IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 31, 2021, accepted September 26, 2021, date of publication October 5, 2021, date of current version October 12, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3118050*

# A Finite Precision Implementation of an Image Encryption Scheme Based on DNA Encoding and Binarized Chaotic Cores

**RANIA A. ELMANFALOTY[1,2], ABDULLAH M. ALNAJIM[3], AND EHAB ABOU-BAKR[4,5]**

[1]Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]Department of Electronics and Communications Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21311, Egypt
[3]Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[4]Department of Computer Engineering, The Higher Institute of Engineering and Technology, El-Behera, Egypt
[5]Department of Electrical Engineering, College of Engineering and IT, Onaizah Colleges, Unayzah, Al-Qassim 56447, Saudi Arabia

Corresponding author: Rania A. Elmanfaloty (relmanfaloty@kau.edu.sa)

**ABSTRACT** Under finite precision implementation, one dimensional (1D) chaotic maps suffer from limited number of control parameters and converged periodicity, making them unsuitable for hardware based ciphering systems despite their simple implementation and low hardware cost. This paper first discusses the limited periodicity of 1D maps under fixed point precision representation, then, presents an image encryption algorithm based on DNA encoding and two specially configured binarized chaotic cores. The function of both cores is to perform the confusion and diffusion stages of the image by generating pseudo random numbers with excellent cryptographic properties. DNA encoding adds an extra layer of security to the algorithm by converting both the image and the chaotic stream to DNA sequences using specific DNA encoding rule. Initial values of both chaotic cores are image dependent based on a calculated hamming distance. These initial condition and the utilized DNA rules composes the overall secret key of the system with a total length of 336 bits. On the condition that all calculations involved in the scheme are based on binary integer arithmetic, all performed security analysis subjected to the scheme proved that the system could withstand known attacks with excellent encryption properties.

**INDEX TERMS** Chaos, DNA computing, DNA encoding, image encryption, cyber security, entropy, NPCR, UACI.

## I. INTRODUCTION

In the current era, reliance on technology has become an essential component in our daily routines [1]. This reliance has led to more handling of sensitive information through communication networks and cloud storage services. Accordingly, Cryptographers became aware of the importance of advancing the security measures to protect these information from unauthorized access and cyber attacks [2]–[5]. Commonly, ciphering data requires an encryption scheme, a communication channel for data transmission, a decryption scheme, and a key to encrypt/decrypt the ciphered data [6] (Fig.1)

Properties of the key, like its secrecy, difficulty to guess and resistance to exhaustive search (brute force attack) are the major factors in characterizing the strength of an encryption system. Shannon [7] defined the features of a key in an "*unbreakable*" scheme to: i) have the same length as the message, ii) to be truly random and iii) to be used only once (also known as one time pad (OTP)). Nevertheless, some of these properties later proved to be disadvantageous as if there exist a secure link to share a key that long, then, it is more logical to transmit the message itself through it. Also, if the same key is used twice, an attacker could gain information about the messages using simple XOR or frequency analysis resulting in a simple running key cipher [8].

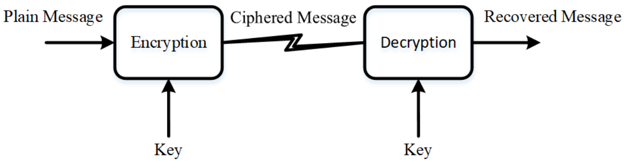


**FIGURE 1.** Fundamental elements of a ciphering system.

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

The impracticality of the OTP opened the door to use stream generators that produce long random sequences using relatively short seeds. These random number generators (RNG) can be classified into true (TRNG) or pseudo (PRNG) [9], the latter in which is deterministic and based on algorithms that produces a sequence with properties mimicking that of true random numbers [10], [11]. Currently, chaos based PRNG are widely used because of their sensitivity to initial conditions, uniformly distributed output and uncorrelated long sequences. Furthermore, discrete chaotic functions are hardware friendly and easy to implement on currently available modules. References [12]–[14].

Interest in the art of cryptography and cryptanalysis [15]–[18] has followed an upward trend in the past few decades, this is mainly due-to the rapid development in electronic technology and the exponential increase in the computational power of modern computers. Nevertheless, when it comes to hardware implementation, factors such as: space utilization, power consumption, high throughput and low latency are of prime importance. As such, the way of representing numbers and performing mathematical operations -especially fraction numbers- significantly affects these factors. Two forms of precision are widely implemented, namely, floating point precision and fixed point precision. From hardware perspective, floating point implementation requires more space on the module, which in turn leads to slow data transfer and high latency. On the other hand, fixed point precision has the advantage of integer like arithmetic which is considered to be hardware friendly.

This paper tackles the two main issues of utilizing low dimensional maps in cryptosystems, namely, i) convergence to periodic orbit due-to finite precision, and ii) limited number of control parameters [19]–[25]. Accordingly, a novel image encryption schemes based on a binarized chaotic cores is presented. Both issues are tackled by implementing a chaotic core comprised of two cross-coupled skew-tent maps as reported in [26]. it was proved that utilizing the cross coupled scheme ensures increasing the aperiodicity of the output stream while increasing the control factors of the generator to four parameters.

This paper is organized as follows: In section II related work and novel curves correlating periodicity to precision length are introduced. The proposed algorithm including the underlying chaotic cores, DNA computing and the encryption scheme is presented in section III. By passing all statistical and security analysis listed in section IV, the proposed algorithm proved to be robust and with excellent confusion-discussion properties.

## II. RELATED WORK

The random like behavior of chaotic systems alongside their deterministic properties made them one of the major source of RRN in most of the recently proposed ciphering schemes [27]–[29]. However, regenerating the same sequence in both ends of the channel requires identical mathematical representation or hardware implementation of these chaotic cores. Recent detailed studies [26], [30], [31] revealed the effect of finite precision on the periodic properties of certain 1D chaotic systems. Elmanfaloty and Abou-Bakr [26] presented -within the hardware perspective- the efficiency of fixed point representation in terms of hardware resources and latency.

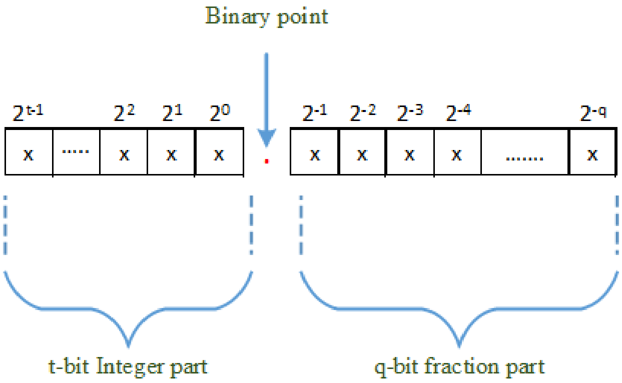


**FIGURE 2. Fixed point representation of binary numbers.**

### A. BINARIZATION OF 1D CHAOTIC MAPS

Binarization of 1D chaotic maps is the process of performing all arithmetic operations under the base-2 representation. These operations includes binary addition, subtraction, multiplication, and division. From hardware perspective, subtraction, multiplication and division are implemented using combination of addition, shifting and negation. This section of the paper briefly revisits the effect of implementing some of the 1D chaotic maps, namely; the logistic map, the tent map and the skew-tent map using fixed point representation. As shown in Fig.2, binary numbers can be represented as $t-bit$ integer part, and $q-bit$ fraction part. To test the effect of $q$ bits length on the periodicity of the output sequence, throughout this work, all mathematical operations of these maps are performed with $t = 4$ bits and $q$ with variable size. For the sake of speeding up the testing while extracting results mimicking hardware implementation, all previously mentioned binary operations were implemented on PC and Matlab. Results of multiplication and division follows the truncation rule mentioned in [26].

#### 1) LYAPUNOV EXPONENT

A chaotic system is mostly characterized by its sensitivity to initial condition, topological transitivity and dense periodic orbits. One common method for determining the sensitivity to initial condition is to calculate the Lyapunov exponent (LE) of the system and check for convergence or divergence between two slightly perturbed trajectories as follows:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \frac{|\delta_1|}{|\delta_o|} \tag{1}$$

where, $\lambda$ denote the LE, $\delta_1$ and $\delta_2$ are the spacing between the two trajectories. If all other conditions implied, $\lambda > 0$ normally indicate chaos [32].

**TABLE 1. Parameters used to generate the graphs in Fig.4.**

| Map | Parameters | |
|---|---|---|
| *Logistic map* | $r = 4$ | $x_o = 0.25$ |
| *Tent map* | $\mu = 2$ | $x_o = 0.25$ |
| *Skew-tent map* | $p = 0.4$ | $x_o = 0.25$ |

### 2) LOGISTIC MAP, TENT MAP AND SKEW-TENT MAP

The logistic map is the typical example of a simple discrete equation that possesses unique chaotic properties. The map was first introduced by the biologist Robert May in 1976 [33]. it is a second-degree equation given by:

$$x_{n+1} = rx_n(1 - x_n) \tag{2}$$

Figure.3 depict the bifurcation diagram of the logistic map along with its LE curve. It is obvious that the map exhibits full chaos and $LE > 0$ in the overall state space at $r = 4$. If the map in (2) is binarized and implemented using fixed point notation, same visual results could be obtained for both the bifurcation diagram and LE. However, when implementing the logistic map using q = {4, 8, 16, 32} bits and the parameters listed in Table.1, inaccurate results of LE and limited periodicity in the bifurcation diagram are illustrated as in Fig.4. It should be noted that LE alone is not an indication to chaos, it is merely an indication to the sensitivity of the system to initial conditions. However, for a topologically mixed system, LE is the common test for checking the chaotic behavior of the system. On the other hand, the periodicity of the system strongly depends on the underlying finite precision. This is clearly depicted in Fig.5, where the periodicity of the logistic map (2), tent map (3)and skew-tent map (4) are plotted against $q$, the fraction part bit length. It is obvious from the figure that the periodicity increases with the increase of $q$, however, these sequences were proved to be have low cryptographic properties and unsuitable for usage in secure ciphering systems [30]. Table.1 lists the parameters used to generate the graphs in Fig.4.

$$x_{n+1} = \begin{cases} \mu x_n & x \in \mathbb{R} : x \in [0, 0.5] \\ \mu(1 - x_n) & x \in \mathbb{R} : x \in (0.5, 1] \end{cases} \tag{3}$$

$$x_{n+1} = \begin{cases} \frac{x_n}{p} & x \in \mathbb{R} : x \in (0, p] \\ \frac{1-x_n}{1-p} & x \in \mathbb{R} : x \in (p, 1) \end{cases} \tag{4}$$

where $p \in (0, 1)$.

## B. DNA COMPUTING

Confusion and dissuasion of the image pixels are the common features that must exist in any robust image encryption algorithm. To satisfy these features, the proposed algorithm relies on DNA encoding along with two chaotic systems cores to generate a ciphered image capable of withstanding known attacks.

Leonard Adleman initiated this field in 1994 by solving a seven-point Hamiltonian path problem using DNA sequences as a form of computation machine [34]. Since then, DNA computing has proved advantageous to the traditional methods given its large storage capacity, parallel processing capabilities and low power consumption. Biologically speaking, Deoxyribonucleic acid (DNA) consists of two helical strands called polynucleotides, in which each is composed of a simpler monomeric units called nucleotides [35]. The constructions of any one of these nucleotides are one of four nitrogen containing nucleobases, namely; "C" cytosine, "G" guanine, "A" adenine and "T" thymine. These nucleotides are characterized by their complementary pairing, i.e. "A" is the complement of "T", "C" is the complement of "G" and vice versa. DNA computing relies on representing each nucleotides by two bits while adhering to the complementary rule. For example, if "A = 00" then "T = 11", if "C = 10" then "G = 01". According to this, there are only 8 out of 24 DNA rules that satisfy this complementary pairing as represented in Table.2.

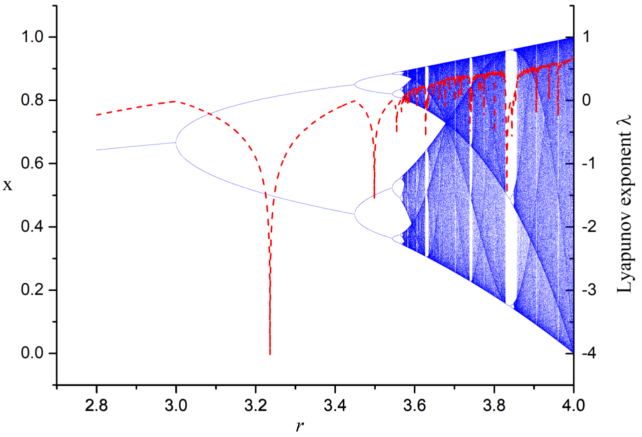
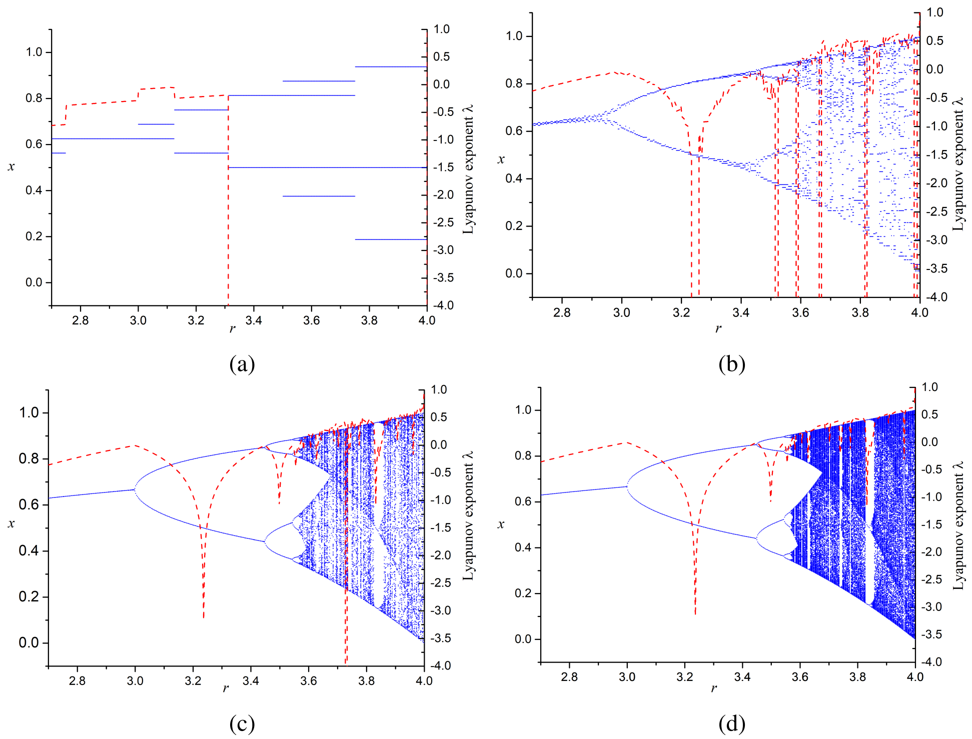


**FIGURE 3.** Bifurcation diagram (blue) and LE (dashed red) for different values of *r* in the logistic map.

**TABLE 2. DNA encoding rules.**

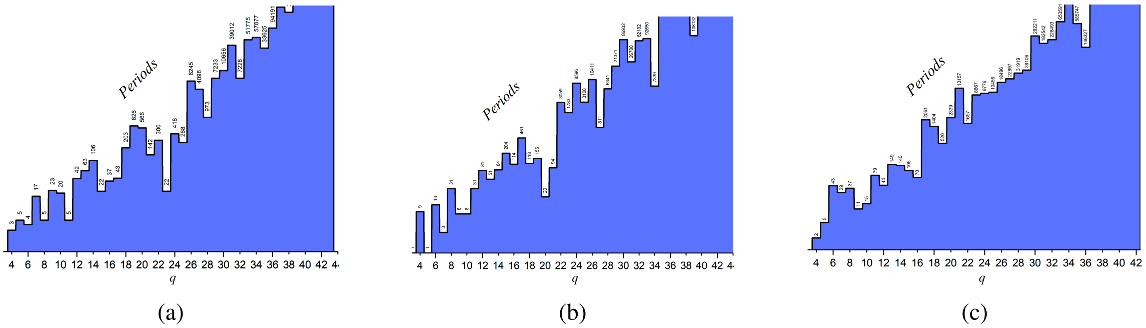
| | *Binary sequence* | | | |
|---|---|---|---|---|
| *Rule* | 00 | 01 | 10 | 11 |
| 1 | A | G | C | T |
| 2 | A | C | G | T |
| 3 | G | A | T | C |
| 4 | G | T | A | C |
| 5 | C | A | T | G |
| 6 | C | T | A | G |
| 7 | T | G | C | T |
| 8 | T | C | G | T |

Using DNA computing requires subjecting the sequence to some logical and algebraic equations, Table.3 list some of these operation for DNA sequences under the first rule. As such, the rest of the 8 rules have also their own unique tables for logical and algebraic operations. Since each pixel in an image is represented by 8 bits, then, each pixel can be transformed to a 4-character DNA sequence according to any one of the DNA encoding rules. For example, under the



(a) (b) (c) (d)

**FIGURE 4.** Effect of fixed point precision (binary fraction) on the bifurcation diagram and LE of the logistic map, (a) 4-bit fraction, (b) 8-bit fraction, (c) 16-bit fraction and (d) 32-bit fraction.



(a) (b) (c)

**FIGURE 5.** Effect of precision on the periodicity of some 1D maps, (a) Logistic map, (b) tent map and (c) skew-tent map.

first rule, a pixel with a value of 224 ('11110100b') would be encoded to "TTCA" in DNA form.

### C. HAMMING DISTANCE

In general, hamming distance finds the number of positions of different symbols in two equally length strings. This paper utilizes this property to calculate bit wise position differences in equally sized blocks of the image by using the following equation:

$$\begin{cases} H(x,y) = \sum_{1}^{n} h(x_i, y_i) \\ h(x_i, y_i) = \begin{cases} 0, & x_i = y_i \\ 1, & x_i \neq y_i \end{cases} \end{cases} \tag{5}$$

Throughout the encryption process, the hamming distance is used in both the confusion and diffusion stages by altering the initial values and parameters of the two chaotic systems making them dependent on the plain image.

## III. PROPOSED ALGORITHM

The proposed algorithm depicted in Fig.6 consists of two chaotic cores, one for pixels confusion and the other for the permutation process. Each core is implemented using chaotic systems previously proposed in [26] as shown in Fig.7. The PRNG consists of two crossed coupled skew tent maps that are fully binarized and relies on fixed point representation in all of its logical and algebraic processes. The output is a stream of n-bit that was subjected to various statistical tests and proved its randomness and cryptographic properties. In this paper, the output of the system is intentionally designed to produce a stream of 8-bits, this makes it suitable for direct implementation in image encryption schemes.

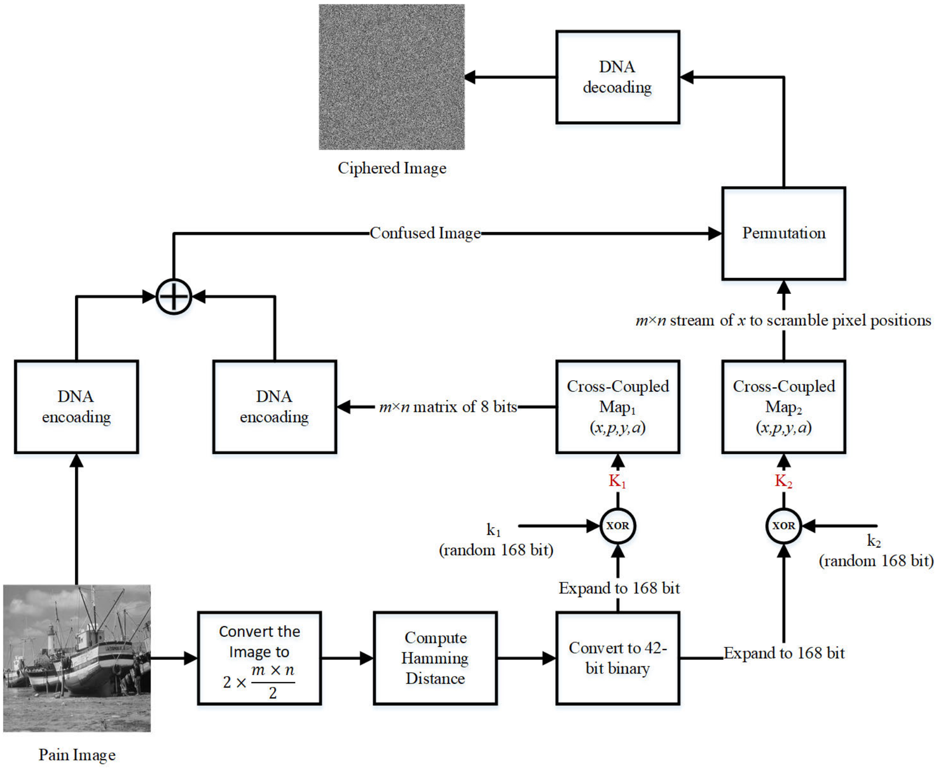


**FIGURE 6.** Block diagram of the proposed algorithm.

**TABLE 3.** DNA operations.

| XOR | A | G | C | T |
|---|---|---|---|---|
| A | A | G | C | T |
| G | G | A | T | C |
| C | C | A | T | G |
| T | T | C | G | A |
| + | A | G | C | T |
| A | A | G | C | T |
| G | G | C | T | A |
| C | C | T | A | G |
| T | T | A | G | C |
| - | A | G | C | T |
| A | A | T | C | G |
| G | G | A | A | C |
| C | C | G | T | T |
| T | T | C | G | A |

## A. KEY STRUCTURE

Each core requires four initial parameter to operate, namely, $\{p, x_o\}$ for the first skew-tent map and $\{a, y_o\}$ for the second. For each map, these parameters are represented by binary sequence of 168 bits and forms the main secret keys $\{K_1, K_2\}$. Moreover, to make these keys dependent on the plain image in the encryption side, the hamming distance is calculated for the plain image and converted to 168 bit stream. Another layer of security is also added to $\{K_1, K_2\}$ stream by XORing the 168 bit calculated hamming distance with another secret keys $\{k_1, k_2\}$. the overall length of the transmitted secret key comprising from $\{K_1, K_2\}$ will be 336 bits.

## B. ENCRYPTION PROCEDURE

The following procedures are followed through the encryption process:

*First:* the Confusion stage

1) Read plain image.
2) Calculate the hamming distance.
3) Convert the calculated hamming distance to 168-bit.
4) XOR the 168-bit hamming code with a secret Sub-key $k_1$ and generate $K_1$ for the first chaotic core.
5) Run the first Chaotic core to generate an $m \times n$ matrix of 8-bits.
6) Encode the plain image with a DNA encoding rule.
7) Encode the matrix of first chaotic System with the same DNA encoding rule.
8) Perform a DNA algebraic operation (Addition).

*Second:* the permutation stage

9) Use the Hamming code with a secret sub-key $k_2$ to generate $K_1$ of 168 bits.
10) Use $K_1$ to extract an $m \times n$ long sequence from one of the generator state variable $x$ or $y$.
11) Permute the output result of stage (7) using the extracted sequence.
12) Perform a DNA decoding using the selected DNA-rule.

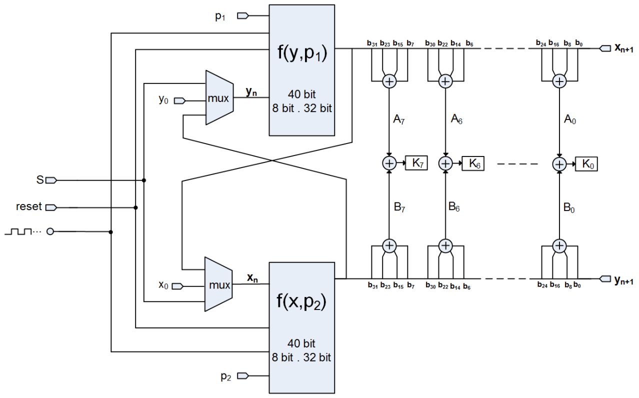


**FIGURE 7.** PRNG proposed in [26].

The choice for using two cores is made to eliminate any correlation between the sequences for both the confusion and diffusion stages. the decryption process is the inverse of the encryption process.

## IV. SECURITY ANALYSIS

### A. HISTOGRAM ANALYSIS

Uniformly distributed histogram for ciphered image - even for images containing weak color intensity distribution- is an indication of the capability of the encryption scheme to resist statistical attacks. The histogram of three images (boat, white, black) and their ciphered images are shown in Fig.8. For the original images, unique histograms are displayed, while those of the ciphered results exhibit a uniform distribution. This again proves the proposed system capability to withstand statistical attacks.

### B. CORRELATION ANALYSIS

A ciphered image is most vulnerable to statistical attacks when there are high correlation in the vertical(V), horizontal(H) and diagonal(D) direction of its adjacent pixels. If the encryption scheme can severely diminish this correlation, then this system is most likely to resist statistical attacks. Calculation can be performed by computing a coefficient $r_{xy}$ using random pairs of adjacent pixels and substituting the values in the following equations:

$$D(x) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \tag{6}$$

$$D(y) = \frac{1}{S}\sum_{i=1}^{S}(y_i - E(y))^2 \tag{7}$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S} x_i \tag{8}$$

$$E(y) = \frac{1}{S}\sum_{i=1}^{S} y_i \tag{9}$$

$$cov(x, y) = \frac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)) \tag{10}$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{11}$$

The result of subjecting a plain grayscale image (512) and its ciphered one to the correlation analysis is depicted in Fig.9 (4000 pixels). For the original image, strong and compact correlation between pixels in all direction is visibly clear. However, for the ciphered output, scattered and no visible compact correlation is shown. Table.4 lists the results of performing the correlation analysis test on several images with different sizes. All the results for the encrypted images show weak correlation and robustness against statistical attacks.

### C. ENTROPY ANALYSIS

Shannon, in 1949, [7] started the field of information theory by measuring the "*uncertainty*" reduced by the message. Subsequently, in any robust encryption algorithm, using "*entropy*" to quantify the amount of information contained in a variable means that; the less information successfully retrieved from the ciphered text, the more secure the algorithm is to entropy attacks. For Image Encryption, Shannon equation for information entropy is as follows:

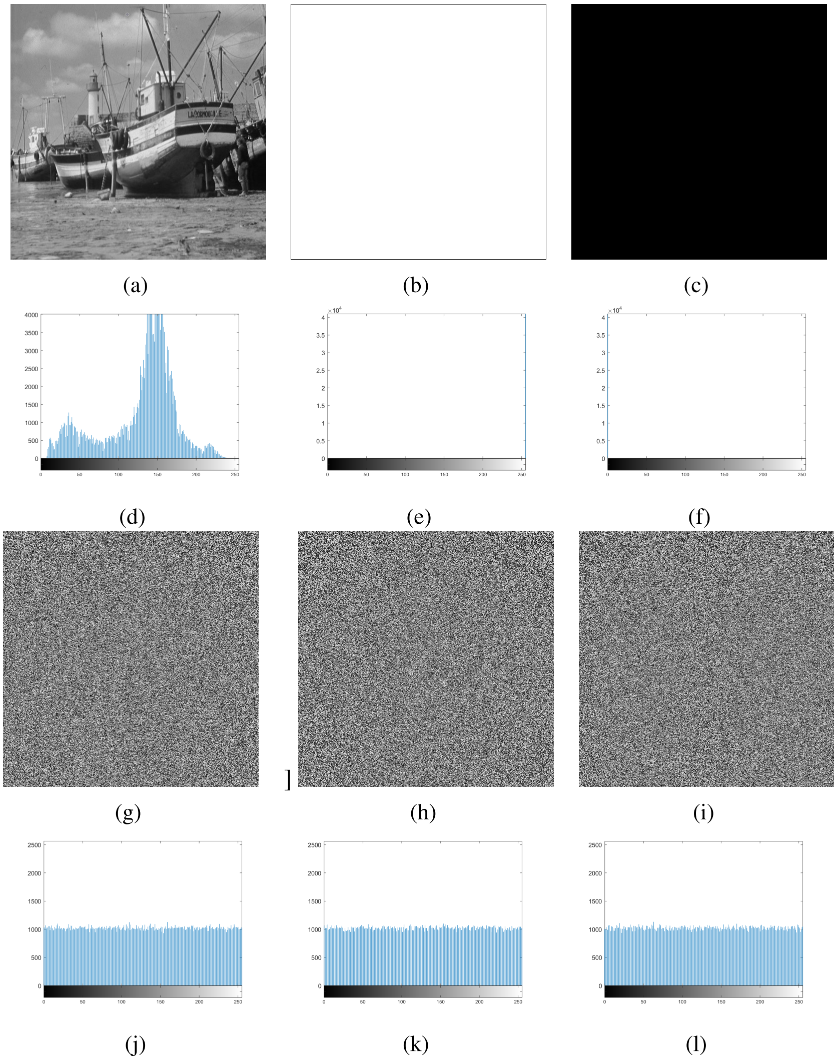
$$H(m) = -\sum_{i=1}^{2^n} P(m_i)log_2\,(P(m_i)) \tag{12}$$

In the above equation, $m_i$ represents one of the 256 grayscale levels from 0 to 255 (or even one of the color intensities levels in colored images), $n$ is the number of bits representing each pixel color intensity, and $P(m_i)$ is the probability of a color intensity $m_i$ in the image. The equation will result in a maximum of 8 for an evenly distributed color intensity in the image. However, this number can only be attained for an ideal system, and results close to 8 could be accepted as an indication of difficulty to extract information. In addition, and relating to subsection.IV-A, it is clear that both histograms (visual) and entropy (mathematical) can be used to quantify the amount of information that can be extracted from the ciphered image. In Table.5, "27" ciphered images with different gray level distribution were subjected to the entropy test. All results listed "*globally*" confirms the uniform distribution of gray levels and the algorithm ability to withstand entropy attacks.

Shannon entropy, also called *global* Shannon entropy -since it acts on the whole image- proved to have many weaknesses [40]; namely, its inaccuracy in detecting the true randomness of an image, its inconsistency since the probability of the grayscale level depends on the size of the image, and its variable performance efficiency depending on the images size. The local Shannon (LSE) entropy [40] overcame these downsides by measuring the mean entropy of same sized non-overlapping blocks from the whole image by:

$$H_{k,T_B}(I) = \sum_{i=1}^{k}\frac{H(I_{B_i})}{k} \tag{13}$$

where, $H(I_{B_i})$ is the local Shannon entropy, $k$ is the number of same sized blocks and $T_B$ is the number of pixels in


(a) (b) (c)

(d) (e) (f)

]

(g) (h) (i)

(j) (k) (l)

**FIGURE 8.** **Histogram analysis of different images with different intensity levels, (a), (b) and (c) are the original image, (d), (e) and (f) are their histogram, (g), (h) and (i) are the encryption of encryption of (a), (b) and (c) respectively, (j), (k) and (l) are their histogram.**

**TABLE 4.** **Vertical (V), horizontal (H) and diagonal (D) correlation of grayscale images and their ciphered ones (original images source, [36]).**

| | | | *Original image* | | | *Ciphered image* | |
|---|---|---|---|---|---|---|---|
| *File name* | *Size* | *V-correlation* | *H-correlation* | *D-correlation* | *V-correlation* | *H-correlation* | *D-correlation* |
| 5.1.09 | 256x256 | 0.9373 | 0.9064 | 0.9012 | -0.0225 | 0.0382 | -0.0050 |
| 5.1.11 | 256x256 | 0.9447 | 0.9557 | 0.9045 | -0.0118 | -0.0673 | 0.0049 |
| 5.1.12 | 256x256 | 0.9763 | 0.9575 | 0.9345 | -0.0072 | -0.0018 | -0.0065 |
| 5.1.13 | 256x256 | 0.8677 | 0.8585 | 0.7554 | -0.0111 | -0.0318 | 0.0185 |
| 1.1.01 | 512x512 | 0.8062 | 0.7344 | 0.5799 | 0.0095 | -0.0405 | -0.0183 |
| 5.2.09 | 512x512 | 0.8559 | 0.8858 | 0.8092 | -0.0084 | -0.0037 | 0.0208 |
| boat.512 | 512x512 | 0.9681 | 0.9388 | 0.9234 | -0.0270 | -0.0031 | 0.0085 |
| cameraman | 512x512 | 0.9903 | 0.9783 | 0.9723 | -0.0350 | -0.0126 | -0.0055 |
| gray21.512 | 512x512 | 0.9996 | 0.9921 | 0.9983 | 0.0097 | -0.0495 | -0.0045 |
| ruler.512 | 512x512 | 0.4465 | 0.3874 | -0.0484 | 0.0000 | 0.0047 | 0.0005 |
| white | 512x512 | NaN | NaN | NaN | -0.0050 | -0.0556 | -0.0125 |
| black | 512x512 | NaN | NaN | NaN | -0.0149 | -0.0660 | 0.0021 |
| 1.4.07 | 1024x1024 | 0.9484 | 0.9655 | 0.9468 | 0.0200 | 0.0698 | -0.0009 |
| 5.3.01 | 1024x1024 | 0.9828 | 0.9765 | 0.9689 | 0.0304 | 0.0005 | 0.0109 |
| 5.3.02 | 1024x1024 | 0.8970 | 0.8929 | 0.8483 | -0.0126 | 0.0191 | -0.0170 |

each block. Derived hypothesis $\langle^*_{Left}$ and $\langle^*_{Righ}$ are used to convert the quantitative results of the LSE into qualitative ones, namely, reject or fail to reject the randomness of an image. Since the measurement is dependent on the number of blocks and their sizes rather than the whole image size, constant values of $\langle^*_{Left}$ and $\langle^*_{Righ}$ can be derived accordingly.

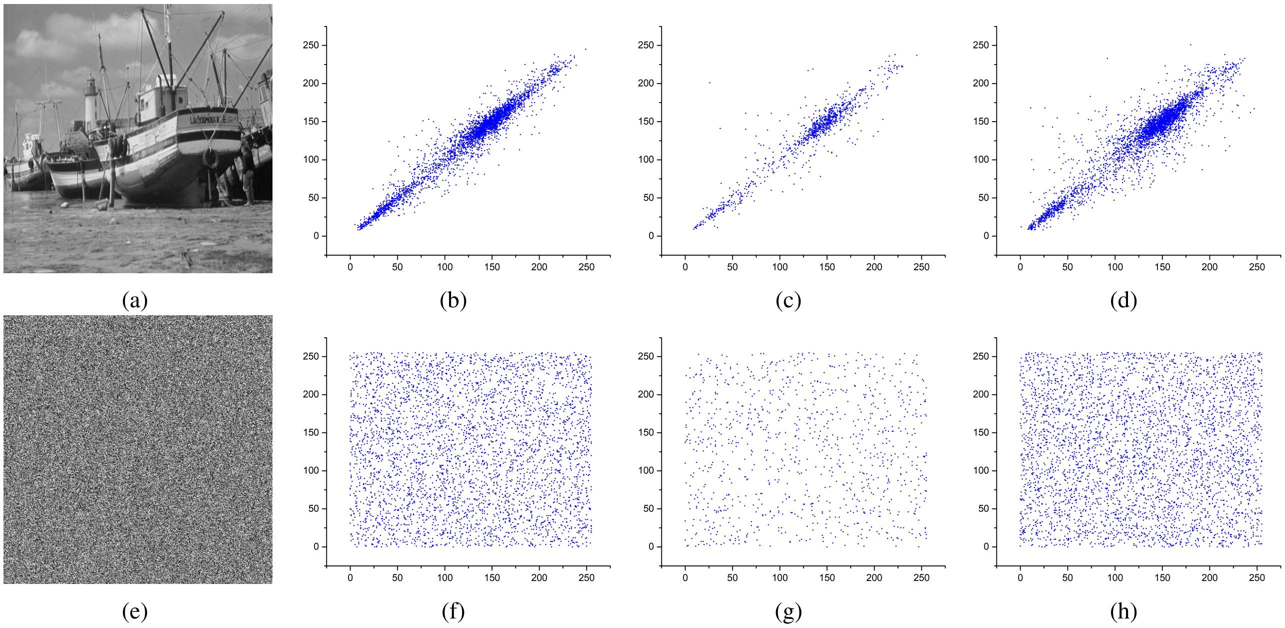


**FIGURE 9.** Correlation analysis of 4000 adjacent pixels, a) original Image, b) V correlation, c) H correlation, d) D correlation, e) ciphered image, f) V correlation, g) H correlation, h) D correlation.

**TABLE 5.** Entropy analysis of sample grayscale images.

| | *Global entropy* | | *LSE* | | | |
|---|---|---|---|---|---|---|
| *File name* | *Original* | *ciphered* | *Proposed Scheme* | Ref.[37] | Ref.[38] | Ref.[39] |
| *Dimention* 256×256 | | | | | | |
| 5.1.09.tiff | 6.709312 | 7.997255 | 7.902246 | 7.903154 | 7.90271 | 7.902475 |
| 5.1.10.tiff | 7.311807 | 7.997796 | 7.90202 | 7.90168 | 7.902473 | 7.9016 |
| 5.1.11.tiff | 6.452275 | 7.997657 | 7.902121 | 7.902725 | 7.902217 | 7.903487 |
| 5.1.12.tiff | 6.705667 | 7.997406 | 7.902232 | 7.901605 | 7.903208 | 7.902023 |
| 5.1.13.tiff | 1.548314 | 7.997307 | 7.902156 | 7.901269 | 7.902951 | 7.901894 |
| 5.1.14.tiff | 7.342433 | 7.996835 | 7.90292 | 7.902341 | 7.901577 | 7.901528 |
| *Dimention* 512×512 | | | | | | |
| 5.2.08.tiff | 7.201008 | 7.999246 | 7.902442 | 7.902038 | 7.902681 | 7.902988 |
| 5.2.09.tiff | 6.993994 | 7.999298 | 7.902606 | 7.902722 | 7.902571 | 7.902867 |
| 5.2.10.tiff | 5.70556 | 7.999378 | 7.903019 | 7.902478 | 7.902411 | 7.903095 |
| 7.1.01.tiff | 6.027415 | 7.999313 | 7.902794 | 7.902012 | 7.9019 | 7.903033 |
| 7.1.02.tiff | 4.004499 | 7.999267 | 7.903024 | 7.902484 | 7.903003 | 7.903289 |
| 7.1.03.tiff | 5.49574 | 7.999362 | 7.902937 | 7.902833 | 7.902116 | 7.902783 |
| 7.1.04.tiff | 6.107418 | 7.999314 | 7.902188 | 7.902047 | 7.902998 | 7.902107 |
| 7.1.05.tiff | 6.563196 | 7.99926 | 7.903004 | 7.902568 | 7.903154 | 7.902479 |
| 7.1.06.tiff | 6.695283 | 7.999146 | 7.902468 | 7.902022 | 7.902009 | 7.902303 |
| 7.1.07.tiff | 5.991599 | 7.99927 | 7.90258 | 7.902398 | 7.903176 | 7.902556 |
| 7.1.08.tiff | 5.053448 | 7.999353 | 7.902675 | 7.902137 | 7.902837 | 7.902488 |
| 7.1.09.tiff | 6.189814 | 7.999163 | 7.902089 | 7.902142 | 7.902068 | 7.90175 |
| 7.1.10.tiff | 5.90879 | 7.999338 | 7.902602 | 7.902171 | 7.903141 | 7.902402 |
| Black.tiff | 0 | 7.999351 | 7.902918 | - | - | - |
| White.tiff | 0 | 7.999301 | 7.902285 | - | - | - |
| boat.512.tiff | 7.19137 | 7.999298 | 7.902659 | 7.902046 | 7.90192 | 7.903294 |
| gray21.512.tiff | 4.392295 | 7.999223 | 7.902273 | 7.902718 | 7.903359 | 7.90204 |
| ruler.512.tiff | 0.500033 | 7.999207 | 7.90211 | 7.902004 | 7.901889 | 7.902625 |
| *Dimention* 1024×1024 | | | | | | |
| 5.3.01.tiff | 7.523737 | 7.999816 | 7.902475 | 7.902057 | 7.903408 | 7.903095 |
| 5.3.02.tiff | 6.83033 | 7.999831 | 7.90204 | 7.902396 | 7.903093 | 7.902575 |
| 7.2.01.tiff | 5.641454 | 7.999827 | 7.902127 | 7.90233 | 7.902316 | 7.902714 |

In this paper, the number of blocks $k$ was selected to be 30, the significance level $\alpha = 0.05$ and the number of pixels in each block $T_B = 1936$. According to these parameters, The appropriate values for both hypothesis listed in [40] are

**TABLE 6.** MSE and PNSR values of the ciphered images with slightly change in the key.

| | *MSE* | | *PSNR* | |
|---|---|---|---|---|
| *File name* | *Change in $K_1$* | *Change in $K_2$* | *Change in $K_1$* | *Change in $K_2$* |
| Boat.512.tiff | $10.927\times10^3$ | $10.914\times10^3$ | 7.746 | 7.751 |
| Black.tiff | $10.961\times10^3$ | $10.850\times10^3$ | 7.732 | 7.776 |
| White.tiff | $10.934\times10^3$ | $10.909\times10^3$ | 7.743 | 7.753 |

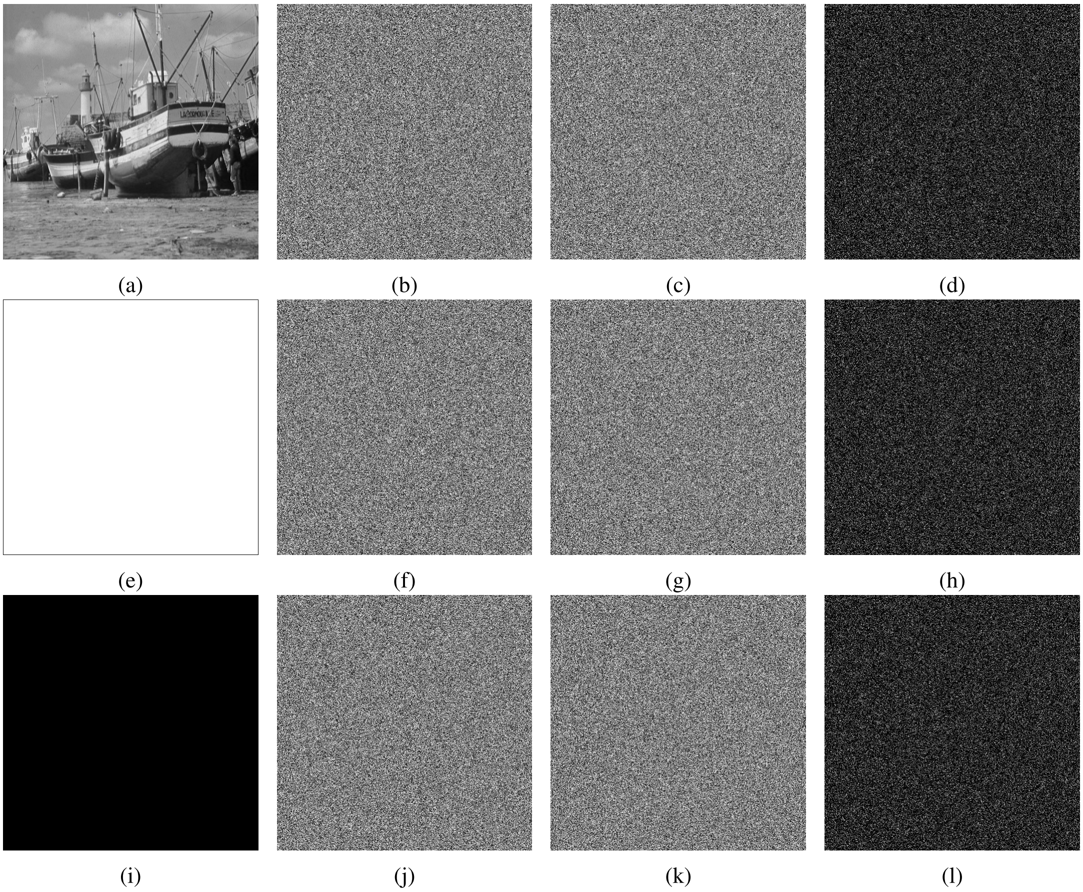


**FIGURE 10.** Key sensitivity analysis of the proposed Algorithm., (a), (e), (i) are the original images, (b), (f), (j) are the encrypted images, (c), (g), (k) are the encrypted images by flipping the LSb of $K_1$, (d) is the absolute difference between (c) and (b), (h) is the absolute difference between (g) and (f), (l) is the absolute difference between (k) and (j).

$h^*_{Left} = 7.901901305$ and $h^*_{Righ} = 7.903037329$. Complete list of calculated LSE for 27 grayscale images are listed in Table. 5 along with a comparison to results of other algorithms. All displayed results fall within the critical values, for different image sizes. This further confirms the ability of the system to withstand entropy attacks.

## D. KEY ANALYSIS

### 1) KEY-SPACE ANALYSIS

A large keyspace is crucial for a robust ciphering scheme to resist brute force attacks. In the proposed scheme, $K_1$ and $K_2$ for the confusion and diffusion stages requires the input of four parameters each, namely: $x_o, p, y_o, a$. Although the system design is capable of varying the fixed-point precision (binary point) size, a 42 bit binary point size was selected for the sake of simulation based on the data previously deducted in [26].

### 2) KEY SENSITIVITY ANALYSIS

Sensitivity of the system to key change is achieved by producing two different encrypted - or decrypted- images with two slightly different keys. For the proposed algorithm, a main key consisting of $\{K_1, K_2\}$ was used to encrypt an image $I$, and produce an output ciphered image $C$. Then, the same image was encrypted again twice to produce $C_1$ and $C_2$ with slightly different keys. For maximum sensitivity test, $C_1$ was produced by flipping the least significant bit (LSb) of $K_1$. While for $C_2$, the LSb of $K_2$ was flipped. The results are illustrated in In Fig.10, where three images underwent this test; a grayscale image in Figure.10a, a white and a black images in Figures (10e and 10i). The encrypted images are shown in Figures (10b, 10f, 10j, 10c, 10g and 10k). A pixel by pixel subtraction between $C_1$ and $C$ was performed and the results are shown in Figures (10d, 10h and 10l). The noisy like output displayed is a proof of the mismatch between

**TABLE 7.** NPCR and UACI score results for 26 images with different sizes.

| | | *NPCR test result* | | | | *UACI test result* | | |
|---|---|---|---|---|---|---|---|---|
| *File name* | *Score%* | *Status* | Ref.[37] | Ref.[39] | *Score %* | *Status* | Ref.[39] | Ref.[? ] |
| *Dimention* 256×256 | | $\mathcal{N}^*_\alpha \geq 99.5693\%$ | | | | $\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha = (33.2824\%, 33.6447\%)$ | | |
| 5.1.09 | 99.588 | pass | 99.6093 | 99.5956 | 33.5688 | pass | 33.4723 | 33.45034 |
| 5.1.10 | 99.6689 | pass | 99.6095 | 99.6018 | 33.5222 | pass | 33.4663 | 33.43234 |
| 5.1.11 | 99.5743 | pass | 99.6133 | 99.6079 | 33.4894 | pass | 33.4554 | 33.41204 |
| 5.1.12 | 99.6277 | pass | 99.6123 | 99.6063 | 33.4975 | pass | 33.4604 | 33.46242 |
| 5.1.13 | 99.5712 | pass | 99.605 | 99.6155 | 33.5465 | pass | 33.4601 | 33.49739 |
| 5.1.14 | 99.5697 | pass | 99.611 | 99.6124 | 33.5711 | pass | 33.4606 | 33.46588 |
| *Dimention* 512×512 | | $\mathcal{N}^*_\alpha \geq 99.5893\%$ | | | | $\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha = (33.3730\%, 33.5541\%)$ | | |
| 5.2.08 | 99.5998 | pass | 99.607 | 99.6021 | 33.5446 | pass | 33.4734 | 33.46463 |
| 5.2.09 | 99.6086 | pass | 99.6106 | 99.6082 | 33.4976 | pass | 33.4572 | 33.48115 |
| 5.2.10 | 99.6048 | pass | 99.6096 | 99.6269 | 33.3785 | pass | 33.4575 | 33.4547 |
| 7.1.01 | 99.5934 | pass | 99.6095 | 99.6017 | 33.4887 | pass | 33.4726 | 33.47657 |
| 7.1.02 | 99.6094 | pass | 99.6117 | 99.6128 | 33.5073 | pass | 33.4563 | 33.45195 |
| 7.1.03 | 99.6025 | pass | 99.6123 | 99.5968 | 33.4612 | pass | 33.4535 | 33.41221 |
| 7.1.04 | 99.6189 | pass | 99.6114 | 99.6098 | 33.5243 | pass | 33.4475 | 33.49961 |
| 7.1.05 | 99.6094 | pass | 99.6099 | 99.6021 | 33.4804 | pass | 33.4559 | 33.40539 |
| 7.1.06 | 99.6105 | pass | 99.6064 | 99.6014 | 33.4292 | pass | 33.4515 | 33.51457 |
| 7.1.07 | 99.6078 | pass | 99.6068 | 99.6136 | 33.4592 | pass | 33.4638 | 33.52977 |
| 7.1.08 | 99.6052 | pass | 99.6097 | 99.6089 | 33.4667 | pass | 33.4536 | 33.51067 |
| 7.1.09 | 99.604 | pass | 99.6112 | 99.6079 | 33.4781 | pass | 33.4729 | 33.43775 |
| 7.1.10 | 99.5983 | pass | 99.6096 | 99.6037 | 33.4367 | pass | 33.4605 | 33.49378 |
| Black | 99.6189 | pass | - | - | 33.5084 | pass | - | - |
| White | 99.6101 | pass | - | - | 33.4178 | pass | - | - |
| boat.512 | 99.6365 | pass | 99.6084 | 99.5991 | 33.4683 | pass | 33.4434 | 33.4869 |
| gray21.512 | 99.6178 | pass | 99.6074 | 99.6124 | 33.545 | pass | 33.4588 | 33.51263 |
| ruler.512 | 99.6231 | pass | 99.6092 | 99.6185 | 33.4407 | pass | 33.4637 | 33.45417 |
| *Dimention* 1024×104 | | $\mathcal{N}^*_\alpha \geq 99.5994\%$ | | | | $\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha = (33.4183\%, 33.5088\%)$ | | |
| 5.3.01 | 99.6063 | pass | 99.6095 | 99.6094 | 33.4725 | pass | 33.4511 | 33.42413 |
| 5.3.02 | 99.602 | pass | 99.6095 | 99.6064 | 33.4983 | pass | 33.4536 | 33.4987 |
| 7.2.01 | 99.6073 | pass | 99.6096 | 99.608 | 33.4723 | pass | 33.4606 | 33.43706 |

the two ciphered images which relates to the robustness of the proposed system for the diffusion and confusion process. Same results were obtained when conducting the same test on the decryption process.

To further empathize on the results obtained, the mean square error (MSE) and peak signal to noise (PSNR) between $C$ and both $C_1$ and $C_2$ were conducted according to:

$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[E_1(i,j) - E_2(i,j)]^2}{M \times N} \tag{14}$$

$$PSNR = 20log_{10}\frac{255}{\sqrt{MSE}} \tag{15}$$

The listed results in Table.6 confirms the sensitivity of the proposed scheme to any small change in the *key*.

## E. RESISTANCE TO DIFFERENTIAL ATTACK

To resist differential attacks, the system should be sensitive to any errors in the plain image, that is; while using the same key, any small change in the plain image, should produce a completely different ciphered image with good discussion properties. The most standard methods for measuring the system sensitivity to this type of errors are the number of pixels' change rate (NPCR) and unified average changing intensity (UACI).

*NPCR* is the rate of change of pixel locations from the plain image to the ciphered image, the closer the result of NPCR result to "*unity*", the higher the system ability to resist differential attacks. Using the same key, the NPCR of a plain image $I$ and slightly altered image $I'$ with their ciphered image $C$ and $C'$ can be calculated using:

$$\begin{cases} NPCR(C, C') = \sum_{i,j} \frac{D(i,j)}{T} \\ D(i,j) = \begin{cases} 0 & when \;\; C(i,j) = C'(i,j) \\ 1 & when \;\; C(i,j) \neq C'(i,j) \end{cases} \end{cases} \tag{16}$$

where $T$ is the number of pixels. Since a "*unity*" $NPCR = 1$ is difficult to attain, values very close to could be accepted

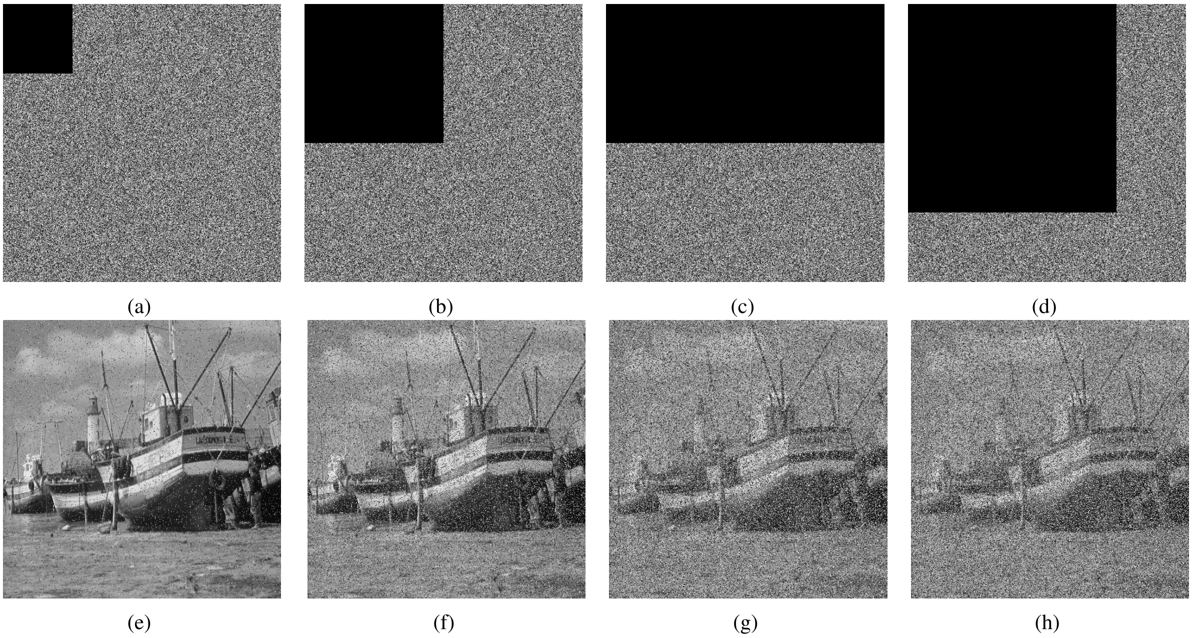


**FIGURE 11.** **Results of analyzing occlusion attack. (a) 1/8 occlusion, (e) decryption result, (b) 1/4 occlusion, (f) decryption result, (c) 1/2 occlusion, (g) decryption result, (d) 3/4 occlusion, (h) decryption result.**

under the criterion of one-sided hypotheses $\mathcal{N}$ and its significance level $\alpha$, namely, when the value of $NPCR \geq \mathcal{N}$, and $\mathcal{N}$ is given by [41]:

$$\mathcal{N}_{\alpha}^{*} = \frac{L + \Phi^{-1}(\alpha)\sqrt{L/T}}{L+1} \tag{17}$$

In the above equation, $\Phi(.)^{-1}$ is the inverse Cumulative distribution function (CDF) of the standard Normal distribution $\mathbb{N}(0, 1)$.

On the other hand, *UACI* finds the difference in average intensity between two ciphered images $C$ and $C'$ using:

$$UACI(C, C') = \sum_{i,j} \frac{|C(i,j) - C(i,j)|}{T \times L} \tag{18}$$

where $L$ is the maximum level of color intensity. The result of UACI is considered a "*Pass*", if its value falls in between the interval $[\mathcal{U}_{\alpha}^{*-}, \mathcal{U}_{\alpha}^{*+}]$:

$$\begin{cases} \mathcal{U}_{\alpha}^{*-} = \mu_{\mathcal{U}} - \Phi^{-1}(\alpha/2)\sigma_{\mathcal{U}} \\ \mathcal{U}_{\alpha}^{*+} = \mu_{\mathcal{U}} + \Phi^{-1}(\alpha/2)\sigma_{\mathcal{U}} \end{cases} \tag{19}$$

$$\tag{20}$$

$$\mu_{\mathcal{U}} = \frac{L+2}{3L+3} \tag{21}$$

$$\sigma_{\mathcal{U}} = \frac{(L+2)(L^2+2L+3)}{18(L+1)^2 LT} \tag{22}$$

Table.7 list the results of subjecting 27 grayscale images with different sizes and intensities to the NPCR and UACI tests with ($\alpha = 0.05$). All obtained scores passed the tests taking into consideration the criterion for success. These results are valid indication that the proposed system has good confusion and diffusion properties, and can withstand differential attacks.

### *F. OCCLUSION ATTACK*

It is possible that some of the data could be altered while being transmitted. This altering could be due-to an intentional or unintentional intervene. A good ciphering system should be able to recover recognizable image from this type of attack. This test relies on completely occluding a portion of the encrypted image then decrypting it. The system should be able to scatter and scramble this occlusion though the whole image. For visual verification, Fig.11 depict the effect of multiple percentage of data loss in the encrypted image on the decrypted one. All results show fairly recognized decrypted image, specially when 3/4 of the image was blocked. This proves that the proposed scheme posses excellent confusion and diffusion properties and can withstand brute occlusion attacks.

### *G. EXECUTION SPEED*

The work in this paper was conducted and simulated using MATLAB R2020a installed on an *Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz* computer with 16GB of RAM and windows 10 as operating system. To mimic actual hardware implementation, the binary logic and algebraic operations are coded using arrays, that significantly decreased the execution time, especially when generating sequences form the chaotic cores. Hence, a test for the execution speed would be inaccurate for real time implementation. For example, the time required from a core to generate a sequence of 65536 × 8 sequence (which is the size of a 256 × 256 image) is about 120 seconds. This slow execution is mainly because of the continuous conversion of the binary sequences format from character array to double and vice versa. The authors expect that future hardware implementation of this scheme would lead to a fast execution. This assumption is based on the results in [26] showing that this core configuration requires one clock cycle for each output. In addition, both cores can operate simultaneously in parallel processing environment.

## V. CONCLUSION

By thoroughly studying the effect of finite precision on the periodicity of 1D chaotic maps, a robust hardware friendly image encryption schemes can be designed. This paper presents a novel image encryption scheme based on DNA and binarized chaotic cores, that is, implementing these cores under fixed point precision. The scheme was subjected to multiple statistical and security analysis, all of which proved its robustness and ability to withstand known attacks. However, since the system was implemented via MATLAB programming, an  accurate -real time- execution speed analysis could not be applied to the work in this paper.

## REFERENCES

[1] K. Kushlev, J. D. E. Proulx, and E. W. Dunn, "Digitally connected, socially disconnected: The effects of relying on technology rather than other people," *Comput. Hum. Behav.*, vol. 76, pp. 68–74, Nov. 2017.

[2] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 9203–9208, Apr. 2018.

[3] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2018.

[4] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K.-R. Choo, "Artificial intelligence in cyber security: Research advances, challenges, and opportunities," *Artif. Intell. Rev.*, pp. 1–25, Mar. 2021.

[5] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[6] B. Furht and D. Kirovski, *Multimedia Security Handbook*. Boca Raton, FL, USA: CRC Press, 2004.

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

[8] R. N. Wright, "Cryptography," in *Encyclopedia of Physical Science and Technology*, 3rd ed., R. A. Meyers, Ed. New York, NY, USA: Academic, 2003, pp. 61–77.

[9] P. L'Ecuyer, "Good parameters and implementations for combined multiple recursive random number generators," *Oper. Res.*, vol. 47, no. 1, pp. 159–164, Feb. 1999.

[10] P. L'ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure," *Math. Comput.*, vol. 68, no. 225, pp. 249–260, 1999.

[11] P. L'Ecuyer, "Random number generation," in *Handbook of Computational Statistics*. Berlin, Germany: Springer, 2012, pp. 35–71.

[12] M. F. Tolba, W. S. Sayed, A. G. Radwan, and S. K. Abd-El-Hafiz, "FPGA realization of speech encryption based on modified chaotic logistic map," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Feb. 2018, pp. 1412–1417.

[13] O. A. Aboulseoud and S. M. Ismail, "FPGA floating point fractional-order chaotic map image encryption," in *Proc. 31st Int. Conf. Microelectron. (ICM)*, Dec. 2019, pp. 134–137.

[14] H. Li, L. Deng, and Z. Gu, "An image encryption scheme based on precision limited chaotic system," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19387–19410, Jul. 2020.

[15] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107286.

[16] M. Li, D. D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 31–47, 2019.

[17] Y. Liu, Z. Qin, X. Liao, and J. Wu, "Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled sine map," *Nonlinear Dyn.*, vol. 100, no. 3, pp. 2917–2931, May 2020.

[18] M. Li, H. J. 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.

[19] L. Shujun, M. Xuanqin, and C. Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *Proc. Int. Conf. Cryptol. India*. Berlin, Germany: Springer, 2001, pp. 316–329.

[20] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision," *Comput. Phys. Commun.*, vol. 153, no. 1, pp. 52–58, 2003.

[21] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[22] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[23] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 601–613, 2019.

[24] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Deterministic chaotic finite-state automata," *Nonlinear Dyn.*, vol. 98, no. 3, pp. 2403–2421, Nov. 2019.

[25] R. A. Elmanfaloty and E. Abou-Bakr, "An image encryption scheme using a 1D chaotic double section skew tent map," *Complexity*, vol. 2020, pp. 1–18, Oct. 2020.

[26] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons Fractals*, vol. 118, pp. 134–144, Jan. 2019.

[27] R. Guesmi and M. A. B. Farah, "A new efficient medical image cipher based on hybrid chaotic map and DNA code," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 1925–1944, Jan. 2021.

[28] J. Deng, M. Zhou, C. Wang, S. Wang, and C. Xu, "Image segmentation encryption algorithm with chaotic sequence generation participated by cipher and multi-feedback loops," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13821–13840, 2021.

[29] M. Madani and C. Tanougast, "FPGA implementation of an enhanced chaotic-KASUMI block cipher," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103644.

[30] I. Öztürk and R. Kiliç, "Cycle lengths and correlation properties of finite precision chaotic maps," *Int. J. Bifurcation Chaos*, vol. 24, no. 9, 2014, Art. no. 1450107.

[31] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. A. H. Fahmy, "Finite precision logistic map between computational efficiency and accuracy with encryption applications," *Complexity*, vol. 2017, pp. 1–21, Feb. 2017.

[32] T.-Y. Li and J. A. Yorke, "Period three implies chaos," in *The Theory of Chaotic Attractors*. New York, NY, USA: Springer, 2004, pp. 77–84.

[33] R. M. May, "Simple mathematical models with very complicated dynamics," in *The Theory of Chaotic Attractors*. New York, NY, USA: Springer, 2004, pp. 85–93.

[34] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[35] K. Roberts, B. Alberts, A. Johnson, P. Walter, and T. Hunt, *Molecular Biology of the Cell*. New York, NY, USA: Garland Science, 2002.

[36] University of Southern California. *The USC-SIPI Image Database*. Accessed: Oct. 2021. [Online]. Available: http://sipi.usc.edu/database/

[37] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[38] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2D infinite collapse map for image encryption," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107457.

[39] X. Wang and J. Yang, "A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system," *Optik*, vol. 217, Sep. 2020, Art. no. 164884.

[40] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

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