Information Sciences Letters

Volume 11
Issue 6 *Nov. 2022*

Article 27

2022

Video Encryption Technique Based on Hybrid Chaotic Maps and Multi- Operation keys

Mohamed. Heshmat
Faculty of Computer Science and Artificial intelligence, Sohag University, Sohag, Egypt,
heshmat@fci.sohag.edu.eg

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/110627

Video Encryption Technique Based on Hybrid Chaotic Maps and Multi-Operation keys

Mohamed. Heshmat

Faculty of Computer Science and Artificial intelligence, Sohag University, Sohag, Egypt

Received: 21 Mar. 2022, Revised: 22 Jun. 2022, Accepted: 24 Jul. 2022.
Published online: 1 Nov. 2022.

Abstract: During these critical times of the pandemic, a reliable and fast encryption technique for encrypting medical data for patients is a critical topic to consider. This epidemic forced governments and health care organizations to observe patients of COVID-19. The idea of encryption video is gaining in popularity, because of the growing use of communication technology like video conferencing to conclude corporate meetings and presentations. Video data sent back and forth between sender and recipient must also use the unsecured communication medium available, the internet. This paper proposed a way to encrypt video by using hybrid schemes, which used the advantage of both henon, elliptic curve, and logistic. The proposed method achieved significantly improved results. Simulations results are performed to gauge the efficacy of the presented method.

Keywords: COVID-19, Henon, Image encryption, Improve Logistic, MRI images, Video encryption.

1 Introduction

The patients' health record [1] is kept in a database or clouds. It can be available on the internet, by researchers, physicians, healthcare institutes, and insurance specialists, especially during the COVID-19 pandemic. These records [2] include personal and medical data that attract the phishing for stealing them. Moreover, keeping them secure may face many risks. For example, a hacker may employ data mining methods to obtain them while also storing these records in a local data store, or system administrators may use clouds to sell the patients' data [3].

In any event, there are serious worries about the safety and security of these records. Portable applications are used by governments and healthcare organizations to track COVID 19 patients and control the spread of the pandemic. Such applications are exceptionally noteworthy, but there must be a law to guarantee the protection of patients, keeping money nuances, shopping records, and so on. Governments are forced to use an encryption system to secure and guarantee patients' privacy during these critical times. So far, encryption systems are the most commonly used procedures to protect such accurate data from being transmitted. Current developments in the field of communication have led to an increase in the transmission of images and videos across the public network, as well as the dramatic development of social media, which has led to the sharing of Images and videos on the Internet frequently. Due to the intensification of sharing digital images and videos, a focus on safety has become very important, when transferring data over any network. The method called encryption guarantees this. Different encryption strategies are accessible [4-12], and the traditional systems utilized to data encrypt and decrypt are the data encryption standard. Advanced encryption standard and international data encryption algorithm.

For video encryption, a variety of techniques and algorithms are available. By dividing the video file into different sets of frames, applying the method to each frame, aggregating the results of each, and grouping them into a single encrypted video file, symmetric algorithms use a single key for both encoding and decrypting the video file. Asymmetric algorithms encrypt and decrypt using two separate keys. The encoding stage uses only one key, while the decoding stage uses various keys.

Authors at [5] proposed a technique for video encryption, which is thoroughly key independent and fast. They used two different types of video formats, one is compressed, and the other one is uncompressed of different frame sizes and an almost similar number of video frames. Ref. [6] presented a method that used the advantage of both the asymmetric and symmetric techniques by proposed encryption hybrid method, leading to a more secure and faster alternative of video encryption. Sha-ShaYu et al. [7] provided a method for dividing a plain image into four sub-images that can be encoded individually. This method trusted stage truncated short time hyper-chaotic system and the fractional fourier transform. Authors at [8] introduced

*Corresponding author e-mail: heshmat@fci.sohag.edu.eg

an image encryption method, which used maps of 1 dimensional chaotic. Also, it employed undergoes a single round and permutation diffusion structure for video frames encryption. Authors at [9] introduced an encrypted system by three-level security depending on video encryption chaos. The presented encryption technique utilizes a diffusion structure and 1 round permutation. To generate the initial parameters, they combined tent and logistic maps for the proposed encryption method. First, the video outline/frame is chosen to depend on encrypting the outline determination by applying for permutation order. After that on the permuted frame executed the diffusion by generating a diffusion frame. Experimental analyses and results emphasize that the technique is competent. Huang Zhi-Jing et al. [10] presented a method that supported 2D linear canonical transform and chaotic system.

Many of the current methods [13] [14] to provide security for video data are mainly based on a large signal processing algorithm, when implementing encryption takes a long time and consumes a lot of bandwidth, resulting in connection slowness. No single encryption computation is secure enough to deliver perfectly clean and lossless data.

The disadvantage of henon, logistic and elliptic curve map, is easy crack for encrypted image, moreover, the chaotic high dimension is hard implementation and takes a long time to compute. A unique technique to enhance chaotic properties is proposed. The proposed cryptographic technique utilized a hybrid method to encrypt video, where it used the advantage of both henon, elliptic curve, and logistic. The improved logistic map histogram is more uniform than a logistic map histogram, so it will be utilized to create a secret key for the presented method.

The rest of the paper is organized as follows. Preliminary will be discussed in Section 2. An improved coding algorithm is suggested in Section 3. Confirm the performance analysis in Sections 4. In Section 5, it will be indicated how to improve the performance of the presented method.

2 Preliminary

In this section, three main methods which are used in our proposed method are explained.

Henon Map, Logistic Map, Elliptic Curve and Permutation technique

- *Henon map* showed an excellent interesting characteristic when it was studied [15]. The henon map is fundamentally a functions group realized from R_2 to R_2 and denoted by:

$$H_{\alpha\beta}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}1-\alpha x^2+y\\ \beta x\end{pmatrix} (1)$$

which α and β ϵ R are the set of real numbers. As an entire, this map group is occasionally performed by the letter H also is observed collectively as just the henon map. Ordinarily, α and β are not equal to zero, thus that the map is often 2 dimensional. If α is equal to zero, then it reduces to α 1-dimensional logistic equation. By plotting points, it is often seen that H is simply a more generalized variety of another group of functions of the form:

$$Fc(x)=1-cx_2 \quad (2)$$

Where c is a constant value. Therefore, one may check the henon map graph as being like to a sideways parabola opening to the left, with its vertex somewhere on the x-axis close to (0,1) in general.

- ***Improve logistic map***

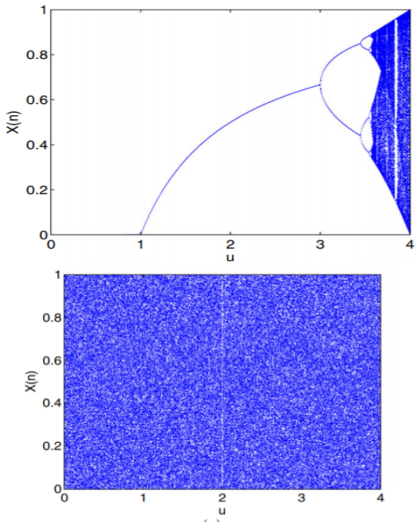
Logistic map could be an exceptionally direct chaotic outline and calculated [16] in the following,

$$x_{n+1} = ux_n(1-x_n) \ (3)$$

in biology it is used to pattern how a population x_n variances with the seasons (integer numbers n is a time), the initial condition is x_1, $3.99465 \leq u \leq 4$, and the control parameter is u. The improved logistic map [17] is defined according to equation (4)

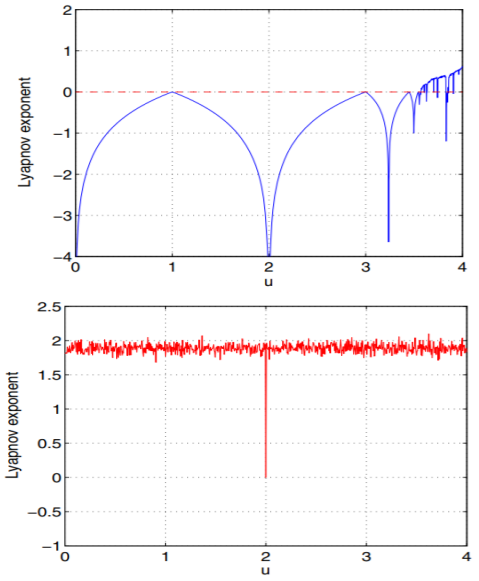
$$\begin{cases} x_{n+1} = L(n,x_n)G(k) - \text{floor}(L(n,x_n)G(k)) \\ L(n,x_n) = ux_n(1-x_n) \\ G(k) = 2^k, k \in Z^+, k \geq 8 \end{cases}$$

When $3.99465 \leq u \leq 4$, the chaotic attitude is explored by the improved logistic map. The bifurcation diagram and lyapunov exponent diagram are shown in fig. 1 and fig. 2 respectively. From the fig. 2, the positive lyapunov exponent result indicates that the system has chaotic behavior; also, a large lyapunov exponent indicates a higher sensitivity.



a , b

Fig. 1: The bifurcation diagram of the a) logistic map and b) improved logistic map.



a, b

Fig. 2: The lyapunov exponent diagram of the a) logistic map and b) improved logistic map.

- *Elliptic Curve*, F^2m is a finite binary field, and it may be declared like a dimension m for vector space over the field F^2. A non-super singular elliptic curve E is defined with mathematical formula as in equation:

$$y_2 + x\,y = x_3 + g_1x_2 + g_2 \quad (5)$$

Where $g_1, g_2 \in F^2m$ with $g_2 \neq 0$. All the points (x, y), $x \in F^2m$ and $y \in F^2m$ [18] are found in the obtained points E (F^2m) set.

- *Permutation Technique*

This technique is utilized to develop/construct a cipher frame. Permutation utilizes the plain image pixels but rearranges their order. We will encipher the image/frame utilizing a change that divides the image into 8 blocks, at that point convert each block from decimal to binary after that make scrambling, then convert from binary to decimal, as appeared in fig. 3.

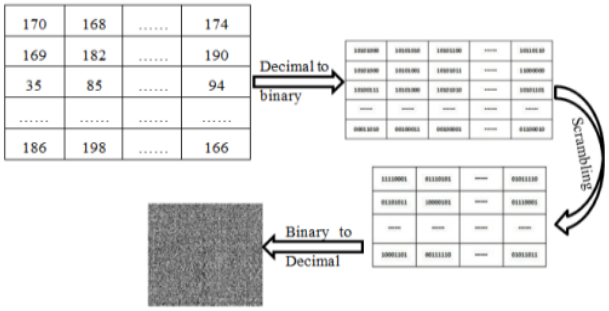


Fig.3: The permutation technique

- *The suggested method's theoretical analysis*

The Lyapunov exponent (LE) is used to evaluate the chaotic behavior of the suggested approach in order to theoretically analyze its effectiveness. Higher positive LE values are associated with good chaotic behavior. In this section, we provide a proof analysis of the chaotic behavior of HE structures. (combine of Henon and Elliptic curve maps). The HEL structure (combine of Henon, Elliptic curve, and logistic maps) is similar.

Suppose x_0, y_0 are two initial values with a too little difference between them. Additionally, x_1, y_1 represent the following iteration of x_0 and y_0. H(x), E(x) are Henon and Elliptic maps respectively. We have:

$$|x_1 - y_1| = \frac{|H(E(x_0)) - H(E(y_0))|}{|H(x_0) - H(y_0)|}\frac{|H(x_0) - H(y_0)|}{|x_0 - y_0|}$$

If $x_0 \rightarrow y_0$ then $H(x_0) \rightarrow H(y_0)$ and we have:

$$\left|\frac{d(H)}{dx}\right|_{H(x_0)} \approx \lim_{H(x_0)-H(y_0)} \frac{|H(E(x_0)) - H(E(y_0))|}{|H(x_0) - H(y_0)|},$$

$$\left|\frac{d(E)}{dx}\right|_{x_0} \approx \lim_{x_0-y_0} \frac{|E(x_0) - E(y_0)|}{|x_0 - y_0|},$$

Now we have:

After n iterations, we get the following result.:

$$|x_1 - y_1| \approx \left(\left|\frac{d(H)}{dx}\right|_{H(x_0)}\right)\left|\left|\frac{d(E)}{dx}\right|_{x_0}\right)|x_0 - y_0|$$

$$\Delta P(x) \approx \left(\left|\prod_{i=0}^{n-1}\frac{d(H)}{dx}\right|_{d(E(x_i))}\right)\left|\left|\prod_{i=0}^{n-1}\frac{d(E)}{dx}\right|_{x_i}\right)^{\frac{1}{n}}$$

Let $\Delta P(x)$is the average change in each iteration from $|x_1 - y_1|$ to $|x_n - y_n|$ we have:

According to the definition of Lyapunov export (LE), the LE of P(x) can be calculated as follows:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left(\left|\frac{d(H)}{dx}\right|_{d(E(x_i))}\right) + \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left(\left|\frac{d(E)}{dx}\right|_{x_i}\right) =$$

$$\lambda_{P(x)} = \ln(\Delta P(x)) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left(\left|\frac{d(H)}{dx}\right|_{d(E(x_i))}\left|\frac{d(E)}{dx}\right|_{x_i}\right) =$$

$$\lambda_{H(x)} + \lambda_{E(x)}$$

Where $\lambda_{H(x)}$and $\lambda_{E(x)}$ are Lyapunov export of H(x) (Henon map) and E(x) (Elliptic curve). We already know that a positive HE with a higher value has greater chaotic performance, so $\lambda_{H(x)}$ and $\lambda_{E(x)}$must be a positive number, and it is clear that $\lambda_{P(x)} \geq \lambda_{H(x)}$ and $\lambda_{P(x)} \geq \lambda_{E(x)}$. Consequently, we showed that the structure with a combination of Henon map and Elliptic curve (HE system) has a high chaotic range, rather than Henon map and Elliptic curve alone.

3 Proposed Method

In this section, the encryption scheme for video frames is proposed. We read the video frame in the beginning and the Henon map is used to get a henon key, then XORed the video frame with the henon key, then, with the result, use the permutation approach to get the cipher frame; this step is called henon encryption (HE). The result is XORed with the key EC (Elliptic Curve), then uses permutation to generate the second encryption frame; this step is called henon-elliptic encryption (HEE). One more time the XORed results with improved Logistic map key produced by improved Logistic, the permutation method is then applied to the result to get the final cipher frame. The final ciphered video frame is called henon-elliptic-logistic encryption (HELE). After encryption, we used the cipher frame to form transmission video sequence, as shown in fig. 4.

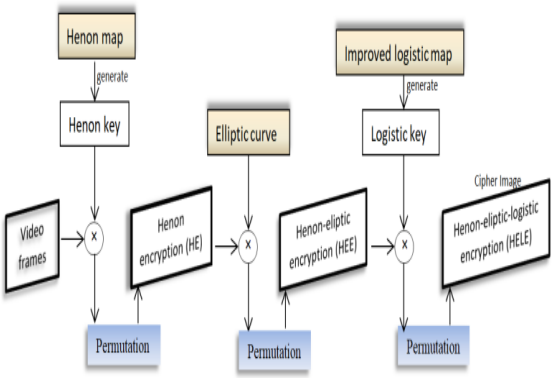


Fig. 4: The proposed video encryption method.

Algorithm for the proposed method

Step 1: Read video frames.
Step 2: Utilize a Henon map to generate the henon key.
Step 3: Apply operation of XOR among the plain video frame and henon key to generate cipher video frame, then applied permutation method; this step is called henon encryption (HE).
Step 4: Use HE video frame as a key and XORed with the elliptic curve, then apply permutation method; this step is called henon-elliptic encryption (HEE).
Step 5: Use an improved logistic map to generate a logistic key.
Step 6: Apply XOR operation between the HEE video frame and the logistic key to generate an encrypted video frame; this step is called henon-elliptic-logistic encryption (HELE).

Motivation: the first motivation, we presented to use a hybrid chaotic system. Which logistic, henon, and the encryption effect will be harmed by elliptic curve maps, making encryption images easier to crack. Hence, have limitations of chaotic performance. Furthermore, high-dimensional chaotic maps are difficult to implement and have a large computing cost. The second motivation is to be more efficient and reduce time complexity.

4 Result analysis

In our experiments, two types of experiments are executed, one for different standard video sequences as "CLAIRE", "MTHR_DOTR", "FOREMAN" and "car" are used to analyze the execution of the presented encryption scheme. Each video sequence contains 100 frames. The other kind is for a single video frame, the grayscale SIPI Miscellaneous data set [19] are Lena and Baboon. Different COVID-19 image/video dataset as e1, e2, e3 and coim with size 256×256 are used [20]. Different security test measures are applied to demonstrate the performance of the presented scheme. We used different measures as follows: key map analysis, for image data entropy performance, statistical analysis, security checks, such as measuring the number of pixel change rates (NPCR) and unified average changing intensity (UACI), and histogram analysis and computing the peak signal-to-noise ratio (PSNR). The following is an analysis of the proposed scheme's performance:

- *Histogram Analysis*

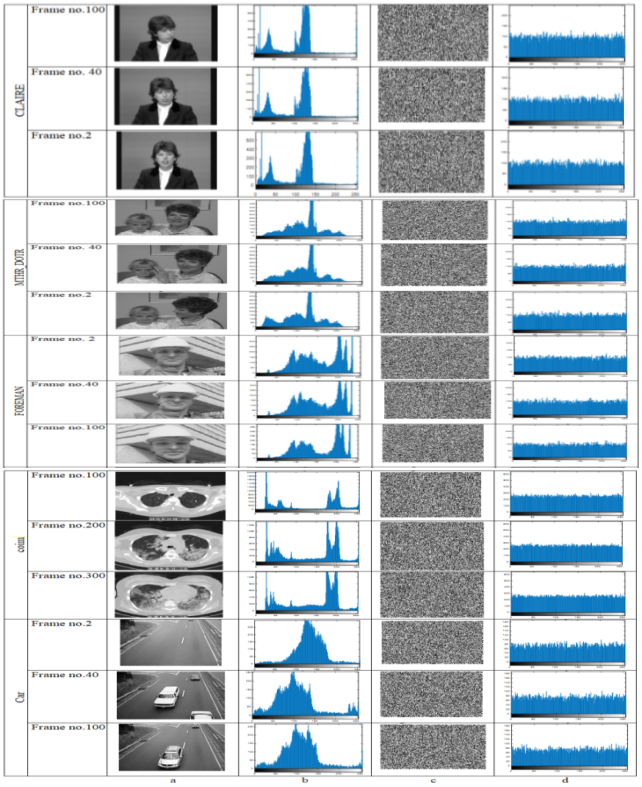


Fig. 5: a) Original video frames, b) Original video Histogram, c) HELE video frame, d) HELE histogram for video frames of the proposed method.

To avoid data loss, make sure the cipher frame has no statistical similarities to the plain frame. A good algorithm of video encryption must generate an encrypted frame of a

unique histogram all the time for any plain frame. During this step, the histograms are plotted for grayscale plain and ciphered frames. The histograms of the ciphered frame possessed a unique level distribution and good balancing property, as shown in fig. 5(a – d). The statistical advantage of the plain frame is improved in such a way that the cipher frames are significantly various and fairly unique about plain frames. Also, the original and encrypted histograms are different as proven in fig. 6(a-b). From the outcomes of histograms analysis, we can conclude that the presented method can resist statistical attacks.

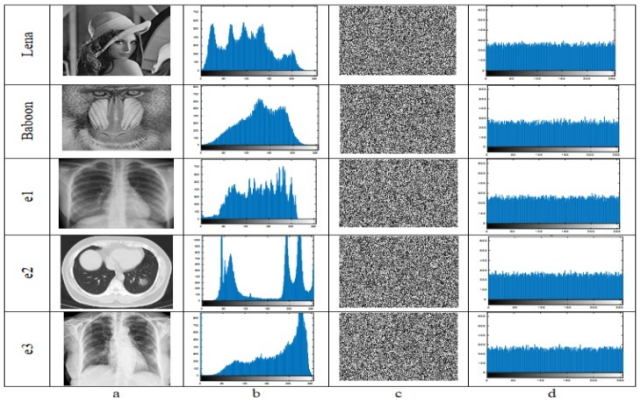


Fig. 6: a) Original images, b) Original image histogram, c) HELE image, d) HELE histogram of the proposed method.

- *Entropy Analysis*

To point out the degree of uncertainties inside the system the entropy is employed. The entropy (n) of a message source n can be computed as:

$$H(n) = -\sum_{i=0}^{255} P(n_i)\log_2 P(n_i) \quad (6)$$

which P(ni) is the probability of ni. The occurrence number of every grayscale recorded, as well as the occurrence probability for video frames, are computed for all supplied cipher frames in table 1. We discovered that the entropy of cipher frames is very close to eight, indicating that all of the pixels in the ciphered frames occur with almost equal probability. As a result, the presented encryption technique has a low data loss and is secure against entropy-based attacks.

Table 1: Entropy values for video frames.

	Video	Frame number	Original frame	HE	HEE	HELE
The Proposed method	CLAIRE	2	6.4085	7.9322	7.9929	7.9932
		40	6.3697	7.9332	7.9927	7.9933
		100	6.3377	7.9264	7.9934	7.9925
	R – D	2	7.0476	7.9488	7.9928	7.9926
		40	6.8852	7.9472	7.9928	7.9930
		100	6.8827	7.9424	7.9926	7.9927
	FOREMAN	2	7.2882	7.9581	7.9930	7.9932
		40	7.3212	7.9640	7.9923	7.9916
		100	7.1417	7.9399	7.9924	7.9923
	coim	100	6.31528	7.8892	7.99711	7.9970
		200	6.91445	7.9522	7.99691	7.9973
		300	7.0086	7.94946	7.99729	7.9971
	Car	2	7.0297	7.97264	7.9917	7.9897
		40	7.4173	7.95926	7.99166	7.9896
		100	7.3145	7.9608	7.990002	7.9907
	Lena	1	7.58079	7.97840	7.99728	7.99719
	Baboon	1	7.389	7.9922	7.9971	7.9971
	e1	1	7.4716	7.9943	7.9975	7.9971
	e2	1	6.9780	7.9655	7.9967	7.9972
	e3	1	7.45094	7.954963	7.99719	7.9969

PSNR

The peak signal to noise ratio is known as PSNR. which is computed by the equation in [21], [22] is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (7)$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (8)$$

Where MAX_f is the maximum value that exists in the original image, f original image, g encrypted image, and MSE the mean squared error. The low value of PSNR, as shown in Table 2, confirms that the proposed method obtains the best rate of flatness in the encrypted data histogram value and uniform histogram

Table 2: Average PSNR values of video frames.

	Video	Average PSNR
The Proposed method	CLAIRE	28.769
	MTHR_DOTR	27.919
	FOREMAN	26.476
	coim	27.467
	Car	27.611
	Lena	28.68
	Baboon	27.40
	e1	27.43
	e2	26.70
	e3	26.06

- *Correlation Analysis*

Every two consecutive pixels in a simple frame are known to be significantly correlated vertically, horizontally, and diagonally. Those might be characteristics of any normal frame. The correlation coefficient test has a maximum value of 1 and a minimum value of 0. The correlation coefficient value of a robust video frames encryption method against a statistical attack could have ~ 0. Table 3 shows the findings of horizontal, vertical, and diagonal directions for various video frames. The acquired results showed that there is a tiny correlation value between the two consecutive pixels within the cipher frame, as seen in fig. 7.

Table 3: Correlation coefficient for video frames.

	Video	Frame Number	Horizontal	Vertical	Diagonal
The Proposed method	CLAIRE	2	-0.00133	-0.004619	-0.00296
		40	-0.00153	0.000638	0.00208
		100	0.004846	0.011737	0.002027
	MTHR_ DOTR	2	-0.001338	-0.00676	-0.00126
		40	0.008979	-0.001263	0.009859
		100	0.000021	0.002340	0.002934
	FORE MAN	2	0.005617	0.007869	0.009724
		40	-0.01029	-0.002687	0.008124
		100	-0.005042	-0.004915	-0.00357
	coim	100	0.000807	-0.001097	-0.00446
		200	-0.006240	0.007330	0.003296
		300	0.0044055	0.002381	-0.00690
	Car	2	0.00795	0.000330	0.00288
		40	-0.000168	-0.00184	-0.00152
		100	0.005641	-0.00497	0.003462
	Lena	1	0.001548	-0.005947	0.01148
	Baboon	1	-0.00023	0.001597	-0.00201
	e1	1	0.0009	0.0025	-0.0056
	e2	1	-0.0018	-0.0001	0.0003
	e3	1	-0.00283	0.001498	-0.0018

- *Sensitivity Analysis*

To avoid the known-plaintext attack, we used an efficient algorithm based on hybrid maps to encrypt the video frames; this algorithm has good results of several experiments display that the presented technique for chipper video frames provides an efficient and secure approach to the video encryption, we obtained a very good cipher grayscale image, as evidenced by calculating uniform average changing intensity (UACI) and number of pixels change rate (NPCR) [23] between plain frame and encrypted frame. This means that the proposed methods are susceptible to minor changes within the plain frame.

$$\mathrm{NPCR} = \frac{\sum_{I,j} S(I,j)}{WxH} x100 \qquad (9)$$

$$\mathrm{UACI} = \frac{100}{WxH} \sum_{i,j} \frac{|R_1(i,j) - R_2(i,j)|}{255} x\ 100 \qquad (10)$$

The two ciphered frames are R1 and R2, whose corresponding plain frame has a 1-pixel only difference. R1(i, j) and R2(i, j) are greyscale amounts of the pixels at grid (i,j) with same size W×H, and used to specific S(i, j) value by,

$$S(i,j) = \begin{cases} 1 & ,R_1(i,j) = R_2(i,j), \\ 0 & ,otherwise \end{cases}$$

Table 4 displays the values of UACI and NPCR. We deduce that all NPCR test greater than 99.55 and UACI test are in the range [27.56 34.93], these results prove the presented method's robustness.

Table 4. NPCR and UACI values of video frames.

	Video	Frame Number	NPCR	UACI
The Proposed method	CLAIRE	2	0.9962	0.3068
		40	0.9968	0.30768
		100	0.9964	0.3068
	MTHR_DOTR	2	0.99625	0.28313
		40	0.99538	0.27569
		100	0.99633	0.27698
	FOREMAN	2	0.99550	0.30442
		40	0.99613	0.30465
		100	0.99633	0.30995
	coim	100	0.99635	0.35572
		200	0.99615	0.33270
		300	0.99597	0.31619
	Car	2	0.99630	0.27114
		40	0.99557	0.30072
		100	0.99604	0.28713
	Lena	1	0.99626	0.30430
	Baboon	1	0.99626	0.28057
	e1	1	0.99603	0.28766
	e2	1	0.99630	0.34930
	e3	1	0.99579	0.33735

-*Noise attack*

We tried the security of our method against noise. Into the cipher frames, two distinct kinds of noises are consolidated. The first is salt and pepper (with densities of 0.05 and 0.1) and the second is Gaussian noise (with the variance of 0.01 and 0.1). For estimating, we utilized the peak signal-to-noise ratio (PSNR) and the mean square error (MSE). PSNR and MSE are computed by the equations number 6 and 7. Mean square error & Peak signal to noise ratio

between cipher and the decrypted image/frame under various noise attacks, as appeared in table 5, table 6, and fig. 8. The results show that the proposed technique is satisfactory against salt and pepper noise and has an edge with Gaussian noise.

Table 5. Salt and pepper noise attack

	Video	Frame number	salt and pepper 0.05		salt and pepper 0.1	
			MSE	PSNR	MSE	PSNR
The Proposed method	car	2	346.	25.397	650	28.129
		40	433	26.373	842	29.256
		100	370	25.691	790	28.981
	coim	100	605	27.821	1216	30.850
		200	553	27.430	1083	30.350
		300	490	26.906	988	29.951
	Lena	1	441	26.444	873	29.412
	Baboon	1	354	25.490	722	28.589
	e2	1	568	27.550	1172	30.689
	e3	1	552	27.421	1097	30.405

Table 6. Gaussian noise attack

	Video	Frame number	Gaussian noise with variance of 0.01		Gaussian noise with variance of 0.1	
			MSE	PSNR	MSE	PSNR
The Proposed method	coim	100	12078	40.820	12207	40.866
		200	10748	40.313	10647	40.272
		300	9709	39.871	9701	39.868
	car	2	6630	38.215	6643	38.223
		40	8450	39.268	8374	39.229
		100	7694	38.86	7671	38.848
	Lena	1	8987	39.536	8953	39.519
	Baboon	1	7401	38.693	7393	38.688
	e2	1	11603	40.645	1165	40.665
	e3	1	10824	40.344	10887	40.369

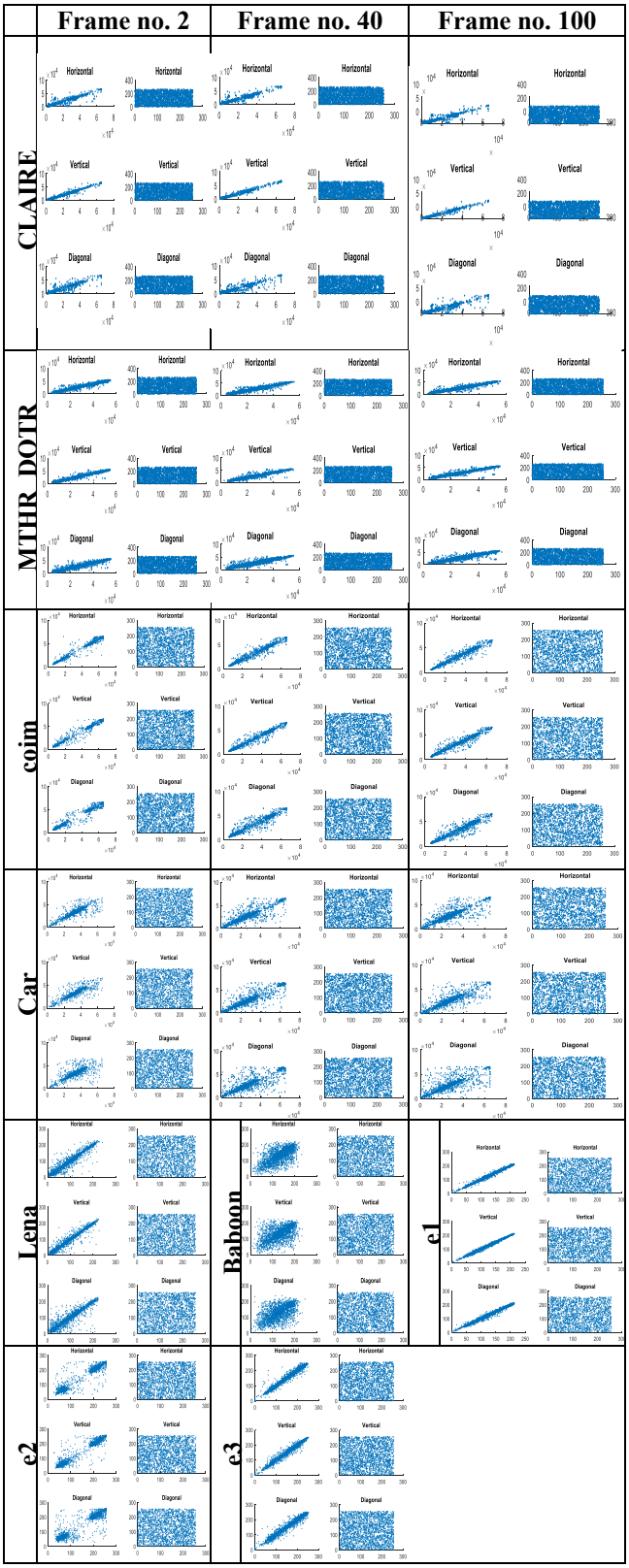


Fig. 7: Correlation between two adjacent pixels

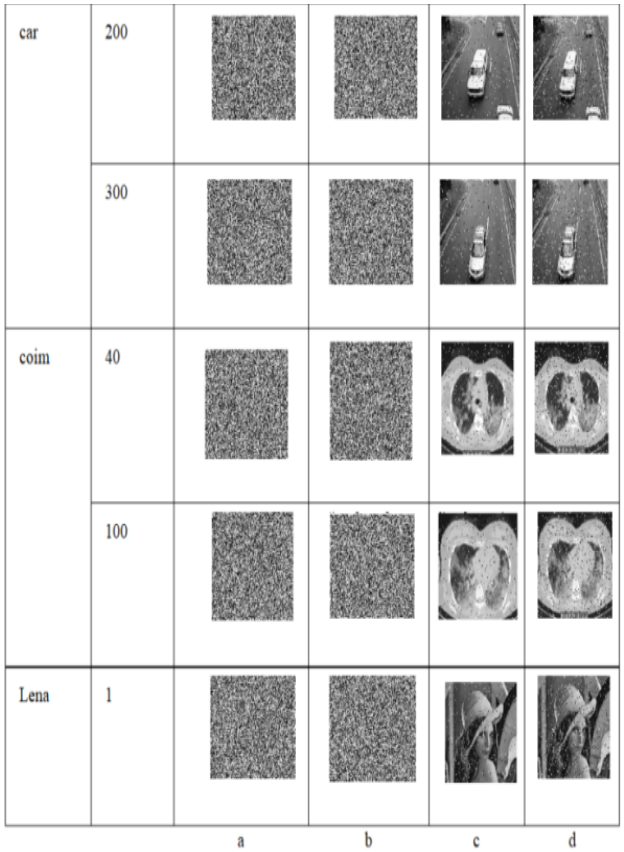


Fig. 8: Noise effect: a) decrypted frame with Gaussian noise of variance 0.01, b) decrypted frame with Gaussian noise of variance 0.1, c) decrypted frame with Salt and pepper noise of densities 0.05, and d) decrypted frame with Salt and pepper noise of densities 0.1.

- Statistical analyses
- Irregular deviation factor (IDF): this factor is based on how much the deviation caused by encryption is irregular. The following is a summary of the method:
- compute the matrix D, which contains the absolute values of the difference between each pixel value before and after encryption. D=|I – J|,(I is the input image and J is the encrypted image).
- create the absolute deviation histogram H. H = histogram (D).
- compute the average value of how many pixels are deviated at every deviation value. This average DC can be calculated as:

$$DC = \frac{1}{256}\sum_{i=0}^{255} h_i \quad (11)$$

Where hi is the amplitude of the absolute difference histogram at value i.
- Take the absolute value of the result after subtracting this average from the deviation histogram.

$$AC(i) = |H(i) - DC| \quad (12)$$

- Calculate the area under the absolute AC curve, which is the sum of the deviation histogram's change from the uniformly distributed histogram.

$$IDF = \sum_{i=0}^{255} AC(i) \quad (13)$$

The encryption algorithm with the lower IDF value is better.
Deviation from the uniform histogram (MD): This factor measures the quality of encryption that describes a formula for deviation from an ideal assumed uniform histogram. The uniform histogram is presented as

$$Hc_i = \begin{cases} \frac{M\times N}{256} & 0 \le c_i \le 255 \\ 0 & elsewhere \end{cases} \quad (14)$$

Where H_c histogram of the encrypted image, H_{c_i} the value of the frequency of occurrence at index i. the deviation from uniform histogram shown by equation 14 is calculated as:

$$MD = \frac{\sum_{c_i=0}^{255}\left|H_{c_i} - Hc\right|}{M\times N} \quad (15)$$

The lower the MD value, the higher the encryption quality, as the lower value implies that the encrypted image's histogram is less deviated from the uniform histogram.

Contrast test (CT): The contrast of an image is defined by the following equation.

$$\sum_{i,j}|i-j|^2\, I(i,j) \quad (16)$$

Where I image with I(i,j) representing the pixel value at position (i,j) of the image. [0 (size (Image)-1)^2] is the range of contrast values. More variation in image pixels is implied by higher contrast values.
Homogeneity test (HT): the image homogeneity can be defined by:

$$\sum_{i,j}\frac{I(i,j)}{i+|i-j|} \quad (17)$$

Where i, j depicts the location of image pixels. The homogeneity values lie in the interval [0 1].

Energy test (ET): the energy of an image is defined by:

$$\sum_{i,j} I(i,j)^2 \quad (18)$$

Table 7. Statistical analyses of the encrypted images:

	Video	Frame nu.	IDF	MD	CT	HT	ET
The Proposed method	coim	100	0	0.003768	1.09078e+04	0.03615	2.038517e-05
		200	0	0.003814	1.08943e+04	0.03619	2.037968e-05
		300	0	0.003723	1.09330e+04	0.03609	2.039437e-05
	Car	2	0	0.003494	1.09464e+04	0.03636	2.038347e-05
		40	0	0.004165	1.09194e+04	0.03624	2.037191e-05
		100	0	0.003524	1.09050e+04	0.03629	2.035161e-05
	Lena	1	0.0030	0.573081	1.09329e+04	0.03654	2.036580e-05
	Baboon	1	0.0039	0.701904	1.09684e+04	0.0361	2.038131e-05
	e2	1	0.0045	0.981170	1.09365e+04	0.0363	2.039055e-05
	e3	1	0.0052	0.642044	1.09015e+04	0.0365	2.038420e-05

Irregular deviation factor, maximum deviation, contrast test, homogeneity test, and energy test

The energy values lie in the interval [0 1] and the constant image has maximum energy value of 1. Table 7 shows the values of statistical analysis. This table indicates the quality of our proposed technique.

-*Computational complexity analysis*

The method execution speed is important in image encryption design. The results of the speed test for the proposed method are very fast when compared to recent methods [33] and [34] with Lena image using a 2.7 GHz laptop. The comparison of the encryption time for different methods is shown in table 8. The presented hybrid method is more complex and speedier.

Table 8. The time performance test (ms)

	Henon	Elliptic curve	Logistic	Total	Ref. [33]	Ref. [34]
Lena	9.3469116	9.3738401	9.2767	27.99745	**113.01**	186.94
Baboon	9.35165	9.193845	9.24806	27.79355	------	------

The introduced method is comparable to the entropy and NPCR values proposed by references [24], [25], [26], [27], [28], [29], [30], [31] and [32] as seen in table 9.

The presented technique has the best correlation than Refs. [27], [28] as appear in Table 10. The 3 directions of the correlation effect for original and encrypted lena image shown in fig. 5 for plain and ciphered images.

The results in Table 11 show that the proposed approach is robust against salt and pepper noise attacks.

Table 9. Comparison of entropy and NPCR values for Lena and Baboon gray images

	Scheme	Entropy	NPCR
Lena	The proposed scheme 1.	7.9972	99.63
	Ref. [24].	7.9891	99.59
	Ref. [25].	7.9972	99.63
	Ref. [26].	7.9971	99.59
	Ref. [27].	7.9963	99.62
	Ref. [28].	7.9973	96.67
	Ref. [29].	7.9969	99.59
	Ref. [30].	-------	99.58
	Ref. [31].	7.9972	99.61
	Ref. [32].	7.9973	99.61
	Ref. [34].	7.9894	99.66
Baboon	The proposed scheme 1.	7.9971	99.60
	Ref. [28].	7.9920	99.63
	Ref. [29].	-------	99.60

Table 10. Comparison of Correlation coefficients.

	Video	Horizontal	Vertical	Diagonal
The Proposed method	Lena	0.001548	-0.005947	0.01148
	Baboon	-0.00023	0.001597	-0.00201
	Car	-0.00016	-0.00184	-0.00152
Ref.[23].	Lena	−0.0048	−0.0112	−0.0045
Ref.[24].	Lena	-0.0002	-0.0015	-0.0008

Table 11. Noise attack with Lena image

Noise type		Proposed method	Ref.[34].	Ref.[33].	Ref.[35].
Salt and pepper with density 0.05	MSE	441.03	12.2870	437.9	869.9
	PSNR	26.4447	33.1880	21.7	18.7
Salt and pepper with density 0.1	MSE	873.44	24.2675	893.1	1829.6
	PSNR	29.4123	30.2321	18.6	15.5
Gaussian with variance=0.01 and mean=0	MSE	8987.30	105.0683	2321.4	4410.1
	PSNR	39.5362	23.8677	14.5	11.7
Gaussian with variance=0.1 and mean=0	MSE	8953.58	106.0403	5201.2	5631.4
	PSNR	39.5199	23.8277	11.0	10.6

- *Analysis Key space*

An ideal encryption method ought to have a keyspace of more than 2^{100} [36] to resist the brute force attack. Keyspace is constructed from the parameters that requirements for key generation. For our introduced method, the security key consists of eight parts: (α and $\beta \in R$ is the set of real numbers, the initial condition is x_1, the control parameter is u and g_1, $g_2 \in F^2m$) are the initial values for Henon map, elliptic curve, and new logistic map. Whenever set 14 decimals to the length of every subkey, the key-space will be 10^{112} of the proposed method.

5 Conclusion

The trusted and rapid encryption algorithm to encrypt the patients' medical data is a very important issue that must be considered during these critical times of pandemics. This pandemic obliged the governments and also healthcare institutions to observe COVID-19 patients. Moreover, all patients' data (image, video) are available for the researchers to help them find a vaccine for this pandemic. The presented method relies on a recently introduced encryption technique, which utilized improved logistic, henon, and EC techniques to realize high encryption. A block permutation is used to enhance the efficiency of our method. Experimental results declare that the presented technique could be applied very well to images and video. Also, analysis proved that the proposed technique achieved the required level of security, and it is robust against different attacks

References

[1] J.L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, J.P. Hubaux, "Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy", IEEE/ACM Transactions on Computational Biology and Bioinformatics. 15, pp.1413–1426, 2018. https://doi.org/10.1109/TCBB.2018.2854782.

[2] R. Becker, A. Thorogood, J. Ordish, M.J.S. Beauvais, Regulation, (n.d.) 1–14.

[3] A. Berke, M. Bakker, P. V., K. Larson, A. "Sandy" Pentland, Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy, 2020. http://arxiv.org/abs/2003.14412.

[4] Bhanot, Rajdeep, and Rahul Hans. A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications. Vol. 9.4, pp:289-306, 2015.

[5] Goyal, Dinesh; Hemrajani, Naveen, " Novel Selective Video Encryption for H.264 Video", International Journal of Information Security Science. Vol. 3, Issue 4, p216-226, Dec2014.

[6] Sridhar C. Iyer, R.R Sedamkar, Shiwani Gupta. A novel idea of video encryption using hybrid cryptographic techniques. 2016 International Conference on Inventive Computation Technologies (ICICT). Vol. 3, pp.1-5, Aug 2016.

[7] Sha-ShaYu, Nan-Run Zhou, Li-Hua Gong, Zhe Nieb. Optical image encryption algorithm based on phasetruncated short-time fractional Fourier transform and hyper-chaotic system. Optics and Lasers in Engineering, 2020, vol. 124, pp. 105816.

[8] R. Ranjith kumar, D. Ganeshkumar, A. Suresh. A New One Round Video Encryption Scheme Based on 1D Chaotic Maps. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp.439-444, Mar. 2019.

[9] D. Valli, K. Ganesan. Chaos based video encryption using maps and Ikeda time delay system. The Europian physical journal plus 132: 542, 2017. DOI 10.1140/epjp/i2017-11819-7.

[10] Huang Zhi-Jing, Cheng Shan, Gong Li-Hua, Zhou Nan-Run. Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Optics and Lasers in Engineering, vol. 124, p. 105821, 2020.

[11] Walaa M. Abd-Elhafiez, Mohamed Heshmat. Medical Image Encryption Via Lifting Method", Journal of Intelligent & Fuzzy Systems. vol. 38, no. 3, pp. 2823-2832, 2020.

[12] Walaa M. Abd-Elhafiez, Wajeb Gharibi, Mohamed Heshmat. An efficient color image compression technique. TELKOMNIKA Telecommunication, Computing, Electronics and Control, Vol. 18, No. 4, pp. 2371-2377, October 2020.

[13] Rajalakshmi, K., Dr. K. Mahesh. An Innovative Video Data Embedding Method for Video Security. International Journal of Pure and Applied Mathematics, Vol.118, N0.7, pp:215-219, 2018.

[14] Tang, Lei. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the fourth ACM international conference on Multimedia. 1997

[15] Szczepanski, J., Kotulski, Z. Pseudorandom number generators based on chaotic dynamical systems. Open. Syst. Inf. Dyn. Vol.8, pp:137–146, 2001.

[16] O. Reyad and Z. Kotulski. On Pseudo-random Number Generators Using Elliptic Curves and Chaotic Systems. J. Appl. Math. Inf. Sci., Vol. 9, pp. 31-38, 2015.

[17] L. Rui. New algorithm for color image encryption using improved 1D logistic chaotic map. Open Cybern. Syst. J., Vol. 9, no. 1, 2015.

[18] H. K. Sarmah and R. Paul. Period Doubling Route to Chaos in a Two Parameter Invertible Map with Constant Jacobian. IJRRAS 3 pp. 72-82, 2010.

[19] http://sipi.usc.edu/database/database.php?volume=mic

[20] Ieee8023, GitHub - ieee8023/covid-chestxray-dataset: an open database of COVID-19 cases with chest X-ray or CT images., 2020. (n.d.). https://github.com/ieee8023/covid-chestxray-dataset.

[21] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, M. R. Mosavi. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimed. Tools Appl., Vol. 74, no. 3, pp. 781–811, Feb. 2013.

[22] J. Kalpana, P. Murali. An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. Opt. - Int. J. Light Electron Opt., Vol. 126, no. 24, pp. 5703–5709, Dec. 2015.

[23] W. Xiangjun, B. Chenxi, K. Haibin. A new color image cryptosystem via hyperchaos synchronization. Commun Nonlinear Sci Numer Simulat, Vol. 19, pp. 1884–1897, 2014.

[24] Ahmad, S. Alam, K. M. R. Rahman, H., Tamura, S. A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. International Conference In Networking Systems and Security (NSysS), pp. 1-5, 2015.

[25] Huiqing Huang, Shouzhi Yang. Image encryption technique combining compressive sensing with double random-phase encoding. Hindawi Mathematical Problems in Engineering, 2018.

[26] Xingyuan W., X., Yingqian Z. An image encryption algorithm based on Josephus traversing and mixed chaotic map. The Institute of Electrical and Electronics Engineers, 2018.

[27] Akram Belazi, Ahmed A Abd El-Latif, Safya B. A novel image encryption scheme based on substitution-permutation network and chaos. Signal Processing, 128, pp:155–170, 2016.

[28] Aqeel-ur-Rehman, X. Liao, M. A. Hahsmi, R. Haider. An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Opt. - Int. J. Light Electron Opt., Vol. 153, pp. 117–134, 2018.

[29] Souyah A., Faraaoun K. M., "An efficient and secure chaotic cipher algorithm for image content preservation", Signal processing, DOI: 10.1016/j.cnsns.12.017, PII: S1007-5704(17)30439-2, 2017.

[30] NOROUZI, Benyamin, SEYEDZADEH, Seyed M., M., S. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimedia Tools and Applications, vol. 74, no 3, pp. 781-811, 2015.

[31] LI, Yueping, Wang, Chunhua, Chen, Hua. A hyper-chaos-based image encryption algorithm using pixel level permutation and bit-level permutation. Optics and Lasers in Engineering, vol. 90, pp. 238-246, 2017.

[32] XU, Lu, Gou, Xu, LI, Zhi, A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion, Optics and Lasers in Engineering, vol. 91, pp. 41-52, 2017.

[33] Askar S. S., Karawia A. A., Alshamarani. Image encryption algorithm based on chaotic economic model. Math. Probl. Eng. 341729, 2015.

[34] Li T., Du B., Liang X. Image encryption algorithm based on logistic and two-dimensional Lorenz. IEEE Access, 2019.

[35] Parvin Z., Seyedarbi H., Shamsi M. A new secure and sensitive image encryption scheme based on new substitution with chaotic function. Multimedia Tools Application, 10631-10648, 2016.

[36] Liu W., Zhu C., Sun K., A fast image encryption algorithm based on chaotic map. Journal of ElsevierLTd, 2016.