DOI: 10.22146/jnteti.jnteti.v13i2.9623

Confusion and Diffusion Techniques for Image Encryption Process Based on Chaos System

Magfirawaty Magfirawaty[1], Ariska Allamanda[1], Malika Ayunasari[1], Muhamad Nadhif Zulfikar[1]

[1] Cryptographic Hardware Engineering, Cryptography Department, National Cyber and Crypto Polytechnic, Bogor, Jawa Barat 16120, Indonesia

[Received: 19 September 2023, Revised: 8 December 2024, Accepted: 20 March 2024]
Corresponding Author: Magfirawaty Magfirawaty (email: magfirawaty@poltekssn.ac.id)

ABSTRACT — Face recognition uses biometric technologies to identify humans based on their facial characteristics. This method is commonly used to restrict information access control. The benefits of face recognition systems encompass their ease of use and security. The human face recognition process consists of face detection, face tracking, and face recognition. The process uses some algorithms: the Viola-Jones for face detection, the Kanade-Lucas-Tomasi (KLT) for face tracking, and the principal component analysis (PCA) for face recognition. Furthermore, this research proposed face recognition with an encryption process to protect the data stored in a database. The encryption process consists of two main processes: confusion and diffusion. The confusion process is randomizing the position of the original image pixels. This research utilized the Arnold’s cat map (ACM) for the confusion process, and the diffusion process was performed using the XOR operation with the key generated from the 1D chaos system. Three different 1D chaos systems, namely logistic map, Bernoulli map, and tent map, were compared to see which chaos system had the best encryption results. Tests were conducted by comparing various parameters on the three proposed 1D chaos systems, including correlation coefficient, histogram analysis, entropy value, number of pixel rate changes (NPCR), and unified average change intensity (UACI). Based on testing the image encryption results, the diffusion process utilizing the tent map produced the best image encryption compared to other chaotic systems.

KEYWORDS — Face Recognition, Arnold’s Cat Map, Logistic Map, Bernoulli Map, Tent Map.

I. INTRODUCTION

Many companies use technology to run their operations from time to time. Valuable assets are among objects that a company must protect. These assets are usually stored in a room requiring access control with security authentication. Smart cards are usually used for the authentication process. However, this system is inefficient as cards can be lost due to human error. Therefore, it is necessary to develop an authentication process utilizing technology, especially biometric technology. The use of biometrics is increasing, particularly in security-related applications such as logical and physical access control, forensic investigations, IT security, identity theft protection, and prevention or detection of terrorism [1]. Biometric technology can be classified based on the type of signal used: physiological, behavioral, and cognitive signals [2]. Physiological biometrics uses physical characteristics such as eyes, fingerprints, and faces.

Face recognition is a biometric recognition technology based on human facial features done using 2D input with images or 3D input with training processes [2]. A face recognition system generally consists of face detection, face tracking, and face recognition [3], [4]. In each process, processing algorithms are implemented to obtain the output.

There are many types of algorithms used in the face recognition process. Based on previous research [5]–[7], this research then created a face recognition system using the Viola-Jones algorithm for face detection, Kanade-Lucas-Tomasi (KLT) for face tracking, and principal component analysis (PCA) for face recognition. Prior research used the Viola-Jones algorithm and compared the use of PCA and linear discriminant analysis (LDA) algorithms [5]. The results showed that PCA was better than LDA at a low number of database images.

According to the face recognition system created, securing the image data stored in the database during the training process is necessary to prevent misuse of face images, such as displaying them but not as original images. The process implemented in the security is encryption when storing images and the decryption process for the matching process during face recognition. Previous research performed face recognition with an image encryption scheme using XOR operations and pixel permutation with a randomization method. In addition, this research used LDA for the facial recognition algorithm [8]. This research showed that the proposed system only achieved an accuracy of 8.75%.

Securing image data by applying an image encryption algorithm to a face recognition system can utilize XOR and keys generated through randomization [9]. This study used red-green-blue (RGB) images in image processing, namely in the face recognition system and the image encryption process. The RGB model represents an image of primary colors red, green, and blue, represented by a pixel color vector value [10]. RGB takes longer to process than greyscale images, hence image processing calculations are significantly easier and faster when the RGB image is converted to greyscale [11], [12]. In addition, there is no pixel randomization process before the pixel values are changed.

Image encryption has two processes: confusion and diffusion [13]. Confusion is a process to perform permutation operations or randomization of pixels in the image, while diffusion is to perform substitution of image pixel values. Image encryption that only utilizes the confusion process is not considered secure enough because the attacker can still rearrange the pixels to obtain a plain image. Therefore, it is necessary to add a diffusion process to change the image's pixel values [13], [14].

Some researchers have combined the confusion process of 2D chaos systems and diffusion utilizing 1D chaos systems in image encryption. Prior study used the Arnold's cat map (ACM) chaos system for the confusion process [14]. In the diffusion process, a 1D logistic map chaos system was used to generate a keystream. Besides logistic maps, 1D chaos systems that can create keystreams are tent map and Bernoulli map [13], [15].

From the problems presented, this research implemented an image encryption scheme based on the confusion and diffusion process to secure the face recognition database. It utilized the 2D ACM chaos system in the confusion process. The diffusion process compared three chaos systems: logistic map, Bernoulli map, and tent map. All image processing was done in grayscale format to facilitate computation. This research produced a face recognition system with encrypted image data stored in the database.

This paper consists of four sections. Section I explains the introduction to the research and the proposed method. In Section II, related research that supports the preparation of this research is described, and then in Section III, the methodology is explained. Furthermore, in Section IV, testing and analysis of test results are presented. Conclusions are in Section V.

II. FACE RECOGNITION ENCRYPTION TREND

Several studies have been conducted on data encryption schemes for face recognition systems. Most of the proposed methods use chaos systems and pixel permutations. Research was conducted on secure surveillance mechanisms and lightweight probabilistic image keyframe encryption [16]. It used cosine transform-based chaotic sequence (CTC) to generate a pseudorandom number generator (PRNG) and confusion-diffusion operation for image keyframe encryption.

There has been several research on permutation [17], [18]. A study used the ACM which was combined with the Fibonacci series [17]. It utilized ACM to randomize plain images and modify field diffusion during the period of usability. Subsequent research utilized two pseudo-random grey values of generalized ACM and generalized Bernoulli shift map to increase resistance to statistical, differential, and chosen-plaintext attacks [18]. Research has shown that the proposed method has sufficient key space to prevent brute-force attacks.

Another research on image encryption used more than one chaotic system, which was called hybrid chaos [19]. These chaotic systems were 2D chaotic systems with Hénon maps, discrete-time dynamic systems, 2D chaos maps for pixel permutation, and chaos maps proposed by researchers using iteration functions. From the proposed research, chaos maps were proven to have excellent randomness with a relatively large parameter space, making them suitable for image encryption.

One of the image encryption methods that is widely used is XOR [20]–[23]. Prior research proposed a pixel randomization encryption scheme using Josephus traversing and pixel diffusion to increase the reliability of the encryption system [20]. The pixel permutation and diffusion process used the XOR operation. Furthermore, simulation results and security analysis showed that the scheme was proven to be reliable.

Prior research utilized ACM to randomize by permuting image pixels before encryption [21], [22]. After the tampering, the encryption process continued using the XOR operation with pseudorandom values generated from the Hénon map.

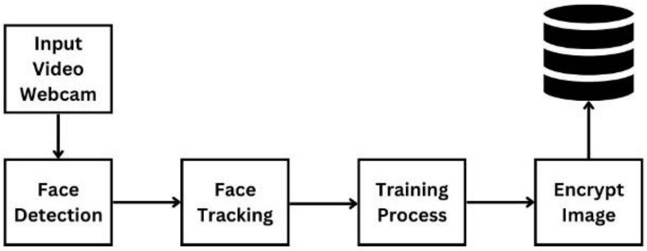


Figure 1. Face training process.

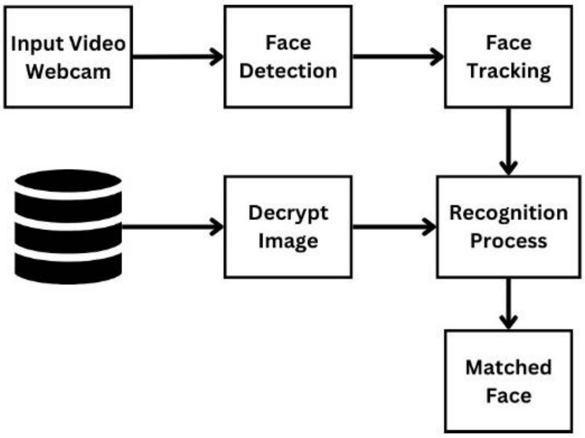


Figure 2. Face recognition process.

Research compared the peak noise to signal ratio (PNSR) values of four methods: ACM, Hénon map, ACM + Hénon map, and Hénon map + ACM [21]. It found that the best PNSR value was the method with ACM + Hénon map. This result indicates that ACM is able to carry out a good tampering process in the image encryption process.

The XOR method is generally used for symmetric cryptographic encryption. It has better security if it uses long random keys to avoid brute force attacks [23]. Therefore, in this research, the XOR operation was applied to encrypt mutated images using ACM. The XOR process in encryption and decryption was operated with a key or keystream generated from a chaos map, such as a tent map.

In other research, the tent map was used to create secret keys [24], [25]. The tent map was used to generate random numbers for the second key for image encryption in research [24], which was then underwent XOR operation with the image that was previously permuted using the Hénon map, and the key was generated using the orthogonal matrix method. In [25], the tent map was combined with the Bernoulli map to produce the second key, while the first key was generated from the 2D logistic sine map and linear congruential generator (LCG).

III. METHODOLOGY

Encryption of facial recognition system image data using confusion and diffusion processes is the main focus of this research. The facial recognition system used the Viola-Jones, KLT, and PCA algorithms. The primary processes of this system are training and the recognition process. Image data encryption involves confusion using ACM for pixel permutation. Another process is diffusion using XOR operations on pixels, which is possible using keystreams generated by the 1D chaos system. Furthermore, this research compared the encryption results with three different 1D chaotic systems in the diffusion process.

Figure 1 indicates the scheme when the face recognition system performs training or collects face images from the webcam video input. The training process obtained several face images after passing the face detection and face tracking stages. The system encrypted the collection of face images and stored them in the database as a datasheet for face recognition.

Figure 2 presents the scheme when the face recognition system performs the recognition process. The recognition process has the same stages as the training process: face detection and face tracking. These stages got a face image from the webcam video input, which was then matched with the datasheet in the database. Furthermore, the recognition process decrypted the face image from the database to get the original face image datasheet. This original face image datasheet was compared with the image from the webcam video input. Next, the matched face process determined whether the two images matched. If both pictures matched, the recognition process was successful. The system stages include face detection, face tracking, training process, RGB to grayscale, image encryption, and face recognition.

A. FACE DETECTION

In this research, the face detection stage used the Viola-Jones algorithm. This algorithm takes a part of the face marked with a yellow box. Using this algorithm, the system will detect the presence of faces from the webcam video as input.

Viola-Jones is an algorithm based on Haar features. Paul Viola and Michael Jones, the creators of this algorithm, poured their research into a paper. The contribution is to propose a face detection method with Haar features, integral image, AdaBoost, and cascade [26]. By using this algorithm, the face detection process is shorter.

B. FACE TRACKING

Face tracking is a stage for extracting unique facial features and tracking objects such as eyebrows, eyes, mouth, and facial outlines. The followings are the stages in the KLT algorithm [27].

1. Capturing the video sequence from the input file.
2. Extracting the features of the region of interest for face detection.
3. The current face image is tracked from the previous face image.
4. This tracker estimates the scale, rotation, and translation between the last and new points.

C. RGB TO GRAYSCSALE CONVERSION

Grayscale images are monochrome images or single-color images that contain only brightness information and no color information. Intensity representation of pixel values in the range between 0 and 1 (minimum and maximum) and between various ranges of gray ranging between 0 and 255 [10]. The initial stage of the RGB to grayscale conversion process is to get the three primary color values (red, green, and blue) and then encode them using gamma expansion with the following formula [10].

$$C_{linier} = \begin{cases} \frac{C_{rgb}}{12.92} & C_{rgb} \leq 0.04045 \\ \frac{(C_{rgb}+0.065)}{1.065} & C_{rgb} > 0.04045 \end{cases} \quad (1)$$

where C_{rgb} is the RGB primaries in the range 0 to 1, and C_{linier} is the intensity value in the field 0 to 1 with the conversion obtained using the $f(x)$ function. Function of $f(x)$ converts RGB values to grayscale values by summing the R, G, and B components [10].

Figure 3. Database of training process.

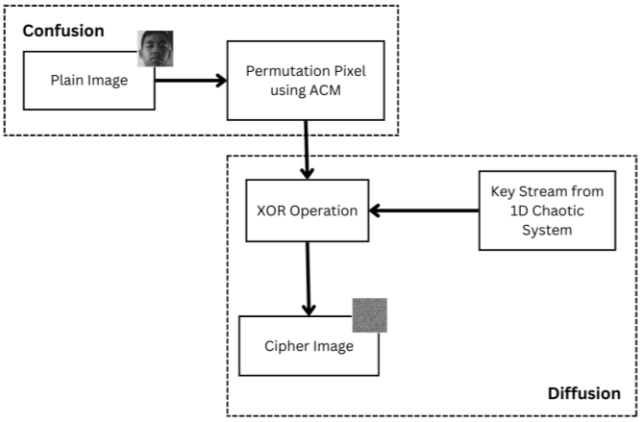

Confusion
Plain Image
Permutation Pixel using ACM
XOR Operation
Key Stream from 1D Chaotic System
Cipher Image
Diffusion

Figure 4. Schematic of encryption process.

$$y = f(x) \quad (2)$$

$$f(x) = 0.2989 * R + 0.5870 * G + 0.1140 * B. \quad (3)$$

D. TRAINING PROCESS

At this stage, the system took several images and stored them in the database. The training process was registering face images as a face recognition matching datasheet. The system took 20 images in each training process and stored them in one folder. Figure 3 shows an encrypted image stored in the database.

E. ENCRYPTION PROCESS

In this research, the encryption process was carried out on face images during training. The image encryption scheme consisted of a confusion process and a diffusion process. Figure 4 presents the face image encryption scheme.

1) CONFUSION

The confusion process was applied using the ACM. In the image confusion process using the ACM, the new image produced results from the permutation of each pixel's position in the image involving the ACM permutation transformation. Before the permutation, the image was first resized to 90×90 pixels because ACM can only be operated on images of size N×N. The new image size was stored in row and column dimension variables. The initialization determined the number of iterations and parameters a and b that was used in the ACM formula. In the program, the number of iterations was determined to be 5, with the value of a = 34 and b = 35. The values of a and b in the matrix $\begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}$ must produce determinants equal to 1 so that the transformation results were area-preserving. That is, they remain in the same image area [14]. The ACM equation to perform pixel permutation using the input pixel coordinates (X, Y) is as follows [14].

$$\begin{pmatrix} X_{i+1} \\ Y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} X_i \\ Y_i \end{pmatrix} mod\ (N). \quad (4)$$

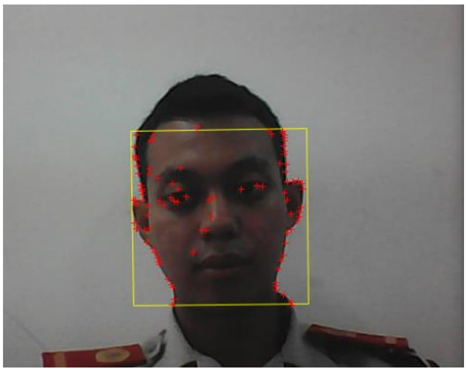


Figure 5. Video input using a webcam.

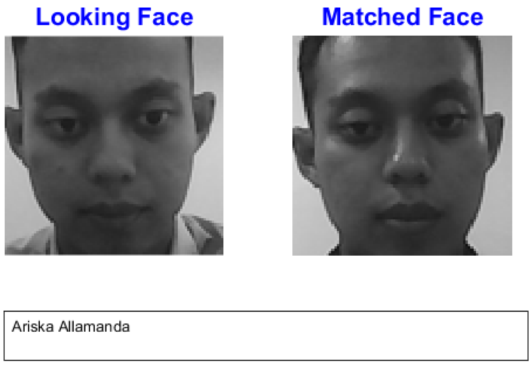


Figure 6. Matching result.

where (X_i, Y_i) is the pixel position in the image, and (X_{i+1}, Y_{i+1}) is the new pixel position after the ith iteration, a and b are arbitrary positive integers. Based on the formula above, iteration occurs for each image pixel and new coordinate calculations occur at each iteration.

2) DIFFUSION

The permutation results using ACM then underwent a diffusion process with pixel substitution, producing an image different from the initial image with pixel values $(p_1, p_2, \dots, p_{NxN})$. These values underwent XOR operation with the keystream generated by the 1D chaotic system. Three 1D chaos systems were compared for encryption results: logistic map (5), Bernoulli map (6), and tent map (7). Those maps can be used to generate a keystream (k),

$$k_{i+1} = rk_i\,(1 - k_i) \tag{5}$$

$$k_{i+1} = \begin{cases} sk_i, & 0 \leq k_i < 0.5 \\ sk_i - 1, & 0.5 < k_i \leq 1 \end{cases} \tag{6}$$

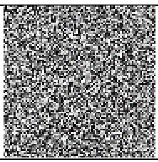
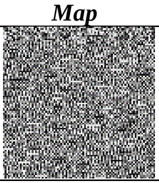
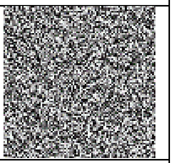
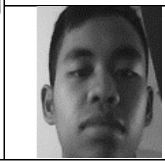
$$k_{i+1} = \begin{cases} tk_i, & 0 \leq k_i \leq \frac{1}{t} \\ \frac{t}{t-1}(1 - k_i), & \frac{1}{t} < k_i \leq 1 \end{cases} \tag{7}$$

where r, s, t are the parameter in positive real numbers. The value k_0 is determined as the initialization value for keystream generation, $r = 3.999$, s and t = 1.999. The general equation for the diffusion process with substitution is as follows.

$$c_j = \left(p_j \oplus c_{j-1}\right) \oplus k_j. \tag{8}$$

The initialization vector, c_0, is the first required pixel $(IV = 0)$. The produced random number must be changed into an integer between 0 and 255. The pixel value and keystream at the j-indexes, which are expressed as integers, underwent XOR operation —with an encrypted image of confused and diffused pixels. Section IV explains the test results obtained.

TABLE I
IMAGE ENCRYPTION RESULT

Plain Image	Encrypted Image		
	Logistic Map	*Bernoulli Map*	*Tent Map*
			
	Decrypted Image		
	Logistic Map	*Bernoulli Map*	*Tent Map*
			

IV. RESULT AND DISCUSSION

This system was created using the MATLAB mathematical programming application by integrating a webcam on the device. The results of the system included the results of the facial recognition process and the results of image encryption from the proposed scheme. Furthermore, testing on this system included face recognition and image encryption, taking several test parameters such as histogram, correlation graph, entropy, number of pixel rate changes (NPCR), and unified average change intensity (UACI).

A. FACE RECOGNITION

The system captured real-time images via webcam video input and stored them in a database. This process produced a database containing 100 images with five people as samples so that each person had a sample with 20 facial images. Image capture was carried out in real-time to match the data contained in the database, and the input face was converted to grayscale. Figure 5 indicates a face detection system via webcam video as input to be stored in a database and for face recognition. Hereafter, Figure 6 presents the matching process results between the captured image and the database image.

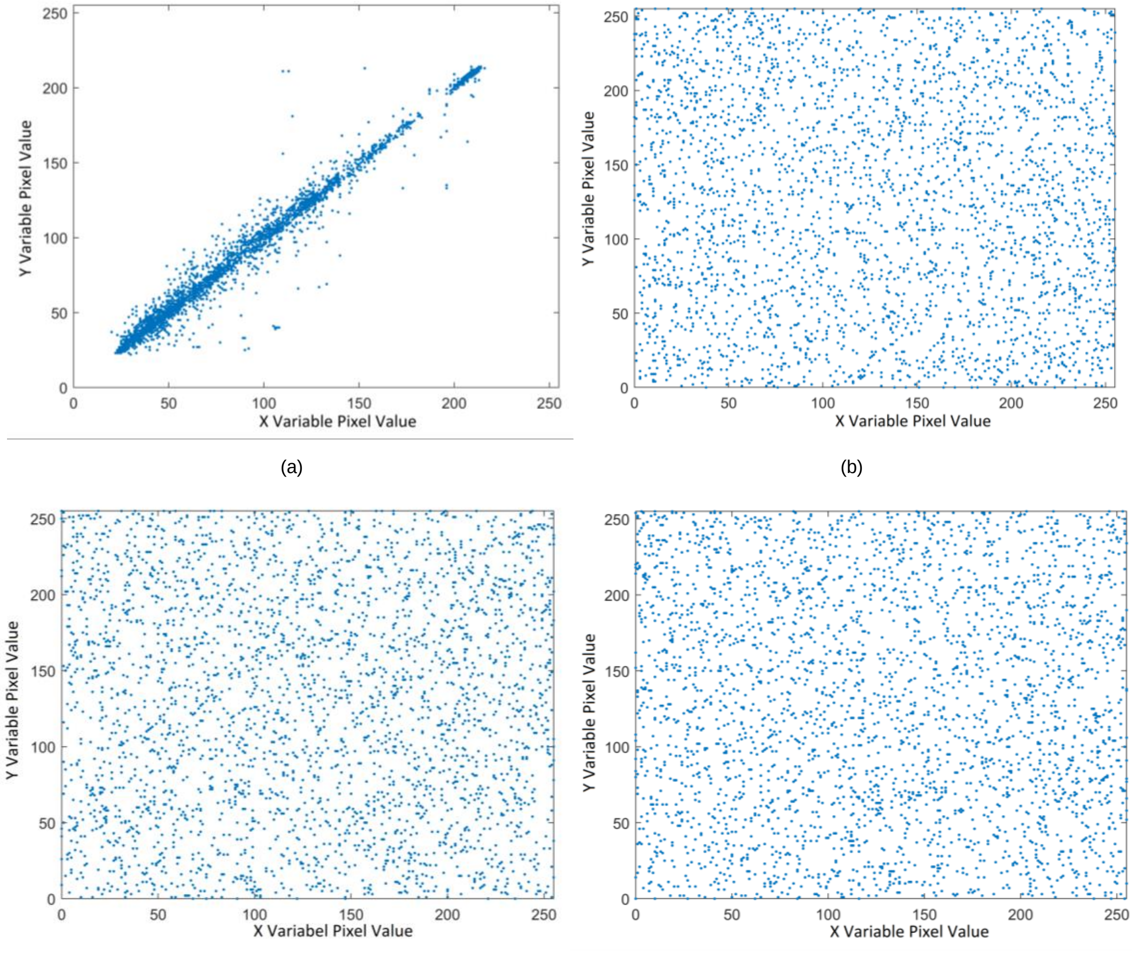
B. IMAGE ENCRYPTION

Encryption was performed during training, and the system stored the images in a database. Therefore, the images stored in the database were encrypted images. In this research, the encryption process used the ACM, and the diffusion used a 1D chaos system. The result of image permutation was an XOR operation with a keystream produced by one of the 1D chaos systems: logistic map, Bernoulli map, and tent map. Furthermore, the resulting encrypted images were compared with different keystream generation methods. The image encryption process for face recognition was carried out on five people. Table I shows the encryption results of one of the five people using ACM and 1D chaos systems.

Table I indicates the differences between the results of encrypted images with keystreams from different 1D chaos systems. Encryption using ACM and one of three 1D chaos systems produced random and irregular images. Therefore, it allowed to prevent brute force attacks on images.

1) CORRELATION COEFFICIENT GRAPH

The results of the correlation coefficient graph in Figure 7 show that the three keystream generation schemes in the



(a)

(b)

(c)

(d)

Figure 7. Correlation coefficient graph of (a) plain image, (b) logistic map, (c) Bernoulli map, and (d) tent map.

TABLE II
CORRELATION COEFFICIENT VALUE WITH LOGISTIC MAP KEYSTREAM

Image	Diagonal		Horizontal		Vertical	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0.9507	-0.0029	0.9199	-0.0027	0.9869	0.0117
II	0.9399	0.0052	0.9322	0.0122	0.9836	0.0122
III	0.8469	0.0132	0.8700	-0.0096	0.9287	0.0085
IV	0.9234	0.0086	0.9332	-0.0020	0.9739	-0.0096
V	0.9548	-0.0068	0.9463	0.0034	0.9863	0.0150

TABLE III
CORRELATION COEFFICIENT WITH BERNOULLI MAP KEYSTREAM

Image	Diagonal		Horizontal		Vertical	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0.9507	0.0067	0.9199	-0.3807	0.9869	-0.0090
II	0.9399	0.0047	0.9322	-0.7326	0.9836	-0.0059
III	0.8469	-0.0425	0.8700	-0.5813	0.9287	0.0289
IV	0.9234	0.0111	0.9332	-0.4356	0.9739	-0.0123
V	0.9548	-4.3672	0.9463	-0.4815	0.9863	-0.0060

TABLE IV
CORRELATION COEFFICIENT VALUE WITH TENT MAP KEYSTREAM

Image	Diagonal		Horizontal		Vertical	
	P(x)	*C(x)*	*P(x)*	*C(x)*	*P(x)*	*C(x)*
I	0.9507	0.0022	0.9199	-0.0024	0.9869	0.0137
II	0.9399	0.0102	0.9322	0.0278	0.9836	-0.0092
III	0.8469	-0.0118	0.8700	0.0017	0.9287	-0.0017
IV	0.9234	0.0131	0.9332	0.0104	0.9739	-0.0156
V	0.9548	0.0057	0.9463	0.0137	0.9863	0.0245

TABLE V
ENTROPY VALUE

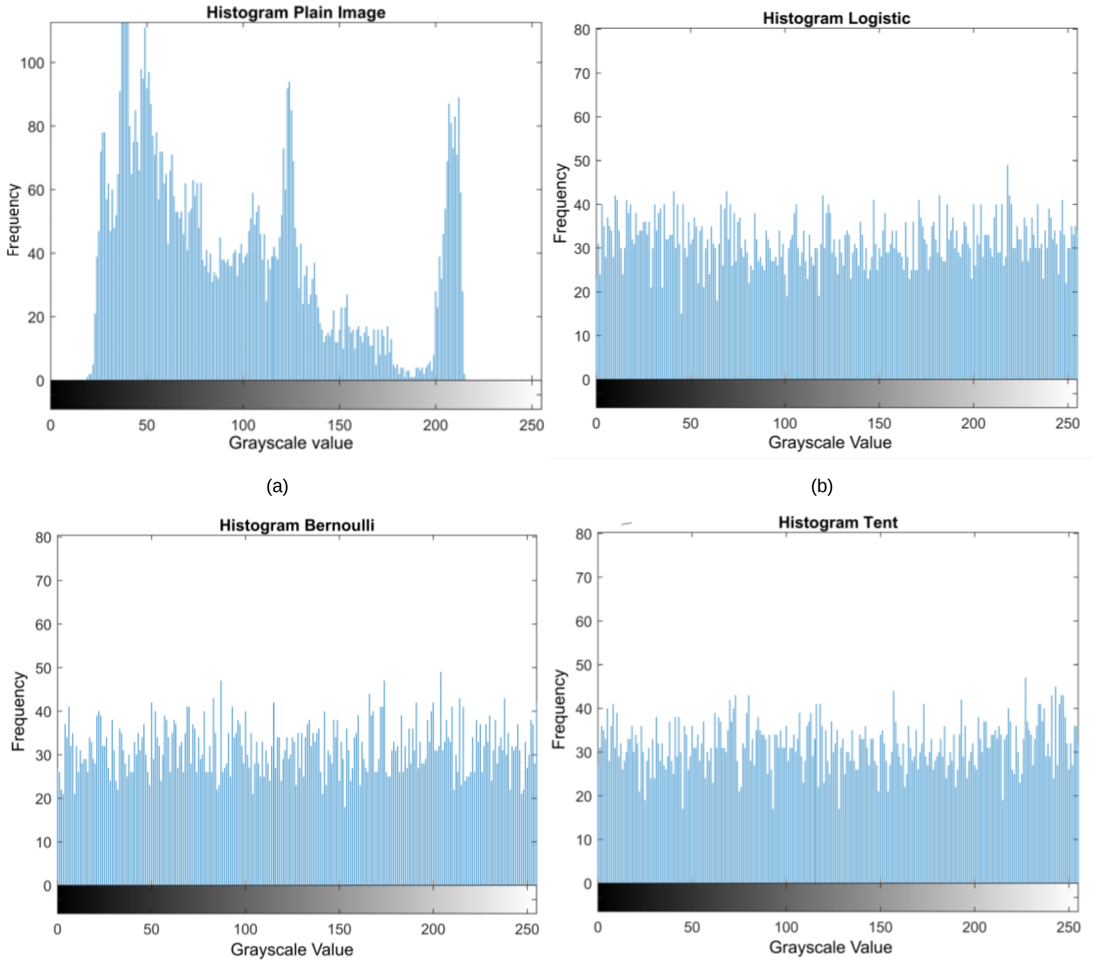
Image	Plain Image	Logistic Map	Bernoulli Map	Tent Map
I	7.2132	7.9778	7.9764	7.9793
II	5.8787	7.9789	7.9726	7.9795
III	6.6086	7.9731	7.9771	7.9782
IV	7.1905	7.9783	7.9782	7.9763
V	6.9445	7.9758	7.9774	7.9777

diffusion process produced a distributed distribution of blue dots, unlike the plain image, whose correlation graph was spread on a single line. There are dots with pixel values around the 45° diagonal line, indicating a strong correlation between the pixels. In contrast, the pixel values were evenly distributed in the encrypted image, so the pixels did not correlate.

In addition, the correlation between two variables can also be identified from the correlation coefficient value produced by an image. Plain images had a correlation coefficient value close to 1, while encrypted images closed to 0. Table II, Table III, and Table IV show the correlation coefficient values produced by all test images and images encrypted with a keystream scheme using several chaos functions.

2) ENTROPY ANALYSIS

In addition to the correlation coefficient, an information entropy value can measure the randomness of an image. The



(a)

(b)

(c)

(d)

Figure 8. Histogram results in (a) plain image, (b) logistic map, (c) Bernoulli map, (d) tent map.

TABLE VI
NPCR AND UACI VALUES

Image	NPCR			UACI		
	Logistic Map (%)	*Bernoulli Map (%)*	*Tent Map (%)*	*Logistic Map (%)*	*Bernoulli Map (%)*	*Tent Map (%)*
I	99.5556	99.5679	99.6173	31.6531	31.1214	31.4001
II	99.5556	99.6420	99.5185	36.4674	36.4076	36.8611
III	99.5802	99.5556	99.6543	30.5049	30.5465	30.2400
IV	99.6420	99.7037	99.6173	32.3277	32.6082	33.0326
V	99.6420	99.7901	99.5802	31.2585	30.9979	30.9502
Average	99.5951	99.6519	99.5975	32.4423	32.3363	32.4968

maximum entropy value that a greyscale image can generate is 8. When the resulting entropy value is close to 8, an image's pixel randomness level is high.

Table V presents that the three proposed schemes had good encryption strength. Entropy is one of the testing parameters of a cryptographic algorithm encryption result. Entropy analysis determines the power of the cryptosystem or the randomness of the execution results of the cryptographic algorithm program. Entropy is ideal if the value is close to 8, while for images that are not adequately scrambled have an entropy value far from 8. The cipher text or image cannot be predicted with a good entropy value.

In this research, an entropy test was conducted on plain images and encrypted images. It can be seen in Table V that the encrypted image value had a value close to 8, and the plain image had an entropy value far from 8. The keystream generated by the logistic map became an encryption scheme with an average entropy value of 7.97678. The average entropy value for the keystream generated by the tent map was 7.9782, and the Bernoulli map was 7.97634.

3) HISTOGRAM ANALYSIS

Histogram analysis is used to find information about the pixel value distribution of the plain and encrypted images. Excellent and robust encryption will produce a histogram with a more random or even distribution of pixel values in the pixel value space. The histogram of the encrypted and plain images will be different to prevent statistical attacks on the algorithm. Figure 8 indicates that the histogram produced by the plain image was uneven, and there was a lot of accumulation at specific values. The histogram of the encrypted image with the diffusion process using the keystream of the three types of 1D chaos systems proposed had an even distribution of lines, indicating that the encryption scheme was implemented to have good enough security in protecting the plain image.

4) NPCR AND UACI

NPCR and UACI are two standard parameters used to examine the effect of a single-pixel change on the entire image. NPCR focuses on the absolute number of pixels that change in value in the differential attack, while UACI focuses on the average difference between the two images being compared. In general, the following equation is used to calculate the NPCR value.

$$\text{NPCR}\ (L_1, L_2) = \frac{\sum_{\text{m,n}} D(\text{m,n})}{W\ x\ H} \times 100\% \qquad (9)$$

where W and H are the width and height of encrypted images, L_1 and L_2. $D(\text{m, n})$ represents the pixel correspondence value between L_1 and L_2. NPCR calculates how many pixels have changed in value between the two encrypted images. In comparison, UACI measures the average difference in pixel values between the two images or, more accurately called, their intensity. The equation for obtaining the UACI value can be defined as follows.

$$\text{UACI} = (L_1, L_2) = \frac{1}{W\ x\ H}\left[\sum_{\text{m,n}} \frac{L_1(\text{m,n}) - L_2(\text{m,n})}{255}\right] \times 100\%. \qquad (10)$$

A high NPCR value indicates that the encryption algorithm causes many changes in the image pixels, and a high UACI means the intensity of the encrypted image with the plain image.

Table VI shows that the NPCR values of five sample images encrypted with the three proposed encryption schemes were close to 100%, indicating that there was a significant change in the pixels of the plain image with the encrypted image. Meanwhile, the UACI value was around 30%, meaning a change in intensity between the plain image and the encrypted image.

V. CONCLUSION

This research shows that using an encryption algorithm on images using keystreams from a 1D chaos system in a face recognition system has increased the security and privacy of image data. The correlation coefficient of evenly distributed points in all types of 1D chaos systems shows the effectiveness in minimizing the dependency between pixels in the image. It indicates that all types of 1D chaos systems produce keystreams with a relatively high level of randomness with evenly distributed histograms. Based on the entropy analysis, the tent map became the keystream for the diffusion process with the highest entropy value of 7.9782. The NPCR analysis of the third keystream of the 1D chaos system was close to 100%, indicating a significant change between the plain and encrypted images. Moreover, the UACI value of around 30% indicates a change in intensity between the plain image and the encrypted image. These two metrics confirm that the encryption algorithm successfully achieves a significant degree of change in the encrypted image, which is an essential characteristic of a good encryption algorithm. Thus, the most robust algorithm used the tent map as the keystream generator. Overall, this study shows that using a 1D chaos system in the image encryption algorithm of a face recognition system can produce visually complex encrypted images while still maintaining face recognition capabilities and can improve data security.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

AUTHORS' CONTRIBUTIONS

Conceptualization, Magfirawaty; methodology, Magfirawaty; software, Ariska Allamanda and Malika Ayunasari; validation, Muhamad Nadhif Zulfikar; formal analysis, Malika Ayunasari; investigation, Ariska Allamanda; resources, Muhamad Nadhif Zulfikar; data curation, Malika Ayunasari; writing, Ariska Allamanda and Malika Ayunasari; supervision, Magfirawaty; funding acquisition, Magfirawaty.

REFERENCES

[1] Q. Xiao, "Technology review - Biometrics-technology, application, challenge, and computational intelligence solution," *IEEE Comput. Intell. Mag.*, vol. 2, no. 2, pp. 5–10, May 2007, doi: 10.1109/MCI.2007.353415.

[2] M.S. Obaidat, I. Traore, and I. Woungang, *Biometric-Based Physical and Cybersecurity Systems.* Cham, Switzerland: Springer, 2018.

[3] F. Gong, Y.M. Zhang, and X.Z. Jiang, "Application research of face recognition algorithm based on MATLAB," *J. Phys., Conf. Ser.*, vol. 2290, pp. 1–6, Jun. 2022, doi: 10.1088/1742-6596/2290/1/012102.

[4] L.A. Ibrahim, Nasser, and M. Ali, "Face recognition based on statistical texture features," *Embedded Selforganising Syst.*, vol. 7, no. 1, pp. 10–15, Feb. 2020, doi: 10.14464/ess.v7i1.471.

[5] U. Jain, K. Choudhary, S. Gupta, and M.J.P. Privadarsini, "Analysis of face detection and recognition algorithms using Viola Jones algorithm with PCA and LDA," *2018. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, 2018, pp. 945–950, doi: 10.1109/ICOEI.2018.8553811.

[6] L. Liying and H. Yue, "Study on access control system based on face recognition," *2008 Int. Conf. Comput. Sci. Softw. Eng.*, 2008, pp. 876–878, doi: 10.1109/CSSE.2008.451.

[7] R. Boda and M.J.P. Priyadarsini, "Face detection and tracking using KLT and Viola Jones," *ARPN J. Eng. Appl. Sci.*, vol. 11, no. 23, pp. 13472–13476, Dec. 2016.

[8] E. Abusham, B. Ibrahim, K. Zia, and M. Rehman, "Facial image encryption for secure face recognition system," *Electron.*, vol. 12, no. 3, pp. 1–26, Feb. 2023, doi: 10.3390/electronics12030774.

[9] M. Magfirawaty *et al.*, "Principal component analysis and data encryption model for face recognition system," *2022 2nd Int. Conf. Electron. Electr. Eng. Intell. Syst. (ICE3IS)*, 2022, pp. 381–386, doi: 10.1109/ICE3IS56585.2022.10010080.

[10] K. Padmavathi and K. Thangadurai, "Implementation of RGB and grayscale images in plant leaves disease detection - Comparative study," *Indian J. Sci. Technol.*, vol. 9, no. 6, pp. 1–6, Feb. 2016, doi: 10.17485/ijst/2016/v9i6/77739.

[11] M. Gao and T.-F. Lu, "Image processing and analysis for autonomous grapevine pruning," *2006 Int. Conf. Mechatronics Autom.*, 2006, pp. 922–927, doi: 10.1109/ICMA.2006.257748.

[12] V. Goel, S. Singhal, T. Jain, and S. Kole, "Specific color detection in images using RGB modelling in MATLAB," *Int. J. Comput. Appl.*, vol. 161, no. 8, pp. 38–42, Mar. 2017, doi: 10.5120/ijca2017913254.

[13] P.S. Sneha, S. Sankar, and A.S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, pp. 1289–1308, Mar. 2020, doi: 10.1007/s12652-019-01385-0.

[14] R. Munir, "Algoritma enkripsi citra digital berbasis chaos dengan penggabungan teknik permutasi dan teknik substitusi menggunakan Arnold cat map dan logistic map," *J. Nas. Pendidik. Tek. Inform., JANAPATI*, vol. 1, no. 3, pp. 166–181, Dec. 2012, doi: 10.23887/janapati.v1i3.9814.

[15] 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*, vol. 21, no. 5, pp. 1–23, May 2019, doi: 10.3390/e21050504.

[16] J. Khan *et al.*, "SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption," *IEEE Access*, vol. 8, pp. 15747–15767, Jan. 2020, doi: 10.1109/ACCESS.2020.2966656.

[17] D. Elmaci and N.B. Catak, "An efficient image encryption algorithm for the period of Arnold's cat map," *Int. J. Intell. Syst. Appl. Eng.*, vol. 6, no. 1, pp. 80–84, Jan.-Mar. 2018, doi: 10.18201/ijisae.2018637935.

[18] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Commun.*, vol. 284, no. 22, pp. 5290–5298, Oct. 2011, doi: 10.1016/j.optcom.2011.07.070.

[19] A.P. Kari, A.H. Navin, A.M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2753–2772, Jan. 2021, doi: 10.1007/s11042-020-09648-1.

[20] Y. Niu and X. Zhang, "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation," *IEEE Access*, vol. 8, pp. 22082–22093, Jan. 2020, doi: 10.1109/ACCESS.2020.2970103.

[21] C. Irawan and E.H. Rachmawanto, "Implementasi kriptografi dengan menggunakan algoritma Arnold's cat map dan Henon map," *J. Masy. Inform.*, vol. 13, no. 1, pp. 15–32, May 2022, doi: 10.14710/jmasif.13.1.43312.

[22] P. Sankhe, S. Pimple, S. Singh, and A. Lahane, "An image cryptography using Henon map and Arnold cat map," *Int. Res. J. Eng. Technol.,* vol. 5, no. 4, pp. 1900–1904, Apr. 2018.

[23] M. Tang, G. Zeng, Y. Yang, and J. Chen, "A hyperchaotic image encryption scheme based on the triple dislocation of the Liu and Lorenz system," *Optik*, vol. 261, pp. 1–22, Jul. 2022, doi: 10.1016/j.ijleo.2022.169133.

[24] S. Kanwal *et al.*, "An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices," *Sensors*, vol. 22, no. 12, pp. 1–17, Jun. 2022, doi: 10.3390/s22124359.

[25] W. Alexan *et al.*, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11541–11554, Feb. 2023, doi: 10.1109/ACCESS.2023.3242311.

[26] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proc. 2001 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR 2001)*, 2001, pp. I-511–I-518, doi: 10.1109/CVPR.2001.990517.

[27] N.H. Barnouti, M.H.N. Al-Mayyahi, and S.S.M. Al-Dabbagh, "Real-time face tracking and recognition system using Kanade-Lucas-Tomasi and two-dimensional principal component analysis," *2018 Int. Conf. Adv. Sci. Eng. (ICOASE)*, 2018, pp. 24–29, 2018, doi: 10.1109/ICOASE.2018.8548818.