ROI Image Encryption using YOLO and Chaotic Systems

Sung Won Kang[1]
Dept. Information Security
Pukyong National University
Busan, South Korea

Un Sook Choi[2]*
School of Artificial Intelligence
Tongmyong University
Busan, South Korea

***Abstract*—In this paper, we design a cellular automata (CA)-based ROI (region of interest) image encryption system that can effectively reduce computational cost and maintain an appropriate level of security. The proposed image encryption system obtains a cryptographic image through three steps. First, a region of interest with high importance is extracted from the entire image using deep learning. We use the YOLO (You Only Look Once) algorithm to extract the ROI from a given original image. Next, the detected ROI is encrypted using the Chen system, a chaotic-based function with high security. Finally, the execution time is effectively reduced by encrypting the entire image using a hardware-friendly CA. The safety of the proposed encryption system is verified through various statistical experiment results and analyses.**

Keywords*—Image encryption; cellular automata; YOLO algorithm; deep learning; Chen system; region of interest

I. Introduction

The development of information and communication technology has brought many changes in our society. Recently, with the emergence of new communication technologies such as the IoT (Internet of Things) and big data, various types of information are efficiently and conveniently transmitted and applied in various ways. The factory automation system improves productivity. It is possible to quickly and conveniently collect and utilize information using computers and mobile devices, and expand opportunities for social participation through SNS (social networking services). In addition, the demand for real-time data transmission has increased in applications such as medical service, the military, finance and education. And problems related to personal information protection such as personal information leakage and cyber terrorism are also frequently occurring. In particular, image security is an essential part of today's communication technology, and very important for safe transmission.

Due to the recent epidemic such as COVID-19, many changes have occurred in the daily life of our society [1]. Changes in daily life such as real-time non-face-to-face online meetings, education, telemedicine, and online collaboration have increased traffic to the network and increased demand for real-time security of multimedia. Multimedia traffic, including video, audio and image content, is very large and has a very high correlation between pixels. Unfortunately, traditional cryptographic algorithms such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm) are suitable for text data, but not for images or video in real-time applications. Many techniques have been developed to protect images [2].

Among these technologies, image encryption is the most intuitive and effective method of converting an image into an unrecognizable image. Through this method, it is possible to prevent theft and illegal reading of personal images, and to prevent leakage of personal information when sending images.

Chaos theory is a dynamic system that is very sensitive to time changes and initial conditions. Chaos theory can effectively generate a random sequence because a logical law exists even in a chaotic state that seems disorderly. The chaos-based encryption system is the most used technology for image encryption due to its many advantages such as high randomness, complexity, sensitivity to initial conditions, and system parameters. The chaos-based image encryption algorithm was introduced by Fridrich [3], and many research results have been proposed over the past 20 years [2-16]. The chaos-based cryptographic algorithm is processed through two steps. The first step is a diffusion process that randomly changes pixel values using a random sequence generated based on a chaotic function. At this time, in order to obtain high security and reliable encryption image, an encryption system that is very sensitive to the key must be used. Another process is the confusion process, which effectively change the position of the pixels. This step is a necessary process to protect the image against unexpected noise generation or deletion attacks in the process of transmitting the encrypted image.

X. Zhang et al. [7] designed an encryption system by introducing a bi-direction diffusion technique to compensate for the weaknesses of the image encryption method. In order to effectively perform permutations in the encryption stage, they proposed a method of wholly constructing permutations by combining small permutations. W. Zhang et al. [8] proposed a chaotic-based image cryptographic algorithm using both a chaotic cat map and a logistic map. They changed pixel planes to each other at the stage of changing the pixel position of the image. Tang et al. [9] proposed a method of an image encryption by dividing it into small blocks and encrypting the image using a chaos function. Zahmoul et al. [10] proposed an effective cryptosystem by designing a new chaos map based on the beta function frequently used in statistics and probability theory. They showed that the proposed beta chaotic function has higher sensitivity and security than other chaotic functions. Wang et al. [16] proposed the logistic-dynamic Arnold coupled logistic map lattice model. They used the proposed model as

*Corresponding Author

the key sequence generator of the image encryption system. Their proposed encryption system uses a dynamic coupling method based on a logistic map, and then applies the Arnold coupled logistic map lattice based on the Arnold map proposed in [6].

Although the cryptographic algorithm based on the chaos function has a high level of security, it is based on mathematical calculations, which increases the calculation cost.

In this paper, we design a CA-based ROI image encryption system that can effectively reduce computational cost and maintain an appropriate level of security. The proposed cryptographic system obtains a cryptographic image through three steps. First, an ROI with high importance is extracted from the entire image using deep learning. Next, the detected ROI is encrypted using a chaotic-based function with high security. Finally, the execution time is effectively reduced by encrypting the entire image using a hardware-friendly cellular automata. The safety of the proposed encryption system is verified through various statistical experiment results and analyses.

II. Background

A. YOLO

YOLO (You Only Look Once) proposed by Redmon et al. [17] is a 1-stage detector suitable for real-time detection. YOLO is composed of one neural network, so it predicts the bounding box surrounding the object and the class probability of which class the object belongs to with one calculation for the entire image. YOLO has superior performance compared to the existing object detection model based on R-CNN. The advantages of YOLO are as follows: 1) Because it is a single neural network structure, the configuration is simple and fast. 2) Because it learns surrounding information and processes the entire image, the background error is small. 3) Detection accuracy is high even for new images not seen in the training stage. Although it is less accurate than the state-of-the-art object detection model. But speed and accuracy are in a trade-off relationship. In this paper we use YOLO to extract the ROI of the original image in this paper.

B. Cellular Automata

CA is a system for analyzing dynamic systems in discrete time and finite discrete space. Cells, the basic unit for storing states of 0 and 1, are connected in a certain shape, and the states of each cell are updated simultaneously by local interaction of cells by a given state transition function [18]. CAs are classified according to the shape in which each cell is arranged. If they are arranged linearly, they are called one-dimensional CAs, if they are arranged in a plane, they are called two-dimensional CAs, and CAs arranged in a cubic shape are classified as three-dimensional CAs. Cells participating in the state transition of each cell are called neighbors. The most basic form is a 1-dimensional 3-neighbor CA with a radius of 1 relative to itself, and a CA with a radius of 2 including itself is called a 1-dimensional 5-neighbor CA. CA can effectively generate a random pattern with good randomness because it is connected to its neighbors by associative logic and its shape is composed of a regular arrangement.

For this reason, CA is applied to cryptographic systems [19-22]. In CA, where the state transition rule applied to each cell of the CA is expressed by XOR logic, the state transition function can be expressed as a matrix. If the characteristic polynomial of the state transition matrix of a given CA is a primitive polynomial, the sequence generated by the CA becomes the maximum periodic sequence [23]. This CA is referred to as a one-dimensional 5-neighbor maximum length CA (FNMLCA). Eq. (1) is a state transition function of a one-dimensional 5-neighbor CA.

$$u_i^{t+1} = a_i u_{i-2}^t \oplus b_i\, u_{i-1}^t \oplus c_i u_i^t \oplus d_i u_{i+1}^t \oplus e_i\, u_{i+2}^t \qquad (1)$$

where u_i^t is the state of the *i*th cell at time t, and $u_i^t = \{0,\ 1\}$, $a_i, b_i, c_i, d_i, e_i \in \{0, 1\}$. In this paper. we use a one-dimensional symmetric FNMLCA in which a_i, b_i, d_i, e_i in Eq. (1) are all 1. One-dimensional symmetric FNMLCA can generate high-quality random sequences than 1-D 3-neighbor 90/150 MLCA [23], and the diffusion rate is twice as fast. Fig. 1 shows the structure of an 8-cell one-dimensional symmetric FNMLCA with the state transition rule <00111010>. Each element of the state transition rule is each $c_i (i = 1,2, \cdots, 8)$in (1). The characteristic polynomial for the state transition matrix in Fig. 1 is $c(x) = x^8 + x^6 + x^5 + x^3 + 1$, and $c(x)$ is primitive.

C. Chen System

Chen system is a structure applied in chaotic dynamic control, synchronization, turbulence modeling and controlled weather model [24]. One of the chaotic dynamic system models, the Chen system, has similar properties to the Lorenz system. The Chen system can generate chaotic sequences sensitive to initial values.

Since the sequence generated by the Chen system has very high randomness, the system is used in key generation of the OTP (one time password) cryptosystem and key image generation in the image encryption process. The Chen system is expressed as a system of third-order nonlinear differential equations as shown in (2).

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \qquad (2)$$

where a=35, b=3, c=28. Fig. 2 shows the attractor of the Chen system.

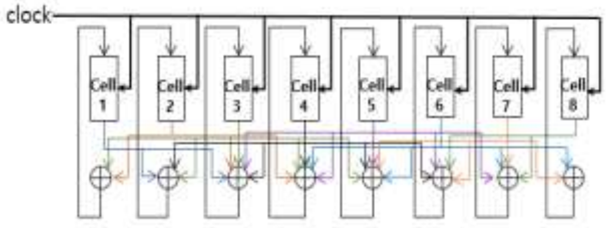

Fig. 1. The Structure of 1-Demensional Sysmetric FNMLCA with Transition Rule <00111010> and Characteristic Ploynomial $x^8 + x^6 + x^5 + x^3 + 1$.

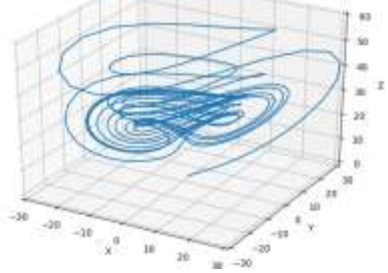

Fig. 2. The Attractor of the Chen System.

III. Proposed Algorithm

In this section, we propose a 1-D FNMLCA-based ROI image encryption algorithm. The proposed algorithm consists of three steps. The first step is ROI detection for the original image, and the second step is the encryption of the ROI.

The encryption of the ROI consists of shuffling the pixels of the ROI image and changing the pixel values using a sequence generated by the Chen system. Finally, the third step consists of encrypting the entire image.

A. Detecting of the ROI

YOLO divides the original image into $n \times n$ grids, and if there is an object in a grid cell, the grid cell detects the object. Assume that L bounding boxes are detected in the image [17]. The coordinates of the four vertices of the ith bounding box can be expressed as $(x_{i,1}, y_{i,1})$, $(x_{i,2}, y_{i,1})$, $(x_{i,1}, y_{i,2})$ and $(x_{i,2}, y_{i,2})$, where $x_{i,2} > x_{i,1}$ and $y_{i,2} > y_{i,1}$. The smallest rectangular area including all L boxes becomes the ROI. The four vertices $(rx_{i,1}, ry_{i,1})$, $(rx_{i,2}, ry_{i,1})$, $(rx_{i,1}, ry_{i,2})$ and $(rx_{i,2}, ry_{i,2})$ of the ROI are calculated as follows.

$$rx_{i,1} = \min(\{x_{i,1} |\ i = 1, 2, \cdots, L\}) \tag{3}$$

$$ry_{i,1} = \min(\{y_{i,1} |\ i = 1, 2, \cdots, L\}) \tag{4}$$

$$rx_{i,2} = \max(\{x_{i,2} |\ i = 1, 2, \cdots, L\}) \tag{5}$$

$$ry_{i,2} = \max(\{y_{i,2} |\ i = 1, 2, \cdots, L\}) \tag{6}$$

Fig. 3 shows the process of detecting the ROI by detecting the bounding box using YOLO for the original image.

B. Encryption of the ROI

ROI encryption consists of shuffling pixel positions and randomly changing pixel values. First, pixel positions are shuffled using one-dimensional symmetric FNMLCA for ROI, which is the minimum area including all bounding boxes detected using YOLO. Unlike mathematical operation-based chaotic functions, one-dimensional symmetric FNMLCA is very efficient because it is easy to implement in hardware and can be implemented in hardware-friendly even when implemented in software. The one-dimensional symmetric FNMLCA F_n having $p_n(x)$ as the characteristic polynomial is synthesized by selecting the primitive polynomial $p_n(x)$ of degree n corresponding to the selected n. For effective synthesis, F_n is synthesized using the state transition function T_n of the one-dimensional 3-neighbor MLCA corresponding to $p_n(x)$.

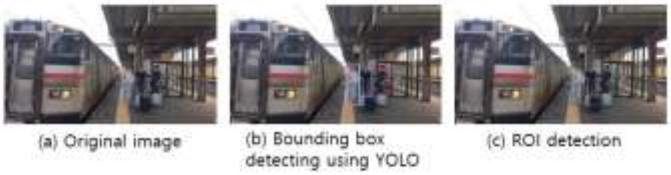

Fig. 3. The Process of Detecting the ROI for the Original Image.

A sequence generated using F_n and the initial state is arranged according to the size of the ROI, and row positions of the ROI are rearranged using the arranged sequence. Reorder the column positions in the same way for the shuffled ROI image in the row positions. In the same way, the row-column pixel shuffling process is repeated k times. To increase the security level, different $F_n s$ and initial values are selected for each round of color component and row-column shuffling of the ROI.

The next step is to change the value of each pixel of the shuffled ROI image to an arbitrary value. Let the size of the ROI detected from the original image be W × H, where W and H are $W = (rx_{i,2} - rx_{i,1})$ and $H = (ry_{i,2} - ry_{i,1})$ from (3)-(6). Using the selected initial value and Chen chaotic system, a sequence of size $\mathrm{W} \times \mathrm{H} \times 3 (= \mathrm{M})$ is generated. In order to generate an efficient chaotic sequence in which the correlation with the initial value is removed, the values generated from the first to the 2000th are discarded and the values generated from the 2001th are used. The ith value $s_i (i = 0, 1, \cdots, M-1)$ of the generated sequence is calculated using (7) to obtain an integer value $k_i (i = 0, 1, \cdots, L-1)$ between 0 and 255.

$$k_i = (s_i \times 10^{14})\ mod\ 256 \quad (\mathrm{i} = 0, 1, \ \cdots, \mathrm{M}-1) \tag{7}$$

By rearranging the generated integer sequence k_i, a W × H color key image with the same size as the ROI is created and XORed with the shuffled ROI image.

C. Encryption of the Entire Image

After performing ROI encryption, the entire image is encrypted. Like the ROI image encryption process, the final encrypted image is obtained through a shuffling step that changes the pixel position and a diffusion step that randomly changes pixel values.

In the entire image, areas excluding the ROI are generally less important than the ROI. Therefore, in the ROI image encryption process, since encryption was first performed using a function with high security strength, the entire image is encrypted with priority over performance speed rather than security strength. In the proposed system, the hardware-friendly one-dimensional symmetric FNMLCA is used to speed up the shuffling process of pixel positions. And it is used to change pixel values for the entire image in the diffusion process.

In the pixel shuffling step, the pixel shuffling process in row-column units is appropriately repeated in the same way as the shuffling process in the ROI encryption process.

To generate a key image for changing pixel values, generate a sequence using FNMLCA and initial values that are appropriately large as much as the entire image size, and adjust the values to fit the range of image pixel values. For example, if the color value of one pixel has values ranging from 0 to 255 for each R, G, and B, the value generated through the state transition of one-dimensional symmetric FNMLCA is processed as mod 256 and XORed with the pixel value. Repeat for the R, G, and B color planes.

D. Proposed FNMLCA-based ROI encryption Algorithm

The FNMLCA-based ROI encryption algorithm proposed in this paper is performed through the following five steps. Among the main algorithms below, FNMLCA is used for the pixel shuffling step and the pixel value change step of the entire image. Algorithm 1 is a sequence generation function using FNMLCA, and Algorithm 2 is a pixel shuffling function using a sequence generated from FNMLCA. Algorithm 3 is the proposed main encryption algorithm. Algorithm 4 is a decoding algorithm. After performing ROI encryption, the entire image is encrypted. Like the ROI image encryption Fig. 4 shows the block diagram of the proposed ROI image encryption system in this paper. Table I shows the proposed ROI image encryption algorithm.

In order to perform the ROI decryption algorithm, the sender needs to transmit the coordinates of the ROI together with the key to the receiver. And the ROI decoding algorithm performs the following processes:

TABLE I. THE PROPOSED ROI IMAGE ENCRYPTION ALGORITHM

Algorithm 1 FNMLCA sequence generator

```
$n$ is a number of cells
$R_n$ is a rule of FNMLCA
$v^t$ is a state vector of the CA at the time t
seq is a list [$v^0$]
def FNMLCA($R_n$, $v^t$, $k$):
    for $i$ in range(0, $k$):
        $v^{i+1}$ ← ($v^i$//4)+( $v^i$//2)+( $v^i \wedge R_n$)+( $v^i$*2)+( $v^i$*4) mod $2^n$
            seq.append($v^{i+1}$)
    return seq
```

Algorithm 2 FNMLCA shuffling

```
P is the input image
W is the width of the P
H is the height of the P
seq1, seq2 are sequences generated by Algorithm 1
def shuffling(P, seq1, seq2):
    S is the empty image with the size W×H
    for i in range(0, W}:
        S[i, :] ← P[seq1[i], :]
    for j in range(0, H):
        S[:, j] ← P[:, seq2[j]]
    return S
```

Algorithm 3 ROI Encryption Algorithm

```
Input : Original image
Output : Encryption image
1: Detect the ROI from the original image using the pre-trained YOLO algorithm.
2: Shuffle the ROI using FNMLCA (Algorithm 2).
3: XOR the key image generated from Chen attractor with the shuffled
   ROI image.
4: Shuffle the entire ROI-encrypted image using FNMLCA (Algorithm 2).
5: Create a key image (KImg) with the same size as the original image
   using FNMLCA (Algorithm 1).
6: XOR the image obtained in step 4 with KImg to generate a encrypted image.
```

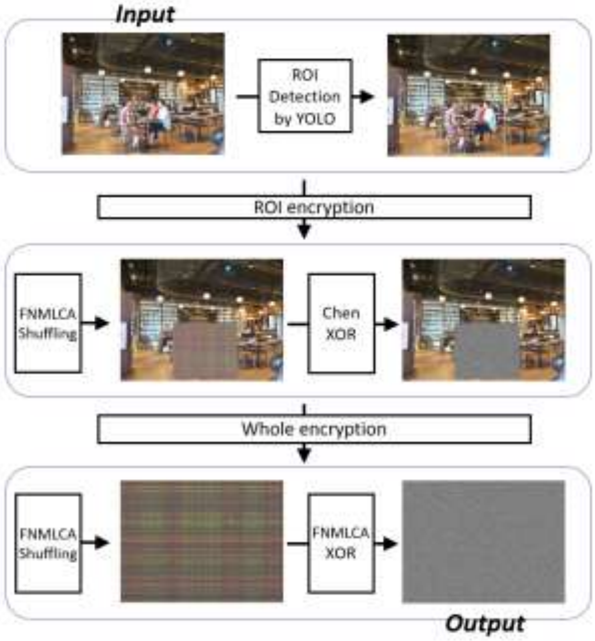

Fig. 4. The Block Diagram of the Proposed ROI Image Encryption System.

- Step 1. After using FNMLCA to create a key image of the same size as the entire area (Algorithm 1), XOR it with the image to be decrypted.
- •Step 2. Shuffle the image of Step 1 using FNMLCA (Algorithm 2).
- Step 3. XOR the key image generated from Chen attractor on the received ROI coordinate area.
- Step 4. Shuffle the ROI image using FNMLCA (Algorithm 2). The image obtained at this time is a decoded image.

IV. EXPERIMENT RESULTS AND SECURITY ANALYSIS

In this section, the results of statistical analysis are presented. Photographs of people in various forms were used as original images for simulation. Fig. 5 shows some of the original image samples of various sizes used in the experiment. For each original image, the serial number is subsequently referenced in the data representing the experimental results. The number in (•) next to each image number is the width × height of the image.

A. Histogram Analysis

In order to defend against statistical attacks, the encryption technique must uniformly spread the pixel values of a given image. Fig. 6 is an image encrypted by the proposed algorithm for each original image in Fig. 5. According to Fig. 6, the encrypted image cannot recognize the original image with the naked eye. Fig. 7 shows the histograms for the original image in Fig. 5 and the encrypted image in Fig. 6. Comparing the histograms for each original image and the encrypted image in Fig. 7, it can be seen that the histogram of the original image has a non-uniform color distribution that reflects the feature of the image. On the other hand, the histogram of the encrypted image shows all pixel values uniformly.

Fig. 5. Original Images and their Image Sizes.

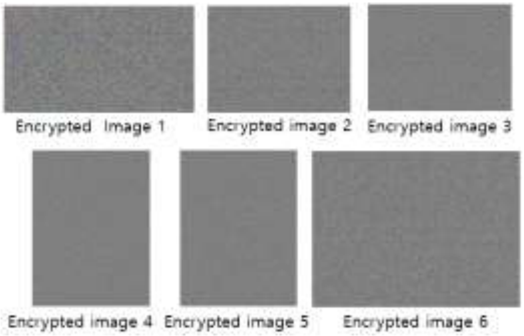

Fig. 6. Images Encrypted by the Porposed Algorithm for each Original Images.

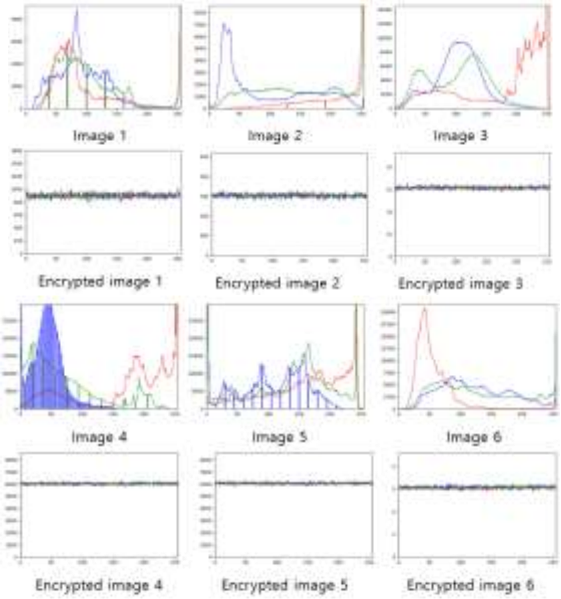

Fig. 7. The Histograms for Original/Encrypted Images.

Therefore, it can be seen that the statistical characteristics of the original image are removed in the encrypted image through the histogram result.

B. Correlation Analysis

The image has a characteristic that the values of adjacent pixels are almost the same. Since a statistical attack can also use this characteristic, the encryption technique must ensure that the values of adjacent pixels vary. The correlation coefficient is used as a measure of the degree of relation between adjacent pixels in image encryption. The degree of correlation is between -1 and +1, and the closer to ±1, the higher the correlation, and the closer to 0, the lower the correlation.

The correlation coefficient is calculated using (8) to show that the correlation between adjacent pixels has disappeared with respect to the image encrypted by the proposed method.

$$\rho_{xy} = \frac{\sum_{i=1}^{N}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i-\bar{Y})^2}} \tag{8}$$

$\bar{X} = \sum_{i=1}^{N} X_i/N$, X and Y are the values of two adjacent pixels in (8). Table II shows the correlation coefficients of pixels adjacent to each other in the horizontal, vertical, and diagonal directions of the original image and the encrypted image.

TABLE II. THE CORRELATION COEFFICIENTS OF PIXELS ADJACENT TO EACH OTHER IN THE HORIZONTAL, VERTICAL AND DIAGONAL DIRECTIONS

Image	color	Horizontal	Vertical	Diagonal
Original image 1	R	0.97972	0.98736	0.97314
	G	0.98040	0.98729	0.97318
	B	0.97956	0.98759	0.97295
Encrypted image 1	R	-0.00422	-0.00824	0.00192
	G	0.00615	0.00269	-0.00280
	B	0.00085	0.00088	-0.00025
Original image 2	R	0.86795	0.85358	0.76400
	G	0.84946	0.83211	0.78305
	B	0.85573	0.84011	0.74209
Encrypted image 2	R	0.00704	-0.00400	0.00102
	G	-0.00069	0.00819	0.00527
	B	0.01022	0.00596	0.01056
Original image 3	R	0.94519	0.95867	0.91887
	G	0.92337	0.94256	0.88494
	B	0.93120	0.94944	0.90104
Encrypted image 3	R	-0.00118	-0.00328	-0.00008
	G	-0.00642	0.00764	-0.00086
	B	-0.00171	-0.00723	0.00518
Original image 4	R	0.98992	0.99155	0.98368
	G	0.99161	0.99385	0.98785
	B	0.99084	0.99327	0.98603
Encrypted image 4	R	0.00146	0.00259	-0.00012
	G	-0.00111	-0.00268	0.00368
	B	0.00242	0.00373	-0.00660
Original image 5	R	0.96853	0.99446	0.95757
	G	0.98370	0.99730	0.97965
	B	0.97507	0.99589	0.96875
Encrypted image 5	R	0.00100	0.00062	-0.00220
	G	-0.00712	-0.00571	-0.01348
	B	0.00328	-0.00475	0.00885
Original image 6	R	0.93681	0.95447	0.92919
	G	0.95735	0.96808	0.94631
	B	0.94541	0.95920	0.93359
Encrypted image 6	R	-0.00012	0.00271	0.00157
	G	0.00115	0.00419	0.00538
	B	-0.00051	0.00255	0.00153

The correlation coefficient was calculated from 2500 samples randomly extracted from the image, and a more accurate correlation coefficient was calculated by calculating the average of the results of 300 repetitions. Also, correlation analysis can be expressed using a scatter plot. In Fig. 8, the scatter plots of pixels adjacent to each other in the horizontal, vertical and diagonal directions for the original image (image 1) in Fig. 5 and the encrypted image for the original image are shown. It can be confirmed that the scatter of the original image has a high positive correlation, and it can be confirmed that the scatter of the encrypted image has a very low correlation. From the results of Table II and Fig. 8, it can be seen that the strong correlation between pixels of the original image has disappeared in the encrypted image by the proposed algorithm. Table III is a comparison of the correlation coefficients of images encrypted by the proposed method and other methods.

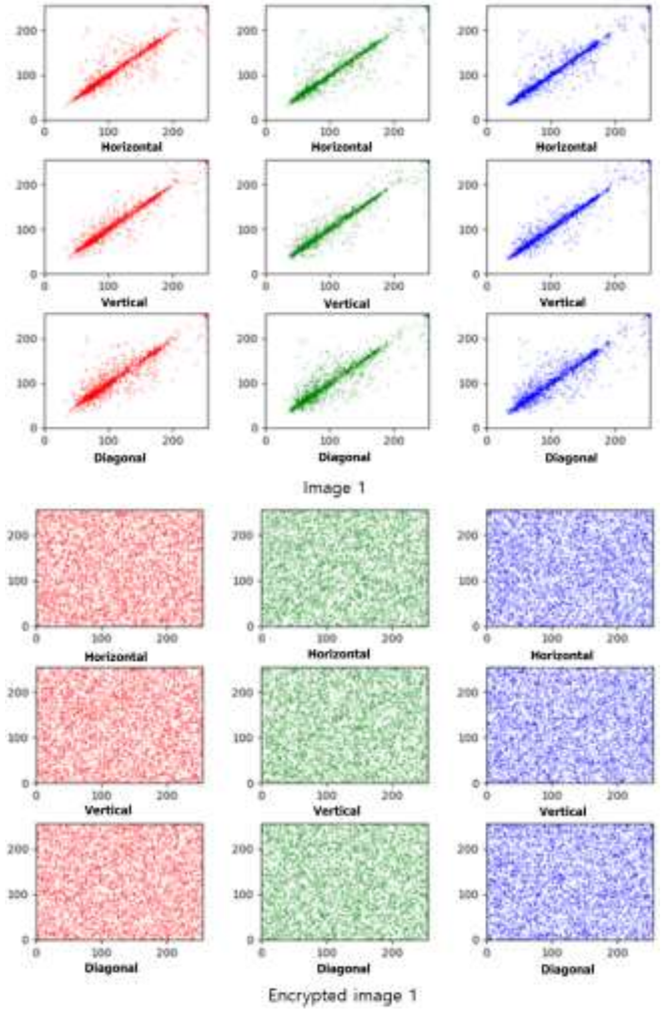

Image 1

Encrypted image 1

Fig. 8. The Correlation Scatter Plots of Pixels Adjacent to each other in the Horizontal, Vertical and Diagonal Directions for the Original/Encrypted Image (Image 1).

TABLE III. THE COMPARISON OF CORRELARION COEFFICENTS OF IMAGES ENCRYPTED BY THE PROPOSED METHOD AND OTHER METHODS

Method		Correlation coefficient	
Proposed		0.0006	
Kamal et al. [25]		-0.0024	
Wade et at. [26]		0.0401	
Yang et al. [27]		-0.0034	
Hua et al. [28]		0.0030	
B	7.56390	B	7.99975

C. Entropy Analysis

The uncertainty of the information should be increased by the encryption technology. In information theory, entropy is used as a measure of information uncertainty. Information entropy means the minimum average bit required to represent a given data. Entropy can be obtained from the distribution of pixel values of a given image. Calculate entropy using (9).

$$H(X) = -\sum_{i=0}^{2^n-1} p(x_i) log_2 p(x_i) \qquad (9)$$

, where $p(x_i)$ is a probability distribution of a pixel value x_i. In a general 8(=*n*) bit format image, the maximum value of entropy is 8, and the maximum entropy means that the given information is uncertain.

Table IV shows the entropies of the given original and encrypted images in Fig. 5 and Fig. 6. The encrypted images by the proposed encryption method have the entropies very close to 8. And Table V shows the comparison of entropy of images encrypted by the proposed algorithm and other methods.

TABLE IV. THE ENTROPIES OF THE GIVEN ORIGINAL AND ENCRYPTED IMAGES

Original color		Entropy	Encrypt. color		Entropy
image 1	R	6.99289	image 1	R	7.99917
	G	7.18091		G	7.99932
	B	7.09116		B	7.99917
image 2	R	6.96075	image 2	R	7.99945
	G	6.93752		G	7.99953
	B	6.94867		B	7.99933
image 3	R	7.59813	image 3	R	7.99977
	G	7.71103		G	7.99978
	B	7.62290		B	7.99976
image 4	R	7.28923	image 4	R	7.99989
	G	7.61027		G	7.99986
	B	7.51687		B	7.99987
image 5	R	7.69426	image 5	R	7.99988
	G	6.85420		G	7.99989
	B	7.72390		B	7.99987
image 6	R	7.43362	image 6	R	7.99977
	G	7.70272		G	7.99973

TABLE V. THE COMPARISON OF ENTROPY OF IMAGES ENCRYPTED BY THE PROPOSED METHOD AND OTHER METHODS

Method	Entropy
Proposed	7.9997
Kamal et al. [25]	7.9973
Wade et at. [26]	7.9422
Zhong et al. [29]	7.9972
Hua et al. [30]	7.9977

D. Difference Analysis

A differential attack is achieved through a selective plaintext attack. This is a way for malicious users to find vulnerabilities in cryptographic systems by using encryption and decryption using different keys.

To be safe from this differential attack, the cryptographic system must be sensitive to even small changes in keys. PSNR, NPCR, and UACI are representative measures to analyze the sensitivity of cryptographic systems. The peak signal-to-noise ratio (PSNR) is the ratio between the original image and the encrypted image. The higher the PSNR, the smaller the difference between the two images. PSNR is calculated by (10).

$$PSNR = 10 \log_{10}(255^2/MSE) \tag{10}$$

where the mean square error (MSE) is the mean squared difference between the original input image and the encrypted image. It is calculated in pixels by squaring the difference of all pixels and dividing by the total number of pixels. MSE is calculated by (11).

$$\text{MSE} = \sum_{i,j}\left(a_{i,j} - b_{i,j}\right)^2/(W \times H) \tag{11}$$

where W and H are the width and height of the given image, and $a_{i,j}$ and $b_{i,j}$ are the pixel values of the cryptographic image encrypted with another key.

Other metrics used to evaluate the cryptographic strength of image encryption algorithms with respect to differential attacks are NPCR and UACI. NPCR is a measure of the absolute pixel change rate between two images, and UACI is the average color intensity difference between the two images. For two cryptographic images C_1 and C_2 generated by different keys with only a 1-bit change, NPCR and UACI are calculated by (12) and (13).

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100(\%) \tag{12}$$

$$\text{UACI} = \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{W \times H \times 255} \times 100(\%) \tag{13}$$

where $D(i,j)$ is 0 for $C_1(i,j) = C_2(i,j)$ and 1 for $C_1(i,j) \neq C_2(i,j)$. Also, $C_1(i,j)$ and $C_2(i,j)$ are the pixel values for each position of C_1, C_2, and W and H are the width and the height of C_1 and C_2.

Table VI shows the difference analysis results for the two images encrypted by the proposed method using different keys for the original images in Fig. 5. Here, the two keys used to encrypt each original image differ only by one bit. The results in Table VI are within the reference value range [32]. Therefore, the proposed image encryption system can sufficiently withstand differential attacks. Table VII shows the comparison of NPCR and UACI of images encrypted by the proposed method and several methods.

E. Robustness Analysis against Data Corruption and Deletion Attacks

Malicious attackers attempt several illegal activities when images are transmitted. In this process, abnormal noise data may be inserted and the image may be damaged. Therefore, cryptographic systems must be robust against variety of data corruption and deletion attacks. Fig. 9 is the result of decrypting the encrypted image with data corruption due to various reasons by the proposed algorithm. It can be seen that the original image is decoded without serious damage when the image in which one part is intensively lost is decoded in the proposed system.

TABLE VI. DIFFERENTIAL ANALYSIS BETWEEN TWO ENCRYPTED IMAGES GENERATED USING DIFFERENT KEYS FOR EACH ORIGINAL IMAGES

Image color		NPCR (%)	UACI (%)	PSNR
image 1	R	99.58724	33.49941	7.73394
	G	99.62847	33.50500	7.74525
	B	99.61632	33.43314	7.75461
image 2	R	99.62603	33.46946	7.74767
	G	99.61883	33.44007	7.77723
	B	99.59722	33.32345	7.75534
image 3	R	99.61255	33.48647	7.74219
	G	99.59920	33.48335	7.74559
	B	99.61688	33.47931	7.75331
image 4	R	99.60663	33.46790	7.74482
	G	99.61496	33.48184	7.74805
	B	99.60042	33.45623	7.74559
image 5	R	99.61692	33.46269	7.74720
	G	99.60322	33.46984	7.74805
	B	99.59699	33.49762	7.73960
image 6	R	99.60988	33.50102	7.73592
	G	99.61230	33.44299	7.75711
	B	99.60874	33.42345	7.75698

TABLE VII. THE COMPARISON OF NPCR AND UACI OF IMAGES ENCRYPTED BY THE PROPOSED METHOD AND OTHER METHODS

Method	NPCR (%)	UACI (%)
Proposed	99.6096	33.4624
Kamal et al. [25]	99.6223	33.4406
Wade et at. [26]	99.6136	31.3253
Yang et al. [27]	99.6122	33.4155
Hua et al. [28]	99.6459	33.3797
Zhong et al. [29]	99.606	33.456
Hua et al. [30]	99.9974	33.2716
Thanikaiselvan et al. [31]	99.5945	33.0644

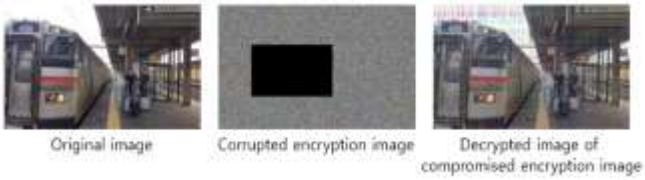
Original image
Corupted encryption image
Decrypted image of compromised encryption image

Fig. 9. Decryption Result of the Encrypted Image with Data Loss.

Therefore, the proposed encryption system can be said to be robust against data corruption and deletion attacks.

F. Analysis of Keyspace

In cryptosystems, the keyspace must be large enough to resist brute force attacks. The number of available keys in a cryptographic system determines the size of the keyspace. In the proposed encryption system, the initial value of the Chen system used to generate the key image in ROI image encryption is used as the key. And the cell size, transition rule, and initial vector of FNMLCAs used in the shuffling process of the ROI image and the whole image and the pixel value change process of the whole image are used as keys.

The size n of the cell of FNMLCA is sufficiently large than 8 which is the number of pixel bits of the image. At this time, the number of transition rules is 2^5 for each cell, so the total number of transition rules is 2^{5n} and the number of initial vectors is 2^n. In this FNMLCA shuffling step, different FNMLCA and different initial vectors are selected in each color plane and in the row and column shuffling step, so the number of keys in one shuffling encryption process is $(2^{6n})^6$. Therefore, the number of keys used in the ROI image shuffling, whole image shuffling, and entire image pixel value change steps is $(2^{18\times6})^6)^3 = 2^{108\times18}$ when n=18. The initial number of Chen system used to generate a key image for changing the pixel value of the ROI image is $10^{16} \approx 2^{53}$. Therefore, the size of the keyspace is large enough to be about $2^{53+108\times18} = 2^{1997}(\gg 2^{128})$ when the size of FNMLCA is 18. Therefore, the proposed cryptosystem can sufficiently resist brute force attacks.

G. Performance Speed Analysis

The proposed encryption system can detect ROI faster than other deep learning models by adopting the YOLO model in the ROI detection process. Most of the chaotic map-based image encryption algorithms encrypt the entire original image using the chaotic map. However, the proposed method minimizes the algebraic operation by using the chaotic map only in the process of changing the pixel value of the ROI with high importance among the original image. This effectively reduced execution time while maintaining security over key areas of the image. And by adopting the FNMLCA system for both the shuffling of the encryption system and the diffusion process for the entire image, the proposed system can be implemented in a hardware-friendly manner. The FNMLCA-based encryption system uses only logical and shift operations. In particular, in the process of changing the position of the pixel during the shuffling process, it is very effective in terms of execution speed because it relocates the pixel position by row and column units rather than by pixel unit. For this experiment, we used Python 3.8 and Intel(R) Core(Tm) i7-4770 CPU 3.40GHz on Windows 10 OS. The proposed algorithm is very fast enough to perform real-time image encryption. Table VII shows the execution time for each partial process in the process of encrypting the original images in Fig. 5 by the proposed algorithm. ROI detection time, ROI shuffling time, ROI diffusion process time, entire image shuffling time, and entire image diffusion process time are shown separately and the encryption execution time of the entire process is shown. In Table VIII, it can be seen that the ROI detection time for image 1 takes more than average time, the ROI detection time is very effective in most images, and it is very effective to perform the diffusion process using only the ROI using the Chen system.

TABLE VIII. THE EXECUTION TIME FOR EACH PARTIAL PROCESS IN THE PROCESS OF ENCRYPTING ORIGINAL IMAGES OF VARIOUS SIZES

	Image 1	Image 2	Image 3
Image size (W × H)	640×360	720×540	1024×768
ROI size (W × H)	123×122	519×274	173×592
ROI detection (sec.)	1.0342	0.4336	0.4335
ROI shuffling (sec.)	0.0156	0.0156	0.0156
ROI diffusion (sec.)	0.0781	0.6929	0.4699
Entire image shuffling (sec.)	0.0156	0.0156	0.0156
Entire image diffusion (sec.)	0.4062	0.6774	1.3075
Total encryption time (sec.)	1.6037	1.8351	2.2421
	Image 4	Image 5	Image 6
Image size (W × H)	1080×1433	1080×1441	1024×768
ROI size (W × H)	348×798	468×1162	407×353
ROI detection (sec.)	0.4233	0.5445	0.4692
ROI shuffling (sec.)	0.0156	0.0156	0.0156
ROI diffusion (sec.)	1.3980	2.6088	0.6561
Entire image shuffling (sec.)	0.0469	0.0781	0.0156
Entire image diffusion (sec.)	2.8169	2.6400	1.2966
Total encryption time (sec.)	4.7034	5.8870	2.4531

V. CONCLUSION

In this paper, we designed a new ROI image encryption system based on FNMLCA. The proposed algorithm can encrypt quickly in terms of speed, and at the same time, it can also increase security for high-value areas. The proposed algorithm detects ROI quickly by using YOLO among deep learning models, and because only the ROI image uses a chaotic map, it is effective in speed compared to other chaotic-based encryption algorithms. In particular, the key sequence was effectively generated through the hardware-friendly FNMLCA. In the pixel shuffling process, the overall encryption speed is improved by performing shuffling in row/column units rather than pixels. In addition, to enhance security, the ROI image is shuffled twice at pixel positions and pixel values by the proposed encryption system. The security strength is strengthened because the replacement process is performed. We plan to apply it to video encryption in the future.

ACKNOWLEDGMENT

This research was supported by the Tongmyong University Research Grants 2018(2018A046).

REFERENCES

[1] T. Favale, F. Soro, M. Trevisan, I. Drago, and M. Mellia, “Campus traffic and e-Learning during COVID-19 pandemic,” Comput. Networks, vol. 176, no. 20, Jul. 2020. doi: 10.1016/j.comnet.2020.107290.

[2] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," Multimed. Tools Appl., vol. 75, no. 11, pp. 6303–6319, Jun. 2016. doi: 10.1007/s11042-015-2573-x.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int J Bifurcation and Chaos, vol. 8, no. 6, pp.1259–1284, Jun. 1998. doi: 10.1142/S021812749800098X.

[4] X. Wang, J. Zhao, and Z. Zhang, "A chaotic cryptosystem based on multi-one-dimensional maps," Mod. Phys. Lett. B, vol. 23, no. 2, pp. 183–189, Jan. 2009. doi: 10.1142/S0217984909017947.

[5] M.S. Azzaz, C. Tanougast, S. Sadoudi, and A. Dandache, "Robust chaotic key stream generator for real-time images encryption," J. Real-time Image Process., vol. 8, pp. 297–306, Sept. 2013. doi: 10.1007/s11554-011-0219-4.

[6] Y.Q. Zhang, and X.Y. Wang, "Spatiotemporal chaos in Arnold coupled logistic map lattice," Nonlinear Anal. Model. Control, vol. 18, no. 4, pp. 526–541, Oct. 2013. doi: 10.15388/NA.18.4.13977.

[7] X. Zhang, and Z. Zhao, “Chaos-based image encryption with total shuffling and bidirectional diffusion,” Nonlinear Dyn, vol. 75, no. 1-2, pp. 319–330, Jan. 2014. doi: 10.1007/s11071-013-1068-4.

[8] W. Zhang, H. Yu, and Z. Zhu, “Color image encryption based on paired interpermuting planes,” OPT COMMU, vol. 338, no. 1, pp. 199–208, Mar. 2015. doi: 10.1016/j.optcom.2014.10.044.

[9] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," Multimed. Tools Appl., vol. 74, no. 15, pp. 5429-5448, Aug. 2015. doi: 10.1007/s11042-014-1861-1.

[10] R. Zahmoul, R. Ejbali, and M. Zaied, “Image encryption based on new Beta chaotic maps,”Opt. Lasers Eng., vol. 96, pp. 39-49, Sept. 2017. doi: 10.1016/j.optlaseng.2017.04.009.

[11] J.S. Khan, and J. Ahmad, "Chaos based efficient selective image encryption," Multidim Syst Sign Process, vol. 30, no. 2, pp.943-961, May 2019. doi: 10.1007/s11045-018-0589-x.

[12] A.Y. Niyat, M.H. Moattor, and M.N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," Opt. Lasers Eng. vol. 90, pp.225–237, Mar. 2017. doi: 10.1016/j.optlaseng. 2016.10.019.

[13] Y. Zhang, "The unifed image encryption algorithm based on chaos and cubic S-Box," Inf. Sci., vol.450, pp. 361–377, Jun. 2018. doi: 10.1016/j.ins.2018.03.055.

[14] R. Parvaz, and M. Zarebnia, "A combination chaotic system and application in color image encryption," Opt. Laser Technol. vol. 101, pp. 30–41, May 2018. doi: 10.1016/j.optlastec.2017.10.024.

[15] H.M. Ghadirli, A. Nodehi and R. Enayatifar, "An overview of encryption algorithms in color images," Signal Processing, vol. 164, pp. 163–185, Nov. 2019. doi: 10.1016/j.sigpro.2019.06.010.

[16] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," Nonlinear Dyn. vol.95, no.1, pp. 2797-2824, Mar. 2019. doi: 10.1007/s11071-018-4723-y.

[17] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: unified, real-time object detection," Proc. of 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.779-788, 2016. doi: 10.1109/CVPR.2016.91.

[18] S. Wolfram, "Random sequence generation by cellular automata," Adv. Appl. Math., vol. 7, no. 2, pp. 123-169, Jun. 1986. doi: 10.1016/0196-8858(86)90028-X.

[19] P. Ping, J. Wu, Y. Mao, F. Xu, and J. Fan, "Design of image cipher using life-like cellular automata and chaotic map," Signal Processing, vol. 150, pp. 233-247, Sep. 2018. doi: 10.1016/j.sigpro.2018.04.018.

[20] G. Kumaresan and N.P. Gopalan, "Reversible data hiding in encrypted images using public cloud and cellular automata, J. Appl. Secur. Res., vol. 14, no. 4, pp. 427-444, Sept. 2019. doi: 10.1080/19361610.2019.1656472.

[21] W. Zhang, Z. Zhu, and H.Yu, "A symmetric image encryption algorithm based on a coupled logistic–Bernoulli map and cellular automata diffusion strategy," entropy, vo. 21, no. 5, 504(23pages), May 2019. doi: 10.3390/e21050504.

[22] U.S. Choi, S.J. Cho, J.G. Kim, S.W. Kang and H.D. Kim, "Color image encryption based on programmable complemented maximum length cellular automata and generalized 3-D chaotic cat map," Multimed. Tools App., vol. 79, no. 10, pp. 1-18, Aug. 2020. doi: 10.1007/s11042-020-09033-y.

[23] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, “New synthesis of one-dimensional 90/150 linear hybrid group cellular automata,” IEEE T COMPUT AID D, vol. 26, no. 9, pp. 1720-1724, Sept. 2007. doi: 10.1109/TCAD.2007.895784.

[24] P. Sooraksa, and G. Chen, “Chen systems as a controlled weather model – physical principle, engineering design and real applications,” Int. J. Bifurcation and Chaos, vol. 28, no. 4, 1830009, 2018. doi: 10.1142/S0218127418300094.

[25] S.T. Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish, and M.M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," IEEE Access, vol. 9, pp. 37855-37865, Mar. 2021. doi: 10.1109/ACCESS.2021.3063237.

[26] M.I. Wade, M. Chouikha, T. Gill, W. Patterson, T.M. Washington, and J. Zeng, "Distributed Image Encryption Based On a Homomorphic Cryptographic Approach," Proc. of 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile(UEMCON), Feb. 2020. doi: 10.1109/UEMCON47517.2019.8993025.

[27] F. Yang, J. Mou, Y. Cao, and R. Chu, "An Image Encryption Algorithm Based on BP Neural Network and Hyperchaotic System," China Communications, vol. 17, no.5, pp 21-28, May 2020. doi: 10.23919/JCC.2020.05.003.

[28] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image Encryption Using Josephus Problem and Filtering Diffusion," IEEE Access, vol. 7, pp. 8660-8674, Jan. 2019. doi: 10.1109/ACCESS.2018.2890116.

[29] Y. Zhong, H. Liu, X. Sun, R. Lan, and X. Luo, "Image Encryption Using 2D Sine-Piecewise Linear Chaotic Map," Proc. of 2018 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR), Chengdu, China, July, 2018. doi: 10.1109/ICWAPR.2018.8521240.

[30] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using highspeed scrambling and pixel adaptive diffusion," signal processing, vol. 144, pp 134-144, Mar. 2018. doi: 10.1016/j.sigpro.2017.10.004.

[31] V. Thanikaiselvan, S. kumar, and R. Gera, "New Image Encryption using Chaotic Map in Wavelet Domain," Proc. of 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, Mar. 2019. doi: 10.1109/ViTECoN.2019.8899365.

[32] Y. Wu, J.P. Noonan and, S. Agaian, “NPCR and UACI randomness Tests for image encryption,” Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), pp 31–38, Apr. 2011.