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

Zahir Muhammed Ziad Muhammad1, Fatih Özkaynak1
1Department of Software Engineering, Fırat University, Elazığ, 23119 Turkey
Corresponding author: Fatih Özkaynak (e-mail: ozkaynak@firat.edu.tr).

ABSTRACT Robust protocols are needed to create a secure computing systems. 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 study, attention has been drawn to this problem. Firstly, 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 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 [39]. One of these successful applications is chaos based cryptology studies. A recent study [50], 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, 29, 33, 36]. 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, 24-27, 31, 32, 37]. 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, 28-30, 33, 35, 36, 38, 42, 43]. One of these studies has been published by Wu et al [31]. 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, 31]. 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 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 [44]. 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 [45]. 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 [41, 45].

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 modelled 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 [29, 44].

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 [34, 40]. 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, 29, 30, 33, 35, 36]. 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 [31]. 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 (i.e., only two functions of the cryptographic protocol).

\[
\begin{align*}
    x_{n+1} &= \mu x_n & x_n < 0.5 \\
    x_{n+1} &= \mu(1 - x_n) & x_n \geq 0.5
\end{align*}
\]  

(Tent map) (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).

\[
\begin{align*}
    \mu_1 &= 1.9, x_{10} = 0.201 \\
    \mu_2 &= 1.7, x_{20} = 0.301 \\
    \mu_3 &= 1.6, x_{30} = 0.401
\end{align*}
\]  

(2)

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 3x3 size image, 9 values are given in Table 1.

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

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.

\[
\begin{align*}
    S_{1i} &= [x_{i1} \times 10^{10}] \mod 256 \\
    S_{2i} &= [x_{i2} \times 10^{10}] \mod 256 \\
    S_{3i} &= [x_{i3} \times 10^{10}] \mod 256
\end{align*}
\]  

(3)

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

(4)

The other parameters defined in function A are indicated by the symbols \(a, b, c, d, r_{min}, r_n, t\). 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.
\[
\begin{align*}
\{ p = \gcd(m, n), p_m = \frac{p}{m}, p_n = \frac{p}{n} \\
\gcd(a, p_m) = 1, \gcd(d, p_n) = 1 \\
(b \mod p_m) = 0 \text{ or } (c \mod p_n) = 0 \\
\gcd(ad - bc, p) = 1
\end{align*}
\] (5)

For example, we want to encrypt a 3x3 image, in this case Eq. (6):

\[
\begin{align*}
p_m &= \frac{3}{3} = 1 \\
p_n &= \frac{3}{3} = 1 \\
\gcd(a, p_m) &= 1 \text{ so probable } a \text{ values \{0,1,2\}} \\
\gcd(d, p_n) &= 1 \text{ so probable } d \text{ values \{0,1,2\}} \\
(b \mod p_m) &= 0 \text{ so probable } b \text{ values \{0,1,2\}} \\
(c \mod p_n) &= 0 \text{ so probable } c \text{ values \{0,1,2\}} \\
\gcd(ad - bc, p) &= 1
\end{align*}
\] (6)

Possible values a, b, c, d for a 3x3 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>
<thead>
<tr>
<th>TABLE II</th>
<th>PROBABLE VALUES FOR 3X3 EXAMPLE IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>a</td>
<td>1</td>
</tr>
<tr>
<td>b</td>
<td>0</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
</tr>
<tr>
<td>d</td>
<td>1</td>
</tr>
</tbody>
</table>

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, \(x \mod 5 = 3\) 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>
<thead>
<tr>
<th>TABLE III</th>
<th>PSEUDO CODE FOR PROBABLE A, B, C, D VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>probable_values=[]</td>
</tr>
<tr>
<td></td>
<td>for a in m</td>
</tr>
<tr>
<td></td>
<td>for b in m</td>
</tr>
<tr>
<td></td>
<td>for c in m</td>
</tr>
<tr>
<td></td>
<td>for d in m</td>
</tr>
<tr>
<td></td>
<td>If (gcd(ad-bc)==1)</td>
</tr>
<tr>
<td></td>
<td>Add probable_values(a,b,c,d)</td>
</tr>
<tr>
<td></td>
<td>end if</td>
</tr>
<tr>
<td></td>
<td>end for</td>
</tr>
<tr>
<td></td>
<td>end for</td>
</tr>
<tr>
<td></td>
<td>return probable_values</td>
</tr>
</tbody>
</table>

The implementation of the pseudo code given in Table 3 with the Java programming language is given in Ref. [47]. Analysis results showed that the number of possible a, b, c, and d quantities is \(<2^{30}\). Since this value is less than \(2^{30}\), 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 are 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.

![FIGURE 2. The example image for analysis.](image)

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

![FIGURE 3. The output of B function in flowchart of Wu et al chaotic image encryption algorithm.](image)
image is lost. This problem is shown in Figure 4. This problem exists in both the original and the improved algorithm.

\[
\begin{array}{ccccccccc}
9 & 7 & 8 & 11 & 12 & 13 & 1 & 2 & 3 \\
3 & 1 & 2 & 14 & 15 & 16 & 4 & 5 & 6 \\
6 & 4 & 5 & 17 & 18 & 19 & 7 & 8 & 9 \\
\end{array}
\]

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

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

\[
\begin{array}{ccccccccc}
9 & 7 & 8 & 11 & 12 & 13 & 1 & 2 & 3 \\
3 & 1 & 2 & 14 & 15 & 16 & 4 & 5 & 6 \\
6 & 4 & 5 & 17 & 18 & 19 & 7 & 8 & 9 \\
\end{array}
\]

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

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).

\[
\begin{align*}
R_{mean} &= 5, \quad G_{mean} = 15, \quad B_{mean} = 5 \\
P &= 8.33333333333333, \quad \delta = 85 \\
R' &= 90, \quad G' = 100, \quad B' = 90,
\end{align*}
\]

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).

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

\[
\begin{array}{cccc}
5 & 16 & 11 \\
146 & 243 & 78 \\
23 & 145 & 150 \\
\end{array}
\quad
\begin{array}{cccc}
89 & 197 & 45 \\
143 & 117 & 138 \\
193 & 190 & 107 \\
\end{array}
\quad
\begin{array}{cccc}
107 & 204 & 97 \\
78 & 109 & 59 \\
113 & 86 & 46 \\
\end{array}
\]

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

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 cryptography.

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.

\[
\begin{align*}
n_{i+1} &= (r_i + g_i + b_i) \mod 256 \oplus s_i(i) \\
g_{i+1} &= (r'_i + g_i + b_i) \mod 256 \oplus s_2(i) \\
b_{i+1} &= (r'_i + g_i + b_i) \mod 256 \oplus s_3(i)
\end{align*}
\]

\[
\begin{align*}
r_0 &= ((9 + 100 + 90) \mod 256) \oplus 194 = 5 \\
g_0 &= ((11 + 90 + 90) \mod 256) \oplus 230 = 89 \\
b_0 &= ((1 + 90 + 100) \mod 256) \oplus 212 = 107
\end{align*}
\]

\[
\begin{align*}
r_1 &= ((7 + 90 + 0) \mod 256) \oplus 219 = 16 \\
g_1 &= ((12 + r_0 + 0) \mod 256) \oplus 185 = 197 \\
b_1 &= ((2 + r_0 + g_0) \mod 256) \oplus 172 = 204
\end{align*}
\]

\[
\begin{align*}
r_2 &= ((8 + g_1 + b_1) \mod 256) \oplus 146 = 11 \\
g_2 &= ((13 + r_1 + b_1) \mod 256) \oplus 196 = 45 \\
b_2 &= ((3 + r_1 + g_1) \mod 256) \oplus 185 = 97
\end{align*}
\]

\[
\begin{align*}
r_3 &= ((3 + g_2 + b_2) \mod 256) \oplus 3 = 146 \\
g_3 &= ((14 + r_2 + b_2) \mod 256) \oplus 24 = 143 \\
b_3 &= ((4 + r_2 + g_2) \mod 256) \oplus 114 = 78
\end{align*}
\]

\[
\begin{align*}
r_4 &= ((1 + g_3 + b_3) \mod 256) \oplus 45 = 243 \\
g_4 &= ((15 + r_3 + b_3) \mod 256) \oplus 154 = 117 \\
b_4 &= ((5 + r_3 + g_3) \mod 256) \oplus 75 = 109
\end{align*}
\]

\[
\begin{align*}
r_5 &= ((2 + g_4 + b_4) \mod 256) \oplus 170 = 78 \\
g_5 &= ((16 + r_4 + b_4) \mod 256) \oplus 250 = 138 \\
b_5 &= ((6 + r_4 + g_4) \mod 256) \oplus 85 = 59
\end{align*}
\]

\[
\begin{align*}
r_6 &= ((6 + g_5 + b_5) \mod 256) \oplus 220 = 23 \\
g_6 &= ((17 + r_5 + b_5) \mod 256) \oplus 91 = 193 \\
b_6 &= ((7 + r_5 + g_5) \mod 256) \oplus 174 = 113
\end{align*}
\]

\[
\begin{align*}
r_7 &= ((4 + g_6 + b_6) \mod 256) \oplus 167 = 145 \\
g_7 &= ((18 + r_6 + b_6) \mod 256) \oplus 36 = 190 \\
b_7 &= ((8 + r_6 + g_6) \mod 256) \oplus 182 = 86
\end{align*}
\]

\[
\begin{align*}
r_8 &= ((5 + g_7 + b_7) \mod 256) \oplus 143 = 150 \\
g_8 &= ((19 + r_7 + b_7) \mod 256) \oplus 145 = 107 \\
b_8 &= ((9 + r_7 + g_7) \mod 256) \oplus 118 = 46
\end{align*}
\]

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 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 $\delta$ value for each image was calculated using Eq. (9).

$$\delta = \left(\sum_{i=1}^{32} h_i\right) / (32 \times 256)$$  \hspace{1cm} (9)

**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. (9) is expected to be close to a certain value.

Figure 7 shows eight different standard test images [46] (256 × 256 sizes). The hash values calculated for the SHA-3 algorithm of these images are given in Table 4. $\delta$ values calculated using Eq. (9) are given in Table 5.

![Figure 7](image_url)
Table IV: Hash Values for Test Images 256 x 256-Size

<table>
<thead>
<tr>
<th>Image</th>
<th>SHA-3 Hash Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>67196f36eeac593484d85e10eabc8d4f20dfe32ed61f0ed6fd2d64baf</td>
</tr>
<tr>
<td>B</td>
<td>301079d780dc77175c7909297778605964bd1595449b5db74790dd540e564</td>
</tr>
<tr>
<td>C</td>
<td>17b60b829ed7321521ed669a13511746e032315b85ace963b1b4e4f1137a5821</td>
</tr>
<tr>
<td>D</td>
<td>a1f6b54f34d0d02d7a86b7586a30a20ea3c9eae66ca62d778dacf906eb3dbfd9e</td>
</tr>
<tr>
<td>E</td>
<td>ec6f16ec53a6f8430f4bb111d6db7cfed7149a2f216c109101074281e89b8da5</td>
</tr>
<tr>
<td>F</td>
<td>5e8917e0875e696ada71ba463a981e1088f8bc95a88bbfbc9e71323f0a5a5d45617</td>
</tr>
<tr>
<td>G</td>
<td>dbe8f20295ae41f27354b95ba164d44bb6048b750181223106e6d02e3bc9f</td>
</tr>
<tr>
<td>H</td>
<td>86f68d84e854e8f19388b0e6c47a28036bc19e3d4f40df54d0d1d2d4c531</td>
</tr>
</tbody>
</table>

Table V: δ Value for Test Images 256 x 256-Size

<table>
<thead>
<tr>
<th>Image</th>
<th>δ Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>0.2333984375</td>
</tr>
<tr>
<td>b</td>
<td>0.266357421875</td>
</tr>
<tr>
<td>c</td>
<td>0.1944580078125</td>
</tr>
<tr>
<td>d</td>
<td>0.2578125</td>
</tr>
<tr>
<td>e</td>
<td>0.2774658203125</td>
</tr>
<tr>
<td>f</td>
<td>0.20361328125</td>
</tr>
<tr>
<td>g</td>
<td>0.26318359375</td>
</tr>
<tr>
<td>h</td>
<td>0.256591796875</td>
</tr>
</tbody>
</table>

Figure 8 shows standard test images of 512x512 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.

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 [48, 49]. 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.


<table>
<thead>
<tr>
<th>IMAGE</th>
<th>SHA-3 HASH VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>02c422ce4298ec49f39f0e70330896ec660d9353fa8bc112d628af12f7b0c9b</td>
</tr>
<tr>
<td>B</td>
<td>e68ace2c584adeedeb409695115b13399ecbc74f6dbd3501b6d345e5696f7f6</td>
</tr>
<tr>
<td>C</td>
<td>37cd5d72f97ec68a3b1c10545524f888ceaf43f7d7ba533c3e6b6faaed5f43a</td>
</tr>
<tr>
<td>D</td>
<td>f149be22d373e048a931d6e10aa8f4900db371d9d6b4f7ac2eb4edc5d4e</td>
</tr>
<tr>
<td>E</td>
<td>6e46a0930252a5d1f1d1a6a2521f6ebc75be644946580a0701704a91686b</td>
</tr>
<tr>
<td>F</td>
<td>9e0e1d86e69d7977a0ad3532c20104769097b854578a026e84561db51050</td>
</tr>
</tbody>
</table>

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

**TABLE VII**

<table>
<thead>
<tr>
<th>Image</th>
<th>( \delta ) VALUE FOR TEST IMAGES 512 × 512-SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>0.209228515625</td>
</tr>
<tr>
<td>b</td>
<td>0.225589375</td>
</tr>
<tr>
<td>c</td>
<td>0.23754882125</td>
</tr>
<tr>
<td>d</td>
<td>0.2330322265625</td>
</tr>
<tr>
<td>e</td>
<td>0.211669921875</td>
</tr>
<tr>
<td>f</td>
<td>0.2677001953125</td>
</tr>
</tbody>
</table>

**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 gratefully thank to the Referee for the constructive comments and recommendations which definitely help to improve the readability and quality of the study.

**REFERENCES**

ZAHIR MUHAMMAD ZIAD MUHAMMAD was born in Erbil in 1978. Between 2000-2004, he completed his B.Sc. education in Software Engineering from College of Engineering University of Salahaddin, Erbil. He is currently master student in Fırat University Faculty of Technology, Department of Software Engineering 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 is an associate professor of Software Engineering at Fırat University. He received his Bachelor of Science degree in Computer Engineering from Fırat University, Elazığ, Turkey in 2005, Master of Science degree from Computer Engineering from Fırat University in 2007, and Doctor of Philosophy in Computer Engineering from Yıldız Technical University in 2013.

Dr. Özkanak’s research interests are cryptography, information security, and chaotic systems. He has co-authored over 50 refereed scientific journal and conference papers. His works have been cited more than 500 times. His h-index is 11. He has taught Algorithm and Programming I/II, Artificial Intelligence, and Cryptography courses at Fırat University. He has supervised 4 Master of Science and 2 PhD students towards their graduation project in information security and cryptography area.