IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 5, 2019, accepted July 18, 2019, date of publication July 23, 2019, date of current version August 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2930606

Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique

ZAHIR MUHAMMED ZIAD MUHAMMAD AND FATİH ÖZKAYNAK
Department of Software Engineering, Fırat University, 23119 Elaziğ, Turkey
Corresponding author: Fatih Özkaynak (ozkaynak@firat.edu.tr)

ABSTRACT Robust protocols are needed to create a secure computing system. Protocols designed without considering various design criteria result in many vulnerabilities. Security has many aspects. The slightest defect in the design processes affects the whole system security. Chaos based image encryption algorithms have become increasingly popular in the recent period. However, most of these algorithms are often based on cryptanalysis driven design technique. Therefore, the security of these algorithms is doubtful as long as the threat of attack continues. In this paper, attention has been drawn to this problem. First, the security problems of two different chaos based image encryption algorithms have been analyzed. In the second analyzed study, the security problem of the first analyzed study has been examined and a new improved version has been published. The common point of these two analyzed studies is that both the original and the improved algorithm are designed on the basis of the cryptanalysis has driven design approach. In other words, the security of these two algorithms is still doubtful. In this study, security problems have been shown for both algorithms and the encryption algorithms have been broken. In the second part of the study, a road map based on a provable secure driven design approach is presented for future studies to avoid such problems.

INDEX TERMS Chaos, cryptography, cryptanalysis, image encryption, security problem.

I. INTRODUCTION

There are many successful applications of chaotic systems, as there are theoretically strong relations between chaos theory and many branches of science [38]. One of these successful applications is chaos based cryptology studies. A recent study [49], in particular, confirmed that chaotic systems may be an alternative to application attacks. However, a notorious cryptographic application of these systems is chaos based image encryption algorithms [6], [28], [32], [35]. The researchers claimed that new image encryption algorithms could be designed using the strong theoretical relationship between chaos and cryptography [1]–[3], [7]–[17], [19], [8], [24]–[26], [30], [31], [36]. However, this strong theoretical relationship has led to the emergence of unsecure designs due to misuse and lack of analysis. So much so; many chaos based image encryption algorithms have been broken shortly after the publication [4]–[6], [18], [20]–[23], [27]–[29], [32], [34], [35], [37], [41], [42]. One of these studies has been published by Wu *et al.* [30]. It has been demonstrated by Zhu and Sun [18] after a short time that the proposed protocol is not secure. An improved algorithm has also been proposed to address existing problems. However, this study shown that both the original algorithm and the improved algorithm contain various problems. One of the most important reasons of these problems is the cryptanalysis driven design technique. This serious problem is still in the other proposals designed based on the cryptanalysis driven design technique. The number of chaos based image encryption algorithms published in the last two years in IEEE Access journal is 15 [1]–[3], [7]–[17], [19], [30]. Therefore, it has not been shown how analyzed algorithms could be broken. The common mistakes made by discussing the causes of the problems have been expressed and suggestions have been made to prevent these mistakes in the new studies to be proposed in the future.

The study consists of five sections. In the second section, cryptographic protocol design process is mentioned. The difficulties of this process, the general errors in the design process, the points of weakness, the point of view of the attacker

The associate editor coordinating the review of this manuscript and approving it for publication was Constantinos Marios Angelopoulos.

and the critical points to be considered in the analysis process are explained step by step in this section. In the third section, weaknesses are shown by using the cryptographic protocol evaluation road map as described in the second section for Wu algorithm. Security analysis for improved version is given in Section 4. The obtained results in the last section have been interpreted and recommendations have been made for future studies.

II. CRYPTOGRAPHIC DESIGN PROCESS

The cryptography science can be defined as the establishment and analysis of the protocol to be used to overcome the negative effects of the attacker [43]. The design of a cryptographic protocol is a difficult process. The smallest error or carelessness affects the security of the entire system. Therefore, the design process should be based on various roadmaps, design approaches and acceptable test scenarios. A provable security approach is used to guarantee security in the modern cryptographic protocol design process [44]. This design approach is based on the principle of mathematically proving that confusion and diffusion properties, which are the basic requirements for cryptographic protocols, are provided by cryptographic primitives used in the protocol. In other words, the effect of each process used in the protocol and its effects on the basic requirements should be examined mathematically [40], [44].

This definition of cryptography is important. It was first introduced by Goldwasser and Micali. The researchers' work has earned them the Turing Prize, the most respected award in the field of computer science (is also known as the Nobel Prize of the computer world). They were deemed worthy of this award in 2012 for their impressive work explaining the complexity theory of cryptology and for the development of new methods for efficient verification of mathematical evidence. ''Provable security refers to any type or level of security that can be proved. Usually, this refers to mathematical proofs, which are common in cryptography. In such a proof, the capabilities of the attacker are defined by an adversarial model (also referred to as attacker model): the aim of the proof is to show that the attacker must solve the underlying hard problem in order to break the security of the modeled system.''

However, it is seen that many image encryption proposals in the chaos based cryptography literature is based on the cryptanalysis driven design approach rather than provable security design approach. Although the cryptanalysis driven design approach is an acceptable design approach, it is not known whether the proposed solution method is a correct solution method because it focuses only on current attacks. Another problem is that the design process cannot be ended. Because as long as the threat of attack continues, the solution method may change [28], [43].

The general problem of chaos based image encryption algorithms is the use of statistical tests such as UACI (unified averaged changed intensity), NPCR (The number of changing pixel rate) and histogram analysis to analyze that the proposed method is secure against various attacks [33], [39]. In many studies, the weaknesses in the protocol have not been studied because the success of these tests is based on security. Several studies have published that these protocols can be broken using known simple attacks. Various template attacks, evaluation guides, design criteria are prepared [4]–[6], [20]–[22], [28], [29], [32], [34], [35]. In the next subsection, various evaluation questions that can be used in the analysis process have been prepared.

A. EVALUATION QUESTIONS FOR SECURITY ANALYSIS

Various evaluation questions that can be used in the analysis of any cryptographic protocol are proposed in this section. The purpose of these questions is to reveal common mistakes that can be made in the protocol design process.

Analysis Question 1: Is there a flowchart of the protocol? The flow chart will allow you to easily see the different operations performed in the protocol.

Analysis Question 2: Does each block in the flowchart correspond to a process in the protocol?

Analysis Question 3: Convert each process in the protocol to a function.

Analysis Question 4: What is the purpose of each function?

Analysis Question 5: Does the mathematical definition of the function provide this objective?

Analysis Question 6: Is there a measurement that can check that it provides the purpose?

Analysis Question 7: What is the definition and display set of each function?

Analysis Question 8: Are there any other functions equivalent to the functions you have obtained?

III. SECURITY PROBLEMS OF WU ALGORITHM

This section analyzes the security problems of image encryption algorithm proposed by Wu et al [30]. The flowchart of the Wu et al. algorithm is shown in Figure 1. This way of expressing the algorithm makes it easy to see many details. For example, the following inferences can be made using only the flowchart.

- The flowchart has two main part. In other words, the encrypted image is determined by the XOR operation of the two main block outputs in the flowchart.
- The right part converts the chaotic values to the key values between 0-255. It is used to provide the confusion property which is one of the basic requirements of the cryptographic protocol.
- The left part is used to change the pixel positions. It is used to ensure the diffusion property of the cryptographic protocol.
- There are nine blocks in the flowchart (there are nine functions in the cryptographic protocol).
- The secret key of the algorithm is used in only two blocks of the flowchart (ie, only two functions of the cryptographic protocol).

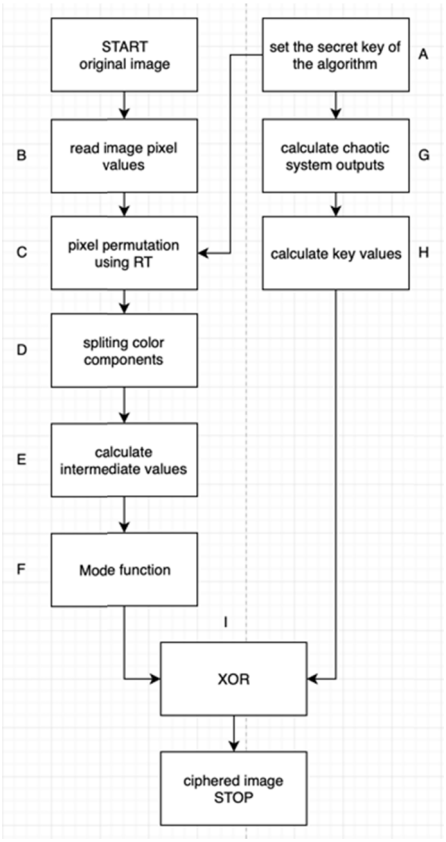

FIGURE 1. The flowchart of Wu et al chaotic image encryption algorithm.

In the flowchart, various symbols are used to distinguish each block easily. In order to better understand the algorithm operation, the algorithm is shown step by step through a 3×3 small image.

The purpose of the process indicated by the symbol A in the flowchart is to determine the secret key parameters of the image encryption algorithm. The values of two different parameter groups are determined in this process. First parameter group is the initial conditions and control parameters of the chaotic system and the second parameter group is values of rectangular transformation for pixel position changing process.

In the Wu et al algorithm, Tent map is used as chaotic system. The mathematical model of Tent map is given in Eq. (1).

$$\begin{cases} x_{n+1} = \mu x_n & x_n < 0.5 \\ x_{n+1} = \mu(1 - x_n) & x_n \geq 0.5 \end{cases} \tag{1}$$

Tent map consists of one initial condition and one control parameter. Since a different chaotic system is used for each of the color components (R, G, B), three different initial conditions and control parameters are required. The initial conditions and control parameters are selected as Eq. (2).

$$\begin{aligned} \mu_i &= 1.9, \quad x_{10} = 0.201 \\ \mu_2 &= 1.7, \quad x_{20} = 0.301 \\ \mu_3 &= 1.6, \quad x_{30} = 0.401 \end{aligned} \tag{2}$$

TABLE 1. Chaotic outputs for tent map.

i	X_{1i}	X_{2i}	X_{3i}
1	0.6738250607	0.3049856093	0.6031158683
2	0.6197323845	0.5184755358	0.6350146105
3	0.7225084693	0.8185915891	0.583976623
4	0.5272339082	0.3083942985	0.6656374031
5	0.8982555742	0.5242703074	0.534980155
6	0.1933144088	0.8087404772	0.7440317519
7	0.3672973768	0.3251411886	0.4095491968
8	0.6978650159	0.5527400207	0.655278715
9	0.5740564696	0.7603419647	0.5515540559

These selected values in Eq. (2) are input to G function of flowchart. The G function calculates $1000 + 9$ times using the output of chaotic systems. The first 1000 values have been ignored for transient behavior. For the 3×3 size image, 9 values are given in Table 1.

The chaotic system outputs calculated at the output of the G function are input to the H function of flowchart. The key values are calculated by using Eq. (3) in the H function.

$$\begin{aligned} S_{1i} &= \left\lfloor x_{1i} \times 10^{10} \right\rfloor mod\ 256 \\ S_{2i} &= \left\lfloor x_{2i} \times 10^{10} \right\rfloor mod\ 256 \\ S_{3i} &= \left\lfloor x_{3i} \times 10^{10} \right\rfloor mod\ 256 \end{aligned} \tag{3}$$

The key values to be used for encrypting R, G, B components are given in Eq. (4) for the selected initial conditions and control parameters.

$$\begin{aligned} S_1 &= [194, 219, 146, 3, 45, 170, 220, 167, 143] \\ S_2 &= [230, 185, 196, 245, 154, 250, 91, 36, 145] \\ S_3 &= [212, 172, 185, 114, 75, 85, 174, 182, 118] \end{aligned} \tag{4}$$

The other parameters defined in function A are indicated by the symbols a, b, c, d, r_m, r_n, t. These parameters will be used to change pixel positions in the C function. However, in the determination of these parameters, it is required to make the selection according to the rules given in Eq. (5). However, these limitations create a weakness for square-sized images. Considering that many test images are square-sized, this problem will cause serious security vulnerabilities.

$$\begin{cases} p = \gcd(m, n), & p_m = \dfrac{p}{m},\ p_n = \dfrac{p}{n} \\ \gcd(a, p_m) = 1, & \gcd(d, p_n) = 1 \\ (b\ mod\ p_m) = 0 & or\ (c\ mod\ p_n) = 0 \\ \gcd(ad - bc, p) = 1 \end{cases} \tag{5}$$

For example, we want to encrypt a 3×3 image, in this case Eq. (7):

$$\begin{aligned} p_m &= 3/3 = 1 \\ p_n &= 3/3 = 1 \\ \gcd(a, p_m) &= 1 \text{ so probable } a \text{ values } \{0, 1, 2\} \\ \gcd(d, p_n) &= 1 \text{ so probable } d \text{ values } \{0, 1, 2\} \\ (b\ mod\ p_m) &= 0 \text{ so probable } b \text{ values } \{0, 1, 2\} \end{aligned}$$

$$(c \; mod \; p_n) = 0 \text{ so probable } c \text{ values } \{0, 1, 2\}$$
$$\gcd(ad - bc, p) = 1 \tag{6}$$

Possible values a, b, c, d for a 3×3 image are given in Table 2. In our example scenario, the parameter values have been selected as $a = 1, b = 0, c = 0, d = 1, r_m = 2, r_n = 2, t = 2$.

TABLE 2. Probable values for 3 × 3 example image.

i	1	2	3	4	5	6	7	8	9
a	1	1	1	1	1	1	1	2	2
b	0	1	2	0	0	2	1	1	1
c	0	0	0	1	2	2	1	1	1
d	1	1	1	1	1	1	2	1	2

If we generalize; in the case of $m = n$ *and* $p = gcd(m, n) = m$. Therefore, $p_m = 1$ and $p_n = 1$. In this case, it is not important to choose for a, d and c. So, the only condition that needs to be provided is $\gcd(ad - bc, p) = 1$.

Mode operation has an important role in the design of cryptographic protocols and is often used. Because the mode operation is both a one-way function and an infinite number of possibilities that give the same output. for example, $x \; mode \; 5 = 3$ has an infinite number of possibilities for x. $x = \{3, 8, 13, 18, 23, 28, 33, \ldots\}$. Similarly $m = 256$ is an infinite key space, the values a, b, c and d must be less than 256. In this case, by using the pseudo code given in Table 3, probable $a, b, c,$ and d values can be determined.

TABLE 3. Pseudo code for probable a, b, c, d values.

```
probable_values={}
for a in m
    for b in m
        for c in m
            for d in m
                İf (gcd(ad-bc)==1)
                    Add probable_values(a,b,c,d)
                end_if
            end for
    end for
end for
return probable_values
```

The implementation of the pseudo code given in Table 3 with the Java programming language is given in Ref. [46]. Analysis results showed that the number of possible $a, b, c,$ and d quartiles is $<2^{30}$. Since this value is less than 2^{80}, it is not resistant to brute force attacks. It shows that the proposed method is not secure.

A more favorable attack scenario occurs when a, d, or b, c pairs is 0. If a, d pairs are 0, the pixel positions will change only in the y coordinate direction, and if b, c pairs are 0, then the pixel positions will change only in the x coordinate direction. This situation will reduce the workload of the attacker.

The R, G, B components of the selected image in B block of the flowchart are obtained. It is assumed that the operation of the algorithm is the best and the pixel values are different from each other. Accordingly, an exemplary image as in Figure 2 has been used in the analyzes. However, the same analysis will apply to the pixel values to be selected at random.

A matrix of size $m \times 3n$ is obtained by combining these three components. The obtained matrix is shown in Figure 3.

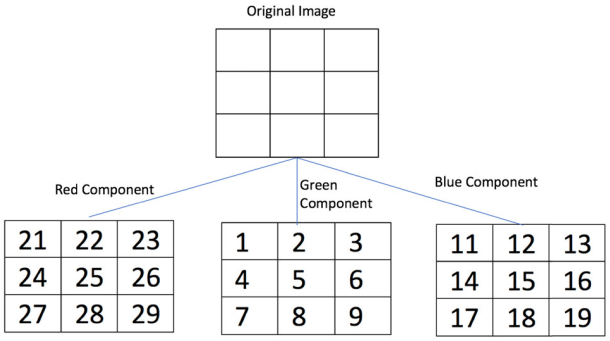

FIGURE 2. The example image for analysis.

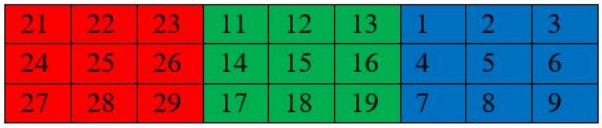

FIGURE 3. The output of B function in flowchart of Wu et al chaotic image encryption algorithm.

The output of function B ($m \times 3n$ matrix) is the input to the function C of flowchart. Pixel positions are changed using Eq. (7). This is known as the diffusion property in cryptographic protocols.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r_m \\ r_n \end{pmatrix} \right] mod \begin{pmatrix} m \\ n \end{pmatrix} \tag{7}$$

However, there is a significant problem for Eq. (7). Since $mod(m, n)$ is used, column values between $n + 1$ and $3n$ do not change. Only values between $2n+1$ and $3n$ are reinserted into columns between 0 and n. Also the red component of the image is lost. This problem is shown in Figure 4. This problem exists in both the original and the improved algorithm.

In the D function, the mx3n matrix is divided into 3 different matrices in $m \times n$ size.

In function E of the flowchart, the various intermediate values to be used in the calculations are calculated. These values are given in Eq. (7).

$$R_{mean} = 5, \quad G_{mean} = 15, \; B_{mean} = 5$$
$$P = 8.33333333333333, \quad \delta = 85$$
$$R' = 90, \quad G' = 100, \; B' = 90, \tag{8}$$

As a result of the process steps indicated by F and I, the encoded image values are obtained. All calculated values are shown step by step in Eq. (8).

9	7	8	11	12	13	1	2	3
3	1	2	14	15	16	4	5	6
6	4	5	17	18	19	7	8	9

FIGURE 4. The output of C function in flowchart of Wu et al chaotic image encryption algorithm.

9	7	8
3	1	2
6	4	5

11	12	13
14	15	16
17	18	19

1	2	3
4	5	6
7	8	9

FIGURE 5. The output of D function in flowchart of Wu et al chaotic image encryption algorithm.

5	16	11
146	243	78
23	145	150

89	197	45
143	117	138
193	190	107

107	204	97
78	109	59
113	86	46

FIGURE 6. The output of I function in flowchart of Wu et al chaotic image encryption algorithm.

The encrypted values for the three color components are shown in Figure 6.

IV. SECURITY PROBLEMS OF ZHU AND SUN IMAGE ENCRYPTION ALGORITHM

Zhu and Sun [18] showed that the Wu algorithm could be broken by using chosen plaintext attack. They then published an improved version of the Wu algorithm to avoid the security vulnerabilities they detected. In the improved algorithm proposed by Zhu and Sun, only chaotic systems are not used. It is also assumed that security can be improved by using strong primitive structures of modern cryptology.

In the Section 3, it has been shown that the Wu algorithm could be broken using brute force attack. One of the other important problems of the Wu algorithm is that the original image has no effect on the key planning algorithm. To eliminate this problem, it has been proposed to use the hash values produced by the SHA-3 algorithm, one of the most recently published cryptographic standards, in the key planning process. It is assumed that the proposed improved design will be secure since there is no security vulnerability that threatens the SHA-3 algorithm. In other words, the cryptanalysis driven design principle is adopted as in the Wu algorithm. The security analysis of the proposed algorithm has been analyzed only by statistical tests.

$$
\begin{aligned}
r_{i+1} &= ((r_i + g_i^{'} + b_i^{'}) mod 256) \oplus s_1(i) \\
g_{i+1} &= (r_{i_i}^{'} + g_i + b_i^{'}) mod 256) \oplus s_2(i) \\
b_{i+1} &= ((r_i^{'} + g_i^{'} + b_i) mod 256) \oplus s_3\,(i) \\
r0 &= ((9 + 100 + 90) mod 256) \oplus 194 = 5 \\
g0 &= ((11 + 90 + 90)\, mod 256) \oplus 230 = 89 \\
b0 &= ((1 + 90 + 100)\, mod 256) \oplus 212 = 107 \\
r1 &= ((7 + g0 + b0) mod 256) \oplus 219 = 16 \\
g1 &= ((12 + r0 + b0) mod 256) \oplus 185 = 197 \\
b1 &= ((2 + r0 + g0) mod 256) \oplus 172 = 204 \\
r2 &= ((8 + g1 + b1) mod 256) \oplus 146 = 11 \\
g2 &= ((13 + r1 + b1) mod 256) \oplus 196 = 45 \\
b2 &= ((3 + r1 + g1) mod 256) \oplus 185 = 97 \\
r3 &= ((3 + g2 + b2) mod 256) \oplus 3 = 146 \\
g3 &= ((14 + r2 + b2) mod 256) \oplus 24 = 143 \\
b3 &= ((4 + r2 + g2) mod 256) \oplus 114 = 78 \\
r4 &= ((1 + g3 + b3) mod 256) \oplus 45 = 243 \\
g4 &= ((15 + r3 + b3) mod 256) \oplus 154 = 117 \\
b4 &= ((5 + r3 + g3) mod 256) \oplus 75 = 109 \\
r5 &= ((2 + g4 + b4) mod 256) \oplus 170 = 78 \\
g5 &= ((16 + r4 + b4) mod 256) \oplus 250 = 138 \\
b5 &= ((6 + r4 + g4)\, mod 256) \oplus 85 = 59 \\
r6 &= ((6 + g5 + b5) mod 256) \oplus 220 = 23 \\
g6 &= ((17 + r5 + b5) mod 256) \oplus 91 = 193 \\
b6 &= ((7 + r5 + g5) mod 256) \oplus 174 = 113 \\
r7 &= ((4 + g6 + b6) mod 256) \oplus 167 = 145 \\
g7 &= ((18 + r6 + b6) mod 256) \oplus 36 = 190 \\
b7 &= ((8 + r6 + g6) mod 256) \oplus 182 = 86 \\
r8 &= ((5 + g7 + b7) mod 256) \oplus 143 = 150 \\
g8 &= ((19 + r7 + b7) mod 256) \oplus 145 = 107 \\
b8 &= ((9 + r7 + g7) mod 256) \oplus 118 = 46 \qquad (9)
\end{aligned}
$$

In analyzing the Wu algorithm, Zhu and Sun have used the Kerchoff's principle. This approach, based on the assumption that the attacker has an infinite computational capacity and s(he) knows everything related to algorithm except the secret key. This is a very strong evaluation approach. In other words; each piece of information associated with the cryptographic protocol may be considered an attack vector. In fact, an attacker does not always examine the algorithm from the designer's perspective. If mathematical proof of the proposed algorithm is not given, reverse engineering, the use of isomorphic structures equivalent to the protocol, and examining effects of the calculation environment are tried to analyze the problems in the algorithm.

In this study, it has been shown that the Zhu and Sun algorithm can be broken by attacking SHA-3 structure which is one of the most powerful features of the improved algorithm. The reason for the weakness of the algorithm is not due to the SHA-3 algorithm. The weakness is related to the use of the SHA-3 algorithm. In the improved algorithm, the hash values of the original images are associated with the initial conditions of the chaotic system. Authors claimed that this approach has been prevented to chosen plaintext attack. The analysis process is shown below in a step-by-step way to best reflect the cryptanalyst perspective.

Step 1: A cryptanalyst should question why each process is used. There is no justification for the use of the SHA-3 in the

FIGURE 7. The test images 256 × 256-size.

TABLE 4. Hash values for test images 256 × 256-size.

IMAGE	SHA-3 HASH VALUES
A	67196f36eae593484d885e10ea83b84134d820d1b32ecd611f8ed66f2db64baf
B	301079d780dc7717f5c790f8297778b05964bd1595449b5db7d4790dd540e564
C	17b0b829ed7321521ed66f9a13511746e032315b85aee963b1b4ef41137a5821
D	a1fb654f34d0dad1ad8b67586a30a20ea3eaeadec6b2d778dafc906bb3dbfd9e
E	e6d16ac453a6f8430f44b1116db7cfc0c7184aab216c109101074281e89b8da5
F	5e8917a0875e696afd71ba463a581e108f3bca88b0bbf6e37123fcaba5d45617
G	dbc8f820295ae41f27b354c95ba164d44bbb604b7b5018122310e6fcd0e3bc9e
H	86fc6644e854ef8f1938b0e6c47a28036bc19e3d4f4f0dff54d0dad12d4c531

improved algorithm developed by Zhu and Sun. Any action that is not clear will constitute a potential threat.

Step 2: What is the purpose of the SHA-3 algorithm? Are there any advantages or disadvantages? SHA-3 is a hash function. It is a one-way function. This is the desired basic feature for cryptography applications. It produces 256-bit length outputs and takes the arbitrary data as input. One-bit change in the input leads to large changes in output. It is not possible to make a statistical deduction on the calculated hash values.

Step 3: How did SHA-3 hash values be used in the algorithm? The δ value for each image was calculated using Eq. (10).

$$\delta = (\sum_{i=1}^{i=32} h_i)/(32 \times 256) \tag{10}$$

Hypothesis: One of the basic requirements in the hash functions is to have a uniform distribution of output values to avoid statistical inference. In this case, the output of Eq. (10) is expected to be close to a certain value.

TABLE 5. δ value for test images 256 × 256-size.

Image	δ Value
a	0.2333984375
b	0.266357421875
c	0.1944580078125
d	0.2578125
e	0.2774658203125
f	0.20361328125
g	0.26318359375
h	0.256591796875

Figure 7 shows eight different standard test images [45] (256 × 256 sizes). The hash values calculated for the SHA-3 algorithm of these images are given in Table 4. δ values calculated using Eq. (10) are given in Table 5.

Figure 8 shows standard test images of 512 × 512 size. The hash values calculated for these images in Figure 8 are given in Table 6 and the delta values are given in Table 7.

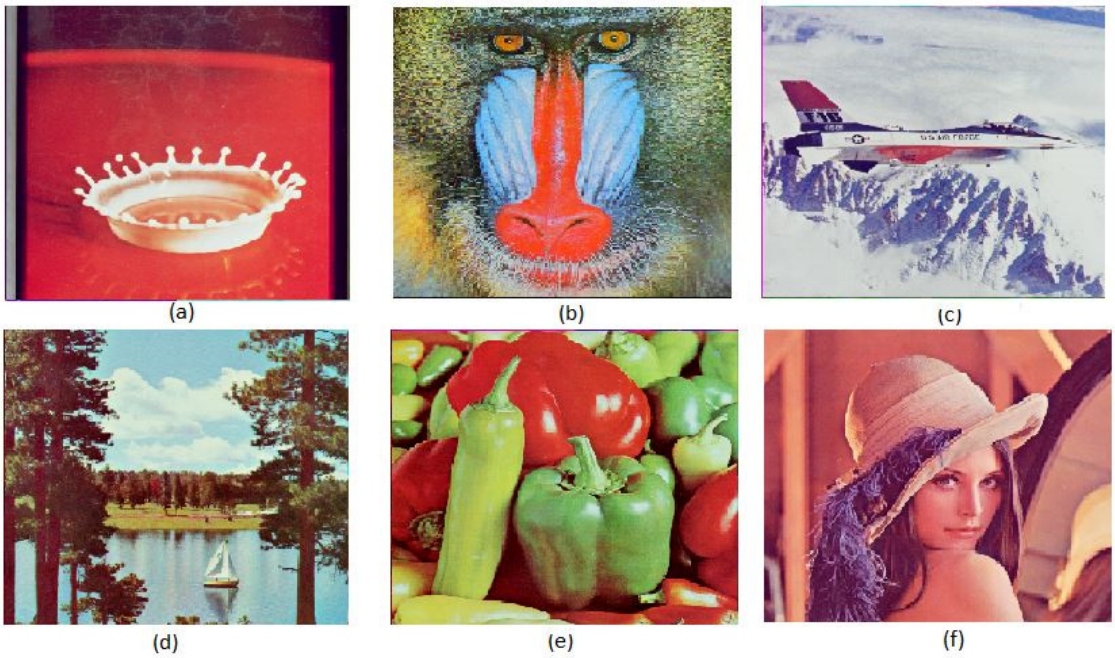

FIGURE 8. The test images 512 × 512-size.

TABLE 6. Hash values for test images 512 × 512-size.

IMAGE	SHA-3 HASH VALUES
A	02c422ce429a8ec49f3f9e7033089b0c660d9353ffa8bc112d628af12f7b0c9b
B	e68aec2c584adeedb4096965115b13399ecb6ccf74fdbd3501fb6d3e5696f7f6
C	37cd5d72f97ec68a3b1c10545524f4d88ceaf43fd7dba5c333e0b6faaed5f43a
D	ff149be22d573ec04ba8a31d6e10aa884f990bd371d9d6e4f7ac2eb4ecdc4dfe
E	6e46bc932025ca5d1f8d1a6a2521f6ebca75be644946580a07017004aa91686b
F	9fe0e1d86be69d7977a0ad3532c20104769097bdb5457b8a02f6e4561db51050

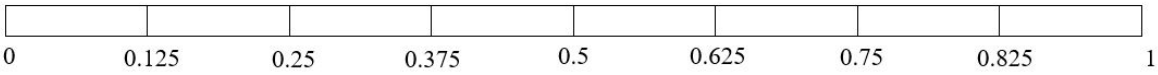

FIGURE 9. The range of data demonstration for 3-bit length machine.

TABLE 7. δ Value for test images 512 × 512-size.

Image	
a	0.209228515625
b	0.2255859375
c	0.237548828125
d	0.2330322265625
e	0.211669921875
f	0.2677001953125

The average values in Table 5 and Table 7 converge to a certain range. The average value for Table 5 is 0.244110107421875. similarly, the calculated average value for Table 7 is 0.23079427083333334. At first glance, it can be thought that these mean values do not make sense since chaotic systems are sensitive to the initial conditions and control parameters. Slight changes in initial conditions will result in different values being calculated. However, in the literature, it has been determined that the effects of numerical deterioration in the realization of chaotic systems on digital computers could be a security weakness [47], [48]. Combining this security weakness with Kerchoff's principle, an attack scenario was designed. According to Kerchoff's principle, an attacker can make any choice. Suppose you perform calculations using a computer with a three-bit computing capacity. In this case, regardless of the computational value, only one of the eight values given in ranges in Figure 9 will be shown as output. All hash values in Table 5 and Table 7 will

be interpreted as 0.25. In other words, the effect of hash functions will be eliminated in this attack scenario. The key obtained as a result of the analysis on a 3-bit machine can be used to obtain the original image from the encrypted image for any computing precision computer such as 32-bit or 64-bit.

V. CONCLUSION

An acceptable design approaches to designing a cryptographic protocol is the transformation of a computationally difficult problem into a cryptographic protocol. One of the most popular examples of these designs over the last two decades has been chaos based cryptographic design proposals. However, the analysis results showed that many of these proposals have been broken. Although there are various reasons for the security weaknesses, it is seen that the most important factor is the cryptanalysis driven design approach. The fact that cryptanalysis has been done only by statistical tests led to an incorrect interpretation of the security perception. Because the success of the statistical tests has been found to be sufficient.

In this study, it has been shown that statistical tests are necessary but not sufficient. To ensure security, the cryptographic protocols should be based on a provable secure design approach. The purpose of each process used in the protocols and its contribution to ensure cryptographic requirements must be justified. Otherwise, the security of the proposals is questionable as long as the threat of attack continues.

In this study, security analyzes of two chaotic encryption algorithms based on cryptanalysis driven design technique are given. Analysis results showed that the first image encryption algorithm known as the Wu et al algorithm is not resistant to brute force attacks. It has been shown that the algorithm may break with less than 2^{30} attempts. In addition, it is shown that the rectangular transformation used to ensure the diffusion requirement in the algorithm does not work for all pixel values. This problem will reduce the workload of brute force attack for different attack scenarios.

A different attack scenario for Wu et al algorithm have been published by Zhu and Sun. They showed that Wu algorithm is not secure against the chosen plaintext attack. They have also published an improved algorithm to address these weaknesses. However, the improved algorithm is also based on the cryptanalysis driven design approach. In this study is shown justification of hypothesis that the threat of attack will continue even if some weaknesses of the algorithm based on cryptanalysis driven design technique is solved.

In the proposed attack scenario; the key planning algorithm based on the SHA-3 algorithm, which is one of the strengths of the improved algorithm, has been targeted. The results show that the algorithm can be broken by changing the calculating machine. The cause of the attack is due to the wrong use of strong cryptographic primitive (SHA-3 algorithm). Therefore, each process must be justified in the cryptographic protocol.

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] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019. doi: 10.1109/ACCESS.2019.2893538.

[2] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019. doi: 10.1109/ACCESS.2018.2890116.

[3] X. Liu, D. Xiao, and Y. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2019. doi: 10.1109/ACCESS.2018.2889896.

[4] W. Feng, Y. He, H. Li, and C. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, pp. 12584–12597, 2019. doi: 10.1109/ACCESS.2019.2893760.

[5] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.

[6] C. Li, "When an attacker meets a cipher-image in 2018: A year in review," 2019, *arXiv:1903.11764*. [Online]. Available: https://arxiv.org/abs/1903.11764

[7] A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-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.

[8] J. Wang, Q.-H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 7801014. doi: 10.1109/JPHOT.2018.2831252.

[9] 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.

[10] A. A. Abdellatif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2018. doi: 10.1109/ACCESS.2017.2777869.

[11] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," *IEEE Access*, vol. 6, pp. 77740–77753, 2018. doi: 10.1109/ACCESS.2018.2884013.

[12] X. Wand, Y. Hou, S. Wang, and R. Li, "A new image encryption algorithm based on CML and DNA sequence," *IEEE Access*, vol. 6, pp. 62272–62285, 2018. doi: 10.1109/ACCESS.2018.2875676.

[13] 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.

[14] 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.

[15] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018. doi: 10.1109/ACCESS.2018.2879844.

[16] J.-M. Guo, D. Riyono, and H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing," *IEEE Access*, vol. 6, pp. 46297–46321, 2018. doi: 10.1109/ACCESS.2018.2863021.

[17] 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.

[18] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018. doi: 10.1109/ACCESS.2018.2817600.

[19] 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.

[20] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018. doi: 10.1109/ACCESS.2018.2883690.

[21] M. Li, D. Lu, W. Wen, H. Ren, and Y. Zhang, "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2018. doi: 10.1109/ACCESS.2018.2867111.

[22] 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*, vol. 25, no. 3, pp. 92–101, Jul./Sep. 2018.

[23] 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

[24] 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, Aug. 2018, Art. no. 3901014. doi: 10.1109/JPHOT.2018.2859257.

[25] 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, Jun. 2018, Art. no. 3900515. doi: 10.1109/JPHOT.2018.2827165.

[26] 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, Apr. 2018, Art. no. 7201714.

[27] W. Feng and Y.-G. He, "Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling," *IEEE Photon. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7909215. doi: 10.1109/JPHOT.2018.2880590.

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

[29] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018.

[30] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017. doi: 10.1109/ACCESS.2017.2692043.

[31] 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.

[32] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, pp. 150–154, Mar. 2017.

[33] 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.

[34] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017.

[35] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Process.*, vol. 118, pp. 203–210, Jan. 2016.

[36] G. Ye and X. Huang, "An image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 23, no. 2, pp. 64–71, Apr./Jun. 2016.

[37] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.

[38] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, 2nd ed. London, U.K.: Taylor & Francis, 2014.

[39] 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.

[40] M. Bellare and D. Cash, "Pseudorandom functions and permutations provably secure against related-key attacks," in *Proc. Annu. Cryptol. Conf.*, 2010, pp. 666–684.

[41] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalyzing an encryption scheme based on blind source separation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 4, pp. 1055–1063, May 2008.

[42] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalysis of an image scrambling scheme without bandwidth expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 3, pp. 338–349, Mar. 2008.

[43] S. Goldwasser and M. Bellare, *Lecture Notes on Cryptography, Summer Course 'Cryptography and Computer Security'*. Cambridge, MA, USA: MIT, 1999.

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

[45] *The USC-SIPI Image Database*. Accessed: Jul. 27, 2019. [Online]. Available: http://sipi.usc.edu/database/

[46] *Source Code Examples for Proposed Cryptanalysis*. Accessed: Jul. 27, 2019. [Online]. Available: www.kriptarium.com/cryptanalysis

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

[48] 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, pp. 238–245, Mar. 2012.

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

ZAHIR MUHAMMED ZIAD MUHAMMAD was born in Erbil, in 1978. He completed the B.Sc. degree in software engineering from the College of Engineering, University of Salahaddin, Erbil, in 2004. He is currently pursuing the master's degree with the Department of Software Engineering, Faculty of Technology, Fırat University, and is currently working on his master thesis on the security analysis of cryptographic protocols that are not based on mathematical principles. Besides his academic career, he has worked as an Engineer in many telecommunications companies.

FATİH ÖZKAYNAK received the Bachelor of Science and Master of Science degrees in computer engineering from Fırat University, Elaziğ, Turkey, in 2005 and 2007, respectively, and the Doctor of Philosophy degree in computer engineering from Yildiz Technical University, in 2013.

He has taught algorithm and programming I/II, artificial intelligence, and cryptography courses at Fırat University. He has supervised four Master of Science and two Ph.D. students towards their graduation project in information security and cryptography area. He is currently an Associate Professor of software engineering with Fırat University. He has coauthored over 50 refereed scientific journal and conference papers. His works have been cited more than 500 times. His h-index is 11. His research interests include cryptography, information security, and chaotic systems.

He serves as a Reviewer for scientific journals, including *Cryptography and Communications - Discrete Structures*, *Boolean Functions and Sequences*, *Information Sciences*, the IEEE Transactions on Very Large Scale Integration Systems, *IET Information Security*, *Security and Communication Networks*, *Computers & Electrical Engineering*, *Applied Soft Computing*, *Physics Letter A*, and *Applied Mathematical Modelling*.