IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 28, 2020, accepted March 19, 2020, date of publication March 23, 2020, date of current version March 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982827

An Image Encryption Algorithm Based on Chaotic Selection of Robust Cryptographic Primitives

ZAHIR MUHAMMAD ZIAD MUHAMMAD AND FATİH ÖZKAYNAK
Department of Software Engineering, Fırat University, Elaziğ 23119, Turkey

Corresponding author: Fatih Özkaynak (ozkaynak@firat.edu.tr)

ABSTRACT With the spread of digital images, the security of these data has become a serious problem. In this study, an image encryption algorithm is designed to ensure the confidentiality of digital images. The original aspect of the proposed algorithm is that it has an architecture that combines unpredictable and random-like features of chaotic systems and cryptographic primitives that have been proven as a result of many years of research. By making use of the advantages of chaotic systems, it has provided the design of an image encryption algorithm that is more resistant to application attacks than mathematical designs. Analysis results and security evaluations have shown that the proposed method can be used successfully in many applications related to security of digital image.

INDEX TERMS Chaos, cryptography, image encryption.

I. INTRODUCTION

The impact of digital transformation continues exponentially. This effect has changed many processes and continues to change. Now even wars are associated with cyber-physical attacks on critical infrastructures [1]. Therefore, the concept of information security has become more important than ever. Digital images are one of the most important types of information used effectively in digital environments. It is known that classical encryption algorithms are insufficient to provide information security due to their some features [2]. Therefore, researchers are doing research on alternative solution suggestions. One of the most striking subjects among these alternative researches is design studies based on nonlinear dynamics [2], [3]. The number of studies on this subject in the last decade is expressed in thousands [4]–[20]. One of the most striking examples to draw attention to the size of this subject is the number of studies published in IEEE Access journal in the last three years. The fact that this number is close to 50 is an indication of how hot the subject is. However, the security weakness of these studies and the problems that may arise in practical applications reveal another aspect of the subject that needs to be addressed.

The aim of this study is to present an image encryption algorithm that can eliminate these security concerns. To achieve this goal, the robust primitives of modern cryptology are combined with the unique features of the chaos theory. Another strong feature of the proposed algorithm is that the security analysis of the study was not made using only statistical tests. The fact that the proposed algorithm can be adapted to both gray and color images is another advantage of the study in terms of practical applicability. The rest of the study is organized as follows. In the Section II, the architecture of the proposed algorithm is detailed. In the Section III, security analyzes of the proposed algorithm have been carried out. The obtained results are discussed and a road map is proposed for future studies in the last section.

II. PROPOSED IMAGE ENCRYPTION ALGORITHM

Due to the unique characteristics of the images, high correlation between pixel values should be eliminated at the end of the encryption steps [2]. The first expected feature of an image encryption algorithm is that distribution of pixel values to have a uniform distribution. One of the most suitable encryption architectures that can be used to meet this requirement is to apply the substitution and permutation processes many times. It was proposed by Shannon, who is considered the father of information theory. It is stated that after applying these substitution and permutation processes many times, statistical requirements can be met [21], [22]. The advantage of this study is that an encryption architecture is used that combines the unpredictable properties of chaotic selections with provable secure substitution and permutation primitives.

The general view of the algorithm is shown in Figure 1. The proposed image encryption algorithm is built on three basic blocks. These basic blocks are:

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

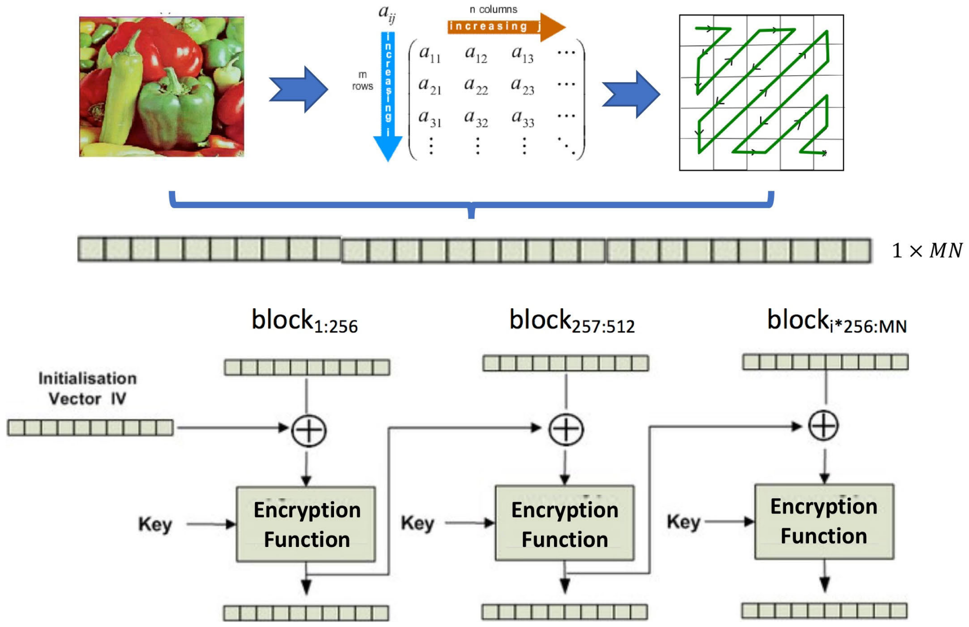


FIGURE 1. General overview of proposed image encryption algorithm.

- Block encryption algorithm with OFB mode
- Encryption function used in the confusion and diffusion process of each block
- Chaotic key generator (CKG) function.

The pseudo code of the proposed algorithm is given in Table 1. The operation steps of the algorithm are explained in detail step by step below.

Step 1: A gray or color image is selected. Row number and column number of the selected image are represented M and N symbols respectively.

Step 2: The selected image is converted into an one-dimensional array with 1 × MN-size. If a color image is used, the dimension of one-dimensional array is 1 × 3MN. Zigzag reading operation is used in the conversion process from a multi-dimensional array to a one-dimensional array.

Step 3: The obtained one-dimensional array is divided into blocks, each containing 256 pixels.

Step 4: If the MN value is not a multiple of 256, a padding process is applied. For the padding process, the pixel value as many times as needed is produced using CKG function. Pixel values range from 0-255.

Step 5: An initialization vector (IV) contain 256 values ranging from 0-255 is produced using CKG function.

Step 6: Steps 7-14 are applied to each block

Step 7: XOR operation is applied for IV and first block then CipheredImage value are generated.

Step 8: A permutation table (PerTab) with size of 16 × 32 has been generated by randomly combining transposed version of DES s-box tables. Each column of this table contains values ranging from 0-15.

Step 9: Two values, which are represented a and b symbols respectively, are generated using the CKG function. a and b values between 1 and 32. These values are used to determine which columns of the PerTab will be selected.

Step 10: The columns of the AES s-box table are permuted according to the values of the column selected with the value of a and new 256 values generated. XOR operation is applied for permutated values and CipheredImage

Step 11: Using the CKG function, 256 key values are generated ranging from 0 to 255 values. XOR operation is applied for CipheredImage and key values.

Step 12: The rows of the AES s-box table are permuted according to the values of the column selected with the value b and new 256 values generated. XOR operation is applied for permutated values and CipheredImage

Step 13: CipheredImage is divided into four parts and one of these four parts is selected according to the round number. The selected part is permuted according to the DES permutation table.

Step 14: CipheredImage is determined as the new IV.

Step 15: Steps 7-14 are repeated round number times. Default values of round number is eight

Details of basic blocks in the encryption function are tried to be explained step by step in the following subsections.

A. GENERATION AND DETAILS OF PerTab OPERATION

Strong components of DES algorithm are used as confusion and diffusion blocks of the proposed encryption algorithm.

TABLE 1. Pseudo-code of proposed algorithm.

```
ImageEncryptionAlgorithm(Image, MasterKey):cipheredImage
           array[M:N]=read_image(Image)
           array[1:MN]=zigzag(Array[M:N])
           block_number=MN/256
           arrayBlocks[1:block_number+1]=partition(array[1:MN])
           if(MN%256!=)
                    padding(arrayBlocks[block_number+1])
           end_if
           IV=CKG(256, 256)
           for i=1 in block_number+1
                 cipheredImage=XOR(IV, arrayBlocks[i])
                 for round=1 in 8
                            colA[1:16]=SELECT(PerTab(CKG(1,16)))
                            table1=SHIFT_ROWS(aes_sbox, colA)
                            cipheredImage=XOR(cipheredImage,table1)
                            key1=CKG(256,256)
                            cipheredImage=XOR(cipheredImage,key1)
                            colB[1:16]=SELECT(PerTab(CKG(1,16)))
                            table2=SHIFT_COLUMNS(aes_sbox, colB)
                            cipheredImage=XOR(cipheredImage,table2)
                            key2=CKG(256,256)
                            cipheredImage=XOR(cipheredImage,key2)
                            sub_block=round%4
                            cipheredImage=Permute(sub_block)
                 end
                 IV= cipheredImage
          end
          return cipheredImage
end
```

Despite having problems such as short key length of DES, variants of DES like 3DES are still used successfully in many practical applications such as electronic passport [23]. The idea behind this success is that the strong cryptographic properties of the DES s-box components. In addition to these strong cryptographic properties, the new table obtained by combining transpose version of eight s-box structures. One of the approaches that can be used in the cryptographic protocol design process is to use engineering designs. As an engineering design example, the first cryptographic primitive is DES s-box structures. This is the most important reason to use DES s-box structures with a different approach in the design of the proposed image encryption algorithm.

This generated new table was named as PerTab in proposed algorithm. The PerTab was generated by making use transpose of DES s-box structures. In the DES block encryption algorithm, there are eight different s-box structures. Size of each s-box table is 4 × 16. The values of each row of these s-box ranges from 0-15. First of all, 16×4 size eight tables are obtained by transposing original eight DES s-box structures. Then, these eight tables are combined using random selection principle with the help of CKG. As a result, PerTab in the size of 16×32 is obtained. The overview of this procedure is shown in Figure 2.

B. DETAILS OF SHIFT_ROWS AND SHIFT_ COLUMNS OPERATIONS

Another approach that can be used in the cryptographic protocol design process in modern cryptography is to use transformations based on strong mathematical functions. The best example of this design approach is the AES s-box structure. AES s-box structures were created using irreducible polynomials on the Galois Field [24]. This s-box structure does not contain any mathematical weakness.

In the proposed encryption function, two random values have been generated using CFG. These values have been used in the selection of two columns from the PerTab. The selected columns have been used to mix the row and column positions of the AES s-box structure. This process is shown in Figure 3.

As a result of the operations shown in Figure 3, a vector of size 1×256 has been produced. XOR operation is applied to block values with these values. The general view of the encryption function is given in Figure 4.

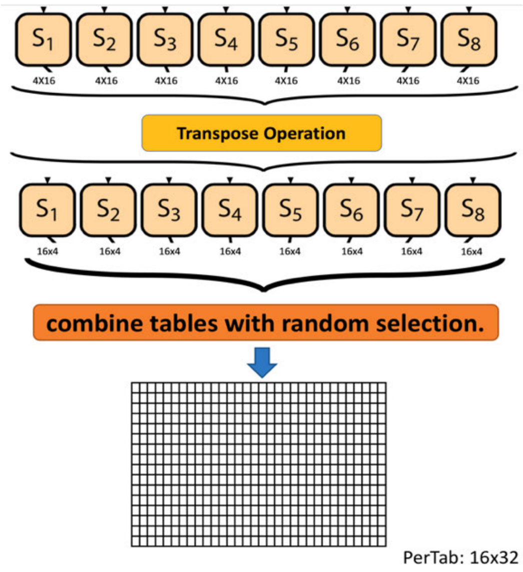
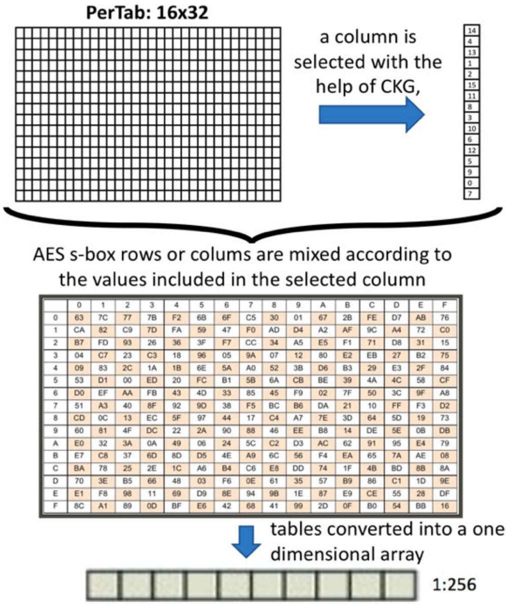

S1 S2 S3 S4 S5 S6 S7 S8
4X16 4X16 4X16 4X16 4X16 4X16 4X16 4X16
Transpose Operation
S1 S2 S3 S4 S5 S6 S7 S8
16x4 16x4 16x4 16x4 16x4 16x4 16x4 16x4
combine tables with random selection.
PerTab: 16x32

FIGURE 2. Details of generation of PerTab operation.


PerTab: 16x32
a column is selected with the help of CKG,
14
4
13
1
2
15
11
8
3
10
6
12
5
9
0
7
AES s-box rows or colums are mixed according to the values included in the selected column
tables converted into a one-dimensional array
1:256

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

FIGURE 3. Details of shift_row and shift_columns operation.

C. DETAILS OF CHAOTIC KEY GENERATION FUNCTION

One of the important features of the proposed image encryption algorithm is the Chaotic Key Generator (CKG) algorithm. The generator function has the ability to generate any-length of random numbers in the desired range. The steps of the algorithm are described below. In the algorithm, an entropy pool has been created by using various chaotic maps with the most suitable initial conditions and control parameters. This entropy pool provides specific statistical requirements. Also, as this process can be realize offline, the generator will be able to produce very fast output using this advantage. The SHA3 algorithm [25] has also been applied to outputs of generated random numbers to solve the security problems that will be detailed In the third section.

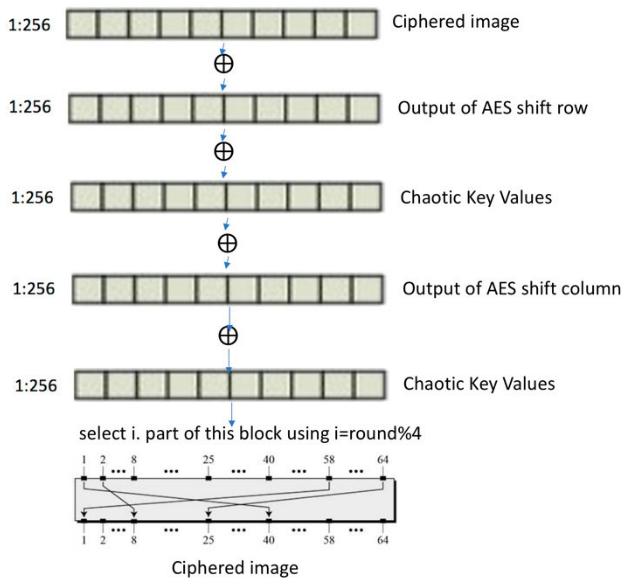


FIGURE 4. The general view of the encryption function.

Step 1: State variables are calculated for four different chaotic maps with special determined initial conditions and control parameter values that will provide randomness properties.

Step 2: These state variables are transform bit values using threshold function.

Step 3: Random bits are generated until a 256-bit length block is obtained.

Step 4: SHA3 is applied to the 256-bit length block and add entropy pool.

Step 5: CFG takes two parameters as input. These parameters are named as upper_values and count. The CFG returns count-length random numbers range from 0 to upper_values as output.

Step 6: x-bit are taken from an entropy pool to meet the condition $2^x \geq$ count

The overview of chaotic key generation function is shown in Figure 5. One of the strong features of the proposed image encryption algorithm can be shown as the use of strong cryptographic components with a different approach. However, chaotic key generator algorithm comes to the fore as the unique aspect of the proposed algorithm. It is shown in detail in the next section with the analysis results that CFG both successfully satisfies cryptographic randomness requirements and can be used as a counter measure to prevent side channel attacks.

III. ANALYSIS OF PROPOSED METHOD

Although chaos-based cryptology studies are a very active topic, they have a bad reputation. One of the most important reasons for this bad reputation is the security weaknesses in many chaos-based image encryption algorithms [2].

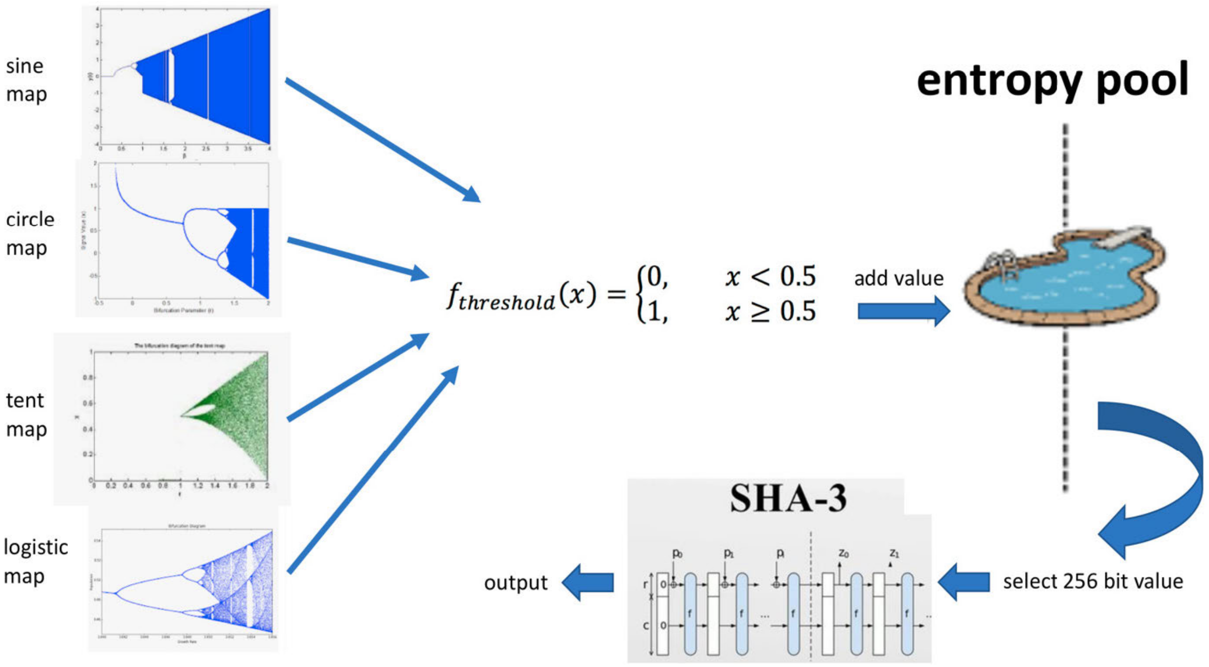


FIGURE 5. Details of chaotic key generation function.

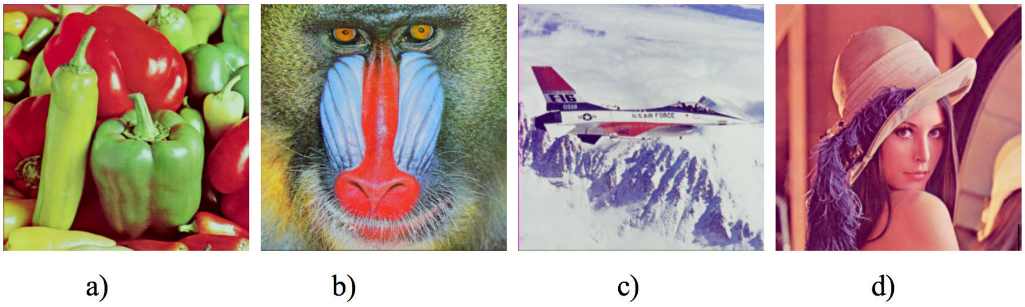


FIGURE 6. Sample standard test images.

The most important reason behind these weaknesses cannot be revealed in the design process is that the security analysis of the designs is performed only with statistical tests. Statistical tests are necessary but not sufficient to evaluate the success of an image encryption algorithm. There are several template attack scenarios and analysis road maps to draw attention to this problem. One of the most important features of the proposed algorithm is that security analyzes are performed using provable security perspective. In the subsections of this section, statistical analysis results are given first. Then analysis of the substitution, permutation and chaotic key generator algorithm are given. Finally, practical issues such as key length analysis and encryption speed are also included.

A. STATISTICAL SECURITY ANALYSIS

The most common approach to evaluate the success of image encryption algorithms are criteria such as NPCR, UACI and correlation distribution [74]. Although there are other statistical tests, it has been proved that statistical tests alone will not be sufficient. Therefore, there is a focus on provable security analysis in other sections instead of other test approaches. Sample test images are given in Figure 6 and their encrypted versions are given in Figure 7. Histogram analysis of original and encrypted images is given in Figure 8. In Figure 9, the correlation distributions in the diagonal axis are given. Table 2 shows the calculated NPCR and UACI values. Ref. [26], [27] can be examined for mathematical formulas and interpretation of these values.

It is desired that the calculated value for the NPCR value be as high as possible. For the UACI measurement, the acceptable value is expressed as 0.33. However, as stated earlier, both tests are statistical tests only. It is known that all outputs with random-like behavior will provide these tests. The results in Table 2 confirmed this hypothesis. In other words, proposed algorithm provides NPCR and UACI features like

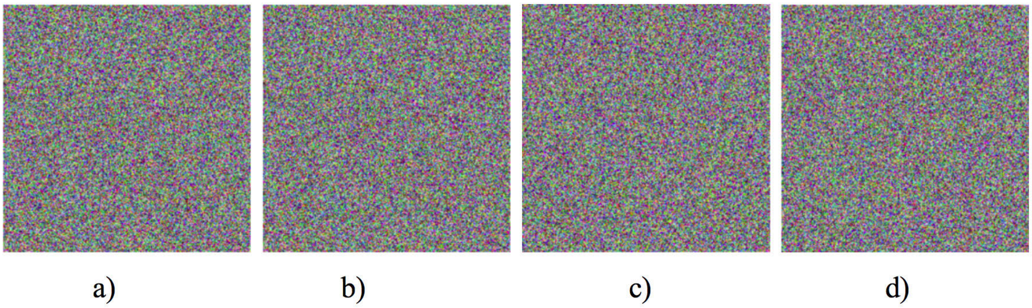


FIGURE 7. Encrypted versions of sample standard test images.

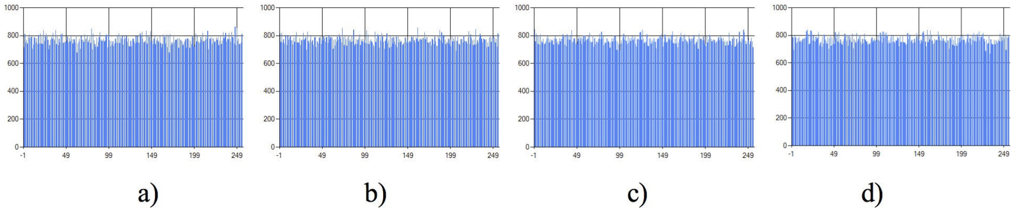


FIGURE 8. Histogram analysis of encrypted images.

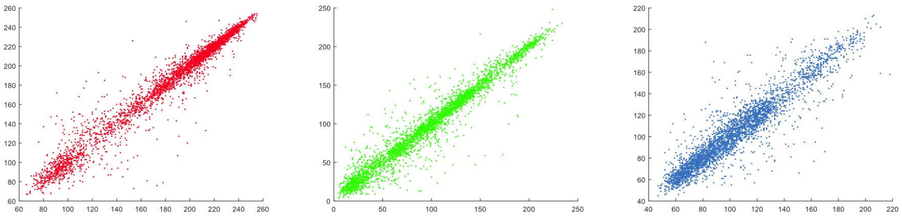


FIGURE 9. Diagonal axis correlation distributions of Figure 5.(a).

TABLE 2. Some statistical test results.

	NPCR	UACI
Figure 5.(a)	% 9979	0.3341
Figure 5.(b)	%.9966	0.3336
Figure 5.(c)	% 9968	0.3348
Figure 5.(d)	% 9973	0.3349

other chaotic image encryption algorithms in the literature. All these statistical analyses have shown that the attacker is not able to make any deductions using the statistical properties. However, it should not be forgotten that these measurements are necessary but not sufficient.

B. SECURITY ANALYSIS OF SUBSTITUTION AND PERMUTATION PRIMITIVES

Strong components of DES and AES algorithms are used as substitution and permutation blocks of the proposed algorithm proposed. Despite having problems such as short key length of DES, variants of DES like 3DES are still used successfully in many more practical applications [23]. Behind this success, the strong cryptographic properties of the DES components play an important role. In addition to these strong cryptographic properties, the new table obtained by combining eight s-box structures using chaotic selection reduced the chance of success of the attacker.

Another strong cryptographic primitive used in the proposed algorithm is the AES s-box structure. The fact that the AES s-box structure has the best cryptographic properties that can be achieved for s-box evaluation criteria such as nonlinearity, bit input/output independence, strict avalanche effect, differential distribution table [24]. These criteria have been critical in the selection process of the new block encryption standard to meet the new security requirements after DES. It has been shown that the success of the attacker can be minimized in the s-box structure proposed by Nyberg, especially after differential cryptanalysis has been shown to be a major threat.

However, new analysis studies in the field of cryptanalysis showed that there may be some problems in application attacks for cryptographic protocols based on strong mathematical functions [28]. A strong encryption architecture has been developed against both classical and application attacks

TABLE 3. Some statistical test results.

Chaotic System	Mathematical Model	Initial Condition	Control Parameters
Circle Map	$x_{n+1} = x_n + a - \frac{b}{2\pi}\sin(2\pi x_n) \bmod 1$	0.29	a=1 b=11.5
Logistic Map	$x_{n+1} = a * x_n * (1 - x_n)$	0.85	4
Sine Map	$x_{n+1} = a * \sin(\pi x_n)$	0.45	0.99
Tent Map	$x_{n+1} = \begin{cases} a * x_n & x_i < 0.5 \\ a * (1 - x_n) & x_i \geq 0.5 \end{cases}$	0.63	1.99

TABLE 4. NIST test results.

NIST TEST	Circle Map		Logistic Map		Sine Map		Tent Map	
	Result	p-value	Result	p-value	Result	p-value	Result	p-value
Monobit test	S	0,65849	S	0,1875	S	0,18885	S	0,063454
Frequency within block test	S	0,85814	S	0,64935	S	0,77268	S	0,06215
Runs_test	S	0,33495	S	0,21414	S	0,98702	S	0,92308
Longest run ones in a block test	S	0,1643	S	0,8478	S	0,94131	S	0,2739
Binary matrix rank test	S	1	S	1	S	1	S	1
Dft test	S	0,13712	S	0,19889	S	0,25135	S	0,76902
Non-overlapping template matching test	S	0,12951	S	0,27742	S	0,86711	S	0,01284
Overlapping template matching test	S	0,5839	S	0,5839	S	0,5839	S	0,5839
Maurers universal test	S	0,56938	S	0,56799	S	0,56951	S	0,5687
Linear complexity test	S	1	S	1	S	1	S	1
Serial test	S	0,452465	S	0,203515	S	0,70286	S	0,549045
Approximate entropy test	S	0,057646	S	0,64612	S	0,87009	S	0,22019
Cumulative sums test	S	1	S	1	S	1	S	1
Random excursion test	S	0,448163	S	0,221548375	S	0,400935	S	0,256564875
Random excursion variant test	S	0,462197222	S	0,55696	S	0,452156	S	0,297296667

by eliminating these problems using DES, AES primitives and chaotic selection algorithm proposed in the study.

C. SECURITY ANALYSIS OF CHAOTIC KEY GENERATION FUNCTION

Randomness is critical issue for many applications. However, more care should be taken during the evaluation of the randomness required in cryptography applications. Since randomness requirements are not met, the security of the whole system will be negatively affected [29]. There are four basic randomness requirements for cryptography applications [30]. The first of these requirements is that the generated numbers have strong statistical properties. Four different chaotic maps have been used in the study. The initial conditions and control parameters of these maps are given in Table 3 [31]. The NIST randomness tests [32] result in Table 4 show that selected entropy source have statistically strong properties.

The second requirement for cryptographic randomness is to ensure that other random numbers are not predicted by using a subset of generated random numbers. The third and fourth requirements are actually detailed forms of the second requirement. One way functions is one of the most suitable options to meet this requirement [25]. One of the unique properties that make the proposed image encryption algorithm privileged is the use of provable secure cryptographic primitives. For this reason, SHA3 algorithm, which is the new hash function standard chosen as a result of many years of analysis, has been used to provide the one-way function requirement. As long as the SHA3 algorithm is secure, the random number generator algorithm will meet the requirements for R2, R3 and R4.

Another major problem of chaos-based encryption algorithms is digital deterioration. Simulation of chaotic behavior on the computer can negatively affect the behavior expected from chaos. By using SHA3 algorithm, this problem will be prevented [33], [34].

One feature of the proposed algorithm that makes it more advantageous than its counterparts is that the generator is designed to provide the best known statistical features. For example, NIST analysis, the result is actually fail for tent map in non-overlapping template matching test. But, the initial conditions and control parameters of the chaotic maps used in this study were determined with the help of optimization algorithms. These determined values provide all NIST tests. Details of the optimization study are examined in Ref. [35].

To show the success in the NIST tests in more detail, Table 5 is related to the chi-square test results, one of the

TABLE 5. Frequencies distribution of generated numbers for chi-square test.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Circle Map	15751	15309	15620	15427	15809	15612	16043	15396	15423	16016	15565	15657	15441	15653	15277	16001
Logistic Map	15747	15667	15452	15640	15604	15642	15700	15751	15586	15644	15608	15657	15589	15616	15526	15571
Sine Map	8261	17685	16489	18170	16543	15042	17732	14877	17390	16764	15361	14367	17925	15040	15124	13230
Tent Map	15514	15468	15701	15678	15642	15510	15662	15726	15590	15615	15689	15746	15739	15645	15617	15458

tests included in the NIST test package. Firstly, 1,000,000 bits were produced. The produced 1,000,000 bits are divided into 4-bit length blocks. By converting each 4-bit block to decimal numbers, 250,000 numbers between 0-15 were obtained. Table 5 shows the frequencies of these numbers. In order for the generator to show statistically good features, each number must have 15,625. In other words, when the distribution in Table 5 is analyzed, it shows the statistical success of the generator, in other words, near ideal values.

D. ANALYSIS OF KEY LENGTH

The proposed image encryption algorithm is an example of a symmetric (secret) key encryption system. Therefore, the architecture detailed in the Section II is known by both the attacker and the parties of the communication. The only secret parameter in the algorithm is the key. Therefore, it should be demonstrated that the key-length is resistant to brute-force attacks.

The master key of the algorithm is the initial condition and control parameters of the chaotic systems in the Table 3. There are nine different initial condition and control parameters. These parameters are real numbers represented double precision. in other words, 52 bits are required to represent each parameter. Therefore, the total key length is expressed as $9^*52 = 468$ bits. The key length must be at least 100 bits to prevent brute force attacks. So, the proposed algorithm is secure against brute force attacks. In the design process, the key length can be expanded by evaluating an additional parameter in the master key for parameters such as the number of rounds.

E. ENCRYPTION SPEED AND OTHER PRACTICAL ISSUES

One of the important criticisms about the proposed image encryption algorithm is what advantages and disadvantages it will have compared to powerful block encryption methods. DES, AES or other similar block cipher algorithms cannot be applied directly to images because there is a correlation problem in the images. However, this problem will be eliminate since the zigzag reading method used in the proposed method converts the image into a one-dimensional text file. The most important questions that comes to mind at this stage are why not encrypt the image with AES or 3DES? What the differences among the proposed algorithm, AES and 3DES? The original aspect of the study is to design an image encryption algorithm that can be more effective than mathematical designs such as AES and 3DES especially against application attacks. New studies have shown that designs based on chaotic systems are more successful than mathematical designs within the scope of application attacks such as side channel analysis. An application of this success in image encryption algorithms has been realized with this study.

Another issue that needs to be analyzed to evaluate the success of the proposed method in the fairest way is the encryption performance. It is clear that both the processes used in the encryption function and the chaotic key generator architecture in the proposed algorithm will adversely affect the encryption performance. However, there is trade-off between security level and encryption performance. If an alternative is being sought against both the critical security level and the application attacks, the proposed algorithm would be a good choice.

IV. CONCLUSION

The purpose of this study is to propose an image encryption algorithm that will eliminate security concerns. To achieve this goal, an architecture combining the unpredictable random-like properties of chaotic systems with strong cryptographic primitives that have been proven secure has been proposed. The security of proposed architecture has been verified both statistical tests and indirectly proof method by using security proofs of strong cryptographic primitives.

The cryptographic primitives used in the study eliminated security concerns and revealed a difficult architecture to break. However, the only disadvantage to this architecture can be experienced if the encryption algorithm is implemented on lightweight platforms. In future studies, an option is planned to be developed for the lightweight platforms. Another future study plan is the design of a medical information security application that will be designed by obtaining the secret keys of the algorithm from the person's biometric data.

ACKNOWLEDGMENT

The authors would like to thank the Referee for the constructive comments and recommendations which definitely help to improve the readability and quality of the study.

REFERENCES

[1] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.

[2] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, Apr. 2018.

[3] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, pp. 1–9, Oct. 2019.

[4] A. Perez-Resa, M. Garcia-Bosque, C. Sanchez-Azqueta, and S. Celma, "Chaotic encryption for 10-Gb Ethernet optical links," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 2, pp. 859–868, Feb. 2019.

[5] M. Li, H. Fan, Y. Xiang, Y. Li, and Y. Zhang, "Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system," *IEEE Multimedia Mag.*, vol. 25, no. 3, pp. 92–101, Jul. 2018.

[6] L. Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, and G. Setti, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, Apr. 2018.

[7] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the Feistel network and dynamic DNA encoding," *IEEE Photon. J.*, vol. 10, no. 4, pp. 1–14, Aug. 2018, doi: 10.1109/JPHOT.2018.2859257.

[8] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–15, Jun. 2018, doi: 10.1109/JPHOT.2018.2827165.

[9] Y. Aydin and F. Özkaynak, "A provable secure image encryption schema based on fractional order chaotic systems," in *Proc. 23rd Int. Conf. Electron.*, Palanga, Lithuania, Jun. 2019, pp. 17–19.

[10] J. Wang, Q.-H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–14, Jun. 2018, doi: 10.1109/JPHOT.2018.2831252.

[11] Y. Burhan, F. Artuger, and F. Özkaynak, "A novel hybrid image encryption algorithm based on data compression and chaotic key planning algorithms," in *Proc. 7th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Barcelos, Portugal, Jun. 2019, pp. 1–5.

[12] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, pp. 1–14, Apr. 2018.

[13] Z. Pan and L. Zhang, "Optical cryptography-based temporal ghost imaging with chaotic laser," *IEEE Photon. Technol. Lett.*, vol. 29, no. 16, pp. 1289–1292, Aug. 15, 2017.

[14] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016, doi: 10.1109/ACCESS.2016.2569421.

[15] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018, doi: 10.1109/ACCESS.2018.2805847.

[16] W. Xingyuan, F. Le, W. Shibing, C. Zhang, and Z. Yingqian, "Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption," *IEEE Access*, vol. 6, pp. 39705–39724, 2018, doi: 10.1109/ACCESS.2018.2855726.

[17] H. Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," *IEEE Access*, vol. 6, pp. 42227–42244, 2018, doi: 10.1109/ACCESS.2018.2858839.

[18] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018, doi: 10.1109/ACCESS.2018.2874336.

[19] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581–67593, 2018, doi: 10.1109/ACCESS.2018.2879565.

[20] Z. M. Z. Muhammad and F. Özkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019, doi: 10.1109/ACCESS.2019.2930606.

[21] S. Goldwasser and M. Bellare, "Lecture notes on cryptography, summer course 'cryptography and computer security," MIT, Cambridge, MA, USA, Tech. Rep., 1999. Accessed: Mar. 23, 2020. [Online]. Available: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

[22] M. Bellare, "Practice-oriented provable-security," in *Proc. Int. Workshop Inf. Secur.*, 1997, pp. 221–231.

[23] L. R. Knudsen and M. Robshaw, *The Block Cipher Companion*. Berlin, Germany: Springer, 2011.

[24] C.-K. Wu and B. Feng, *Boolean Functions and Their Applications in Cryptography*. Berlin, Germany: Springer, 2016.

[25] *Permutation-Based Hash and Extendable-Output Functions*, Standard SHA-3, Federal Information Processing Standards, doi: 10.6028/NIST.FIPS.202.

[26] F. Özkaynak, "Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals," in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 621–624, doi: 10.1109/UBMK.2017.8093481.

[27] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.

[28] M. S. Acikkapi, F. Özkaynak, and A. B. Özer, "Side-channel analysis of chaos-based substitution box structures," *IEEE Access*, vol. 7, pp. 79030–79043, 2019.

[29] F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," *Nonlinear Dyn.*, vol. 78, no. 3, pp. 2015–2020, Nov. 2014.

[30] W. Schindler, "Random number generators for cryptographic applications," in *Cryptographic Engineering* (Signals and Communication Theory), C. K. Koc, Ed. Berlin, Germany: Springer, 2009.

[31] S. H. Strogatz, *Nonlinear Dynamics and Chaos With Applications to Physics* (Biology, Chemistry and Engineering), 2nd ed. New York, NY, USA: Taylor & Francis, 2014.

[32] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Gaithersburg, MD, USA: NIST, 2010.

[33] F. Özkaynak, "A novel method to improve the performance of chaos based evolutionary algorithms," *Optik*, vol. 126, no. 24, pp. 5434–5438, Dec. 2015.

[34] K. J. Persohn and R. J. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," *Chaos, Solitons Fractals*, vol. 45, no. 3, pp. 238–245, Mar. 2012.

[35] E. Tanyildizi and F. Özkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019, doi: 10.1109/ACCESS.2019.2936447.

ZAHIR MUHAMMAD ZIAD MUHAMMAD was born in Erbil, in 1978. He received the B.Sc. degree in software engineering from the College of Engineering, Salahaddin University, Erbil, in 2004. He completed his master's thesis titled Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Architecture, in 2019. He plans to use its experience in the scope of these studies to develop secure designs in future studies. Besides his academic career, he has worked as an engineer in many telecommunications companies.

FATİH ÖZKAYNAK received the B.Sc. and M.Sc. degrees in computer engineering from Fırat University, Elazığ, Turkey, in 2005 and 2007, respectively, and the Doctor of Philosophy in computer engineering from Yildiz Technical University, in 2013.

He has taught Algorithm and Programming, Artificial Intelligence, and Cryptography courses at Fırat University. He has supervised many M.Sc. and Ph.D. degree students towards their graduation project in information security and cryptography area. He has coauthored more than 75 refereed scientific journal and conference papers. His works have been cited more than 700 times. His research interests are cryptography, information security, and chaotic systems.