not always secure [32]–[39]. The reason is the operation of S-box only which creates just confusion in data and the concept of diffusion is skipped that is a very important part of Shannon’s theory [1].

In this study, we have presented cryptanalysis of Khan’s cryptosystem [40] by only one chosen-plaintext attack and one chosen-ciphertext attack with very little computation. The scheme offered in [40] comprises the concept of confusion only and diffusion is being ignored. The encryption schemes based on confusion components only are not secure. The effectiveness of the proposed attack is carried out due to the vulnerabilities in the understudy scheme. We have also implemented some security analyses to verify the quality of retrieved data. Some common analyses such as histogram, correlation, and entropy are performed to ensure the exactness of recovered data by the proposed attacks. We have also suggested an improved encryption scheme to increase encryption security as well as time efficiency.

The remaining article is arranged as follows; In section 2 we have presented a brief description of the understudy cryptosystem; Section 3 presents two types of cryptographic attacks on Khan’s scheme; Some security analyses of the recovered image are performed in section 4; Execution time analysis is depicted in section 5; In section 6 we have suggested a new cryptosystem to increase encryption security of Khan’s cryptosystem; In the last section, we have drawn a conclusion.

II. BRIEF DESCRIPTION OF UNDERSTUDY SCHEME

In cryptography, chaotic systems are utilized for randomness due to their unpredictability and sensitivity to initial conditions. Khan [40] proposed a multi-parameter chaotic system-based encryption scheme by using a combination of Lorenz [41] and Rossler [42]. The system of equations for the proposed system is defined as:

$$
\begin{align*}
\dot{x} & = \sigma (y - x) - y - z, \\
\dot{y} & = rx - y - 20xz + x + ay, \\
\dot{z} & = 5xy - bx + \delta + x(z - c). 
\end{align*}
$$

The system (1) is highly non-linear and exhibits chaotic behavior by taking the parametric values as $\delta = 16, \beta = 45.2, r = 2, a = 0.2, b = 0.2,$ and $c = 5.7$. The subsequent stages were implemented for the image encryption mechanism:

**Step 1:** The initial conditions and chaotic parameters were inserted in the structure (1) as the input of the chaotic map.

**Step 2:** The solution trajectories obtained from step 1 were stored in arrays known as $x, y, \text{ and } z$.

**Step 3:** The attained trajectories are passed through some affine transformation and a single array was generated in the range from 0 to 255.

**Step 4:** Resultant entries attained from step 3 were reshaped into a $16 \times 16$ matrix and stored as the offered Substitution box.

**Step 5:** Image of size $m \times n$ was inserted as the input of encryption algorithm.
Step 6: Obtained S-box from step 4 was employed in the input image and the resultant was stored as the cipher image.

The encryption structure of Khan’s scheme by using the above suggested S-box is elaborated in Fig. 1.

III. CRYPTANALYSIS OF KHAN’S ENCRYPTIONS SCHEME [40]

Generally, we consider that the assailant identifies the detail of the cryptographic structure understudy, this supposition is known as Kirchhoff’s hypothesis [43]. The attacker must be familiar with the encryption and decryption structure of the algorithm but does not own a private key for encryption and decryption. Cryptanalysis of the understudy scheme is performed by the chosen-plaintext attack and the chosen-ciphertext attack. With this regard, the attacker gets some short-term admittance to the encryption device and inserts some chosen-plain data, and encrypts the chosen plain images to get their respective cipher images. In this section, we have applied the chosen-plaintext attack and the chosen ciphertext attack on the encryption system under study.

A. CHOSEN-PLAINTEXT ATTACK

The chosen-plaintext attack is applied to get the encryption key of the algorithm. The encryption key utilized in Khan’s cryptosystem is the Substitution-box. Consider that two parties Alice and Bob are communicating through an insecure channel of communication by Khan’s cryptosystem. Some Trudy interrupts their communication by inserting some chosen-plain data and pretending to be Alice while communicating with Bob. The Trudy has short-term access to the encryption device and chose a special image to insert in the encryption algorithm defined as:

\[
P = \begin{pmatrix}
0 & 1 & \cdots & 255 \\
0 & 1 & \cdots & 255 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 1 & \cdots & 255
\end{pmatrix}_{256 \times 256}
\]  

The Trudy pass chosen image \(P\) through the Khan’s encryption scheme and Bob encrypts \(P\) and the obtained resultant is

\[
S(P) = \begin{pmatrix}
S(0) & S(1) & \cdots & S(255) \\
S(0) & S(1) & \cdots & S(255) \\
\vdots & \vdots & \ddots & \vdots \\
S(0) & S(1) & \cdots & S(255)
\end{pmatrix}_{256 \times 256}
\]  

where \(S\) is the implementation of the S-box on each pixel of the chosen image. The image retrieved after the implementation of the S-box is identified as the cipher image \(C\).

\[
C = \begin{pmatrix}
116 & 3 & \cdots & 7 \\
116 & 3 & \cdots & 7 \\
\vdots & \vdots & \ddots & \vdots \\
116 & 3 & \cdots & 7
\end{pmatrix}_{256 \times 256}
\]  

The cipher image matrix received after the implementation of the chosen-plaintext attack gives the substitution box utilized in the encryption scheme. Each row in the cipher image \(C\) is the entries of the S-box in ascending order. Therefore, the Trudy gets S-box utilized in encryption by just one chosen-plain image. The retrieved S-box after the chosen-plaintext attack is listed in Table 1. Astonishingly, the original Substitution box is retrieved with the help of just one chosen-plain image. This specifies that Khan’s cryptosystem is vulnerable against the chosen-plaintext attacks.

B. CHOSEN-CIPHERTEXT ATTACK

The chosen-ciphertext attack is applied to get the decryption key of the algorithm. The decryption key utilized in Khan’s cryptosystem is the inverse Substitution-box. Suppose that the attacker has short-term entrance to the decryption device and chose a special image to insert in the decryption algorithm defined as

\[
C = \begin{pmatrix}
0 & 1 & \cdots & 255 \\
0 & 1 & \cdots & 255 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 1 & \cdots & 255
\end{pmatrix}_{256 \times 256}
\]
TABLE 1. Substitution box recovered from the chosen-plaintext attack.

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 116 | 3 | 147 | 22 | 55 | 139 |
| 125 | 12 | 156 | 28 | 50 | 124 |
| 133 | 21 | 165 | 34 | 45 | 110 |
| 142 | 30 | 173 | 44 | 32 | 95 |
| 151 | 39 | 182 | 49 | 25 | 79 |
| 160 | 48 | 190 | 53 | 17 | 63 |
| 169 | 57 | 198 | 61 | 0 | 47 |
| 178 | 67 | 206 | 65 | 246 | 31 |
| 187 | 76 | 222 | 68 | 236 | 14 |
| 196 | 85 | 230 | 70 | 226 | 120 |
| 205 | 94 | 237 | 73 | 215 | 235 |
| 214 | 103 | 244 | 74 | 203 | 218 |
| 223 | 112 | 252 | 77 | 191 | 200 |
| 232 | 121 | 2 | 75 | 179 | 164 |
| 241 | 130 | 9 | 64 | 166 | 146 |
| 250 | 138 | 16 | 60 | 153 | 128 |

The chosen image \( C \) is passed through the Khan’s decryption algorithm and obtained resultant is

\[
S^{-1}(P) = \begin{pmatrix}
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255) \\
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255) \\
\vdots & \vdots & \ddots & \vdots \\
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255)
\end{pmatrix}_{256 \times 256}
\]

(6)

where \( S^{-1} \) is the implementation of the inverse S-box on each pixel of the chosen cipher image. The image retrieved after the implementation of the inverse S-box is identified as the plain image \( P \).

The plain image matrix received after the implementation of the chosen-ciphertext attack gives the inverse substitution box employed in the decryption process. Each row in the plain image \( P \) is the elements of the inverse S-box in ascending order. The obtained inverse S-box after the chosen-ciphertext attack is depicted in Table 2.

TABLE 2. Inverse substitution box recovered from the chosen-ciphertext attack.

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 100 | 54 | 210 | 1 | 171 | 230 |
| 242 | 84 | 214 | 38 | 11 | 33 |
| 52 | 187 | 35 | 61 | 207 | 22 |
| 81 | 67 | 20 | 77 | 43 | 83 |
| 227 | 115 | 219 | 113 | 131 | 111 |
| 94 | 126 | 31 | 184 | 235 | 145 |
| 253 | 216 | 108 | 175 | 93 | 123 |
| 193 | 167 | 46 | 151 | 0 | 232 |
| 245 | 119 | 225 | 191 | 231 | 32 |
| 60 | 139 | 229 | 2 | 9 | 158 |
| 80 | 202 | 8 | 186 | 213 | 34 |
| 55 | 138 | 112 | 212 | 56 | 122 |
| 90 | 72 | 23 | 218 | 144 | 254 |
| 58 | 105 | 42 | 188 | 26 | 121 |
| 238 | 7 | 148 | 169 | 104 | 185 |
| 249 | 224 | 10 | 120 | 178 | 174 |

The chosen image \( C \) is passed through the Khan’s decryption algorithm and obtained resultant is

\[
S^{-1}(P) = \begin{pmatrix}
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255) \\
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255) \\
\vdots & \vdots & \ddots & \vdots \\
S^{-1}(0) & S^{-1}(1) & \ldots & S^{-1}(255)
\end{pmatrix}_{256 \times 256}
\]

(6)

where \( S^{-1} \) is the implementation of the inverse S-box on each pixel of the chosen cipher image. The image retrieved after the implementation of the inverse S-box is identified as the plain image \( P \).

The plain image matrix received after the implementation of the chosen-ciphertext attack gives the inverse substitution box employed in the decryption process. Each row in the plain image \( P \) is the elements of the inverse S-box in ascending order. The obtained inverse S-box after the chosen-ciphertext attack is depicted in Table 2.

IV. STATISTICAL ANALYSIS OF RECOVERED IMAGE

This section presents the efficiency of proposed attacks on Khan’s encryption scheme. The analyses performed to evaluate the proficiency of implemented attacks are correlation, histogram, and entropy measure. Each analysis depicts that the recovered image exhibits the same properties as the original ones.

A. CORRELATION ANALYSIS

The neighboring pixels of the plain images are extremely correlated in the horizontal, vertical, and diagonal directions. Generally, the value of the correlation coefficient is high. An idyllic encryption scheme decreases the correlation between image pixels. Statistically, the correlation coefficient is determined as

\[
C_{xy} = \frac{E(y - m_y)(x - m_x)}{S_x S_y},
\]

(8)

where \( E \) is the expected value, \( m \) represents mean deviation, and \( S \) shows standard deviation. This relation measures the value of the correlation among the adjacent pixels \( x \) and \( y \) in each direction.

Here we have determined the correlation coefficient for the original, encrypted, and recovered image. Correlation values of the Baboon image in horizontal, vertical, and diagonal directions are depicted in Table 3. From the enumerated values, we can distinguish that the value of the correlation of the original and recovered image in each direction is the same. This shows that the proposed attack retrieves the original image precisely.
In this section, we present the correlation diagrams for the original, encrypted, and recovered Baboon image in horizontal, vertical, and diagonal directions, as shown in Fig. 2.

![Correlation Diagrams](image)

| Image          | Diagonal | Horizontal | Vertical |
|----------------|----------|------------|----------|
| Original       | 0.8448   | 0.9202     | 0.8567   |
| Encrypted      | 0.0184   | 0.0092     | 0.0210   |
| Recovered      | 0.8448   | 0.9202     | 0.8567   |

Correlation diagrams for original, encrypted, and recovered images in horizontal, vertical, and diagonal directions are presented in Fig. 2. From depicted correlation diagrams we can visibly observe that the original and recovered images exhibit the same pixel distribution. The similarity in the correlation diagram reveals that original data is successfully retrieved by using a chosen-plaintext attack and a chosen-ciphertext attack.

### B. HISTOGRAM ANALYSIS

The randomness of data is observed by histogram analysis. The histogram of an original image is irregularly dispersed and after some encryption process, the histogram becomes uniform. An idyllic encryption algorithm produces a cipher image that exhibits a uniformly distributed histogram. The 3D histograms of the plain Baboon image layers are displayed in Fig. 3 (i-iv), the encrypted image channels are depicted in Fig. 3 (v-viii), and the recovered image layers are presented in Fig. 3 (ix-xii). The visual results indicate that the recovered image is analogous to the plain image.

### C. ENTROPY

Information entropy is measured by the quantity of uncertainty in a random variable. Mathematically information entropy is calculated by:

$$H(m) = \sum_{m=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)},$$

where $M$ represents the value of gray level and $p$ is the percentage of pixels for which the value is equal to $m$. The ideal value of information entropy for a grayscale image with the data range [0, 255] is 8. Entropy values for Baboon original, encrypted, and recovered are listed in Table 4. From the presented results it is evident that the entropy values for the original and retrieved image are the same which designates that the plain image is recovered successfully by the proposed attacks.

### V. EXECUTION TIME COMPLEXITY ANALYSIS

The execution time of a computational task is the highest interval of time the task could proceed to perform on a precise hardware board. The performance of the proposed attacks can be determined by the execution time to perform assaults. Execution time (in seconds) to retrieve Baboon image of different size by the chosen-plaintext attack and the chosen-ciphertext attack is listed in Table 5. From enumerated results, we can observe that the image of size $128 \times 128$, $256 \times 256$, $512 \times 512$
and 1024 × 1024 can be recovered in 0.5 sec, 1.1 sec, 2.0 sec, and 3.4 sec respectively by the chosen-plaintext attack and in 0.45 sec, 0.9 sec, 1.6 sec, and 2.3 sec respectively by the chosen-ciphertext attack. The execution time to perform an attack is very less which indicates that Khan’s encryption scheme is not secure and vulnerable.

The complexity of the algorithm is the time for searching the substitution of all possible 256 entries. The complexity of image data with size \( P \times Q \) becomes \( O(P(Q - 1) + H) \) which is very low for a computer. The complexity decreases when the size of data is small. Therefore, computational complexity is related to the size of the image. The offered cryptanalysis is performed on desktop PC, 8 GB, Core i7, 3rd Gen, MATLAB 20.

### A. COMPARATIVE EXECUTION TIME ANALYSIS

The time for the execution of the chosen-plaintext attack is compared with the existing cryptanalysis scheme in Table 6. From the listed comparison we can observe that the proposed attack retrieves a Baboon image of different sizes in less time as compared to the attacks offered in [39].

The comparison of chosen-ciphertext attack is depicted in Table 7. The comparative results reveal that the performance of offered attacks is much better than the attacks employed in Reference [39].
VI. THE PROPOSED IMPROVEMENT

A robust encryption scheme must adhere to Shannon’s confusion-diffusion theory. The understudy encryption structure possesses confusion only and diffusion was being ignored. The confusion process can be attained by Substitution simply and permutation or XOR operation generates diffusion in ciphers and breaks the relationship between plaintext and ciphertext. To address the vulnerabilities in Khan’s encryption scheme, an improvement is suggested and elaborated as follows:

A. PERMUTATION PHASE

The first step to construct a secure cryptosystem is to add diffusion to the algorithm. Suppose $P^R$, $P^G$ and $P^B$ be the red, green, and blue channels of the plaintext to be encrypted. Here we suggest the shuffling of the array by using some key $k_1$ and bitwise addition by using some key $k_2$. The mathematical steps of permutation are defined as follows:

\[
\text{Shuffling} \begin{cases} 
(P^R, k_1) = C^R_1 \\
(P^G, k_1) = C^G_1 \\
(P^B, k_1) = C^B_1
\end{cases}
\]

where $C^R_1$, $C^G_1$, and $C^B_1$ are respective shuffled image layers of the plain images $P^R$, $P^G$ and $P^B$ by using the private key $k_1$. The shuffled cipher images are passed through the bit-wise addition operation by using a secret key $k_2$.

\[
\begin{align*}
C^R_1 \oplus k_2 &= C^R_2 \\
C^G_1 \oplus k_2 &= C^G_2 \\
C^B_1 \oplus k_2 &= C^B_2
\end{align*}
\]

where $C^R_2$, $C^G_2$, and $C^B_2$ are the cipher channels attained after the bitwise addition operation.

B. CONFUSION PHASE

The cipher image obtained from the permutation phase is passed through the second phase of the proposed improvement that is the confusion phase. Suppose $S$ be the substitution operation applied by using the S-box presented in Table 1. Mathematically, the confusion process is done as follows:

\[
\begin{align*}
S(C^R_2) &= C^R_3 \\
S(C^G_2) &= C^G_3 \\
S(C^B_2) &= C^B_3
\end{align*}
\]

where $C^R_3$, $C^G_3$, and $C^B_3$ are the respective cipher components of plain layers $P^R$, $P^G$ and $P^B$. The combination of three operations, shuffling, bit-wise addition, and substitution gives a secure cryptosystem which can defeat all the cryptographic attack such as chosen-plaintext attack and chosen-ciphertext attacks.

C. SECURITY ANALYSIS

The suggested modified cipher comprises a mixture of three operations that are shuffling, bit-wise addition, and substitution instead of using substitution only. The improved encryption technique can resist chosen-plaintext attacks and chosen-ciphertext attacks. The failure of these attack can be elaborated by the following points:

1. The operation of shuffling and addition becomes invariant by inserting input consisting of all zeros, but Substitution produces cipher by unrevealing the mapping of elements. Consider $P = \bar{0}$ be the input data. Mathematically, the performance of the algorithm is defined by:

\[
\begin{align*}
\text{Shuffling}(P = \bar{0}) &= \bar{0}, \\
\bar{0} \oplus k &= k, \\
S(k) &= C
\end{align*}
\]

where $k$ is the key utilized for bit-wise addition operation and $C$ is the cipher image produced from improved image encryption technique. Therefore, we can observe that by inserting chosen plain data we cannot get information about plain data and the improved technique resists the linear attacks.

2. The Substitution can be retrieved by inserting the matrix with entries arranged in ascending order, but the operation of shuffling and bitwise addition fails this attack. Mathematically, the encryption of chosen-plaintext by modified cipher can be shown as:

\[
\begin{align*}
\text{Shuffling} \begin{pmatrix}
0 & 1 & \cdots & 255 \\
0 & 1 & \cdots & 255 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 1 & \cdots & 255
\end{pmatrix} &= C_1, \\
C_1 \oplus k &= C_2, \\
S(C_2) &= C_3
\end{align*}
\]

where $C_3$ is the final cipher data produced from the modified encryption technique by inserting chosen-plaintext data. From the above mathematical steps, we can observe that the final cipher does not reveal any information about the secret key. Therefore, we can say that the improved encryption technique is secure against all possible attacks.

VII. CONCLUSION

In this study, we have exposed that the chaos-based encryption technique suggested in [40] grants weak security. We have devised two diverse kinds of assaults to break the understudy cryptosystem. It is specified that the keystream can be easily determined with the help of just one chosen-image which designates vulnerabilities of the cryptosystem. The data retrieved by proposed attacks are passed through different kinds of security analyses which possess that the recovered data is the same as the original ones. The similarity in retrieved and original data indicates the efficiency of performed attacks. Moreover, we have suggested a brief idea of an improved cryptosystem to enhance the robustness of Khan’s encryption scheme. From every point of view, the encryption scheme in [40] cannot be considered a safe algorithm and is not recommended for secure encryption.
REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy Systems∗,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] M. T. Tran, D. K. Bui, and A. D. Duong, “Gray S-box for advanced encryption standard,” in Proc. IC-ICS, 2008, pp. 253–258, doi: 10.1109/CIS.2008.205.

[3] O. B. Sahoo, D. K. Kole, and H. Rahaman, “An optimized S-box for advanced encryption standard (AES) design,” in Proc. ICACC, 2012, pp. 154–157, doi: 10.1109/ICACC.2012.35.

[4] N. Munir and M. Khan, “A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic,” in Proc. ICAEM, 2018, pp. 48–52.

[5] S. Farwa, T. Shah, and L. Idrees, “A highly nonlinear S-box based on a fractional linear transformation,” Springerplus, vol. 5, no. 1, p. 1658, 2016, doi: 10.1186/s40064-016-3298-7.

[6] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, “A projective general linear group based algorithm for the construction of substitution box for block ciphers,” Neural. Comput. Appl., vol. 22, no. 13, pp. 1085–1093, 2013, doi: 10.1007/s00521-018-3530-7.

[7] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, “Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes,” IEEE Access, vol. 8, pp. 39781–39792, 2020.

[8] A. Ullah, S. S. Jalal, and T. Shah, “A novel construction of substitution box using a combination of chaotic maps with improved chaotic range,” Nonlinear Dyn., vol. 88, no. 4, pp. 2757–2769, Jun. 2017.

[9] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shaiba, W. Aslam, and M. Alawida, “A novel method for generation of strong substitution boxes based on cost graphs and symmetric groups,” IEEE Access, vol. 8, pp. 75473–75490, 2020.

[10] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, “A genetic algorithm for constructing bijection substitution boxes with high nonlinearity,” Inf. Sci., vol. 523, pp. 152–166, Jun. 2020.

[11] M. Ahmad, N. Mittal, P. Garg, and M. Maitab Khan, “Efficient cryptographic substitution box design using travelling salesman problem and chaos,” Perspect. Sci., vol. 8, pp. 465–468, Sep. 2016.

[12] S. Hussain, S. S. Jalal, 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, doi: 10.1109/ACCESS.2020.3005087.

[13] M. Ahmad, M. N. Doja, and M. M. S. Beg, “ABC optimization based construction of strong substitution-boxes,” Wireless Pers. Commun., vol. 101, no. 3, pp. 1715–1729, Aug. 2018.

[14] A. Javeed, T. Shah, and A. Ullah, “Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group,” Wireless Pers. Commun., vol. 112, no. 1, pp. 467–480, May 2020.

[15] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, “A novel substitution box for encryption based on Lorenz equations,” in Proc. IEEE ICSSC, Jul. 2017, pp. 32–36.

[16] F. Artuğer and F. Özkaynak, “A novel method for performance improvement of chaos-based substitution boxes,” Symmetry, vol. 12, no. 4, p. 571, Apr. 2020.

[17] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, “Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications,” IEEE Access, vol. 8, pp. 116132–116147, 2020, doi: 10.1109/ACCESS.2020.3004449.

[18] G. Zhang and Q. Liu, “A novel image encryption method based on total shuffling scheme,” Opt. Commun., vol. 284, no. 12, pp. 2775–2780, Jun. 2011.

[19] R. Hanza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, “A privacy-preserving cryptosystem for IoT E-healthcare,” Inf. Sci., vol. 527, pp. 493–510, Jul. 2020, doi: 10.1016/j.ins.2019.01.070.

[20] A. Alghafis, N. Munir, M. Khan, and I. Hussain, “An encryption scheme based on discrete quantum map and continuous chaotic system,” Int. J. Theor. Phys., vol. 59, no. 4, pp. 1227–1240, Apr. 2020.

[21] M. Khan and N. Munir, “A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic,” Wireless Pers. Commun., vol. 109, no. 2, pp. 849–867, Nov. 2019, doi: 10.1007/s11277-019-06594-6.

[22] M. Khan and H. M. Waseem, “A novel image encryption scheme based on quantum dynamical spinning and rotations,” PLoS ONE, vol. 13, no. 11, Nov. 2018, Art. no. e0206460.