Journal of Energy Systems

2022, *6*(4)

2602-2052

DOI: 10.30521/jes.1160773

Research Article

A New hyper chaotic algorithm for energy video communication security

Erol Kurt
Gazi University, Technology Faculty, Department of Electrical and Electronics Engineering, Beşevler, TR06500 Ankara, Turkey, ekurt52tr@yahoo.com

Soner Mülayim*
Gazi University, Technology Faculty, Department of Electrical and Electronics Engineering, Beşevler, TR06500 Ankara, Turkey, mlsoner@gmail.com

Submitted: *11.08.2022*
Accepted: *29.09.2022*
Published: *31.12.2022*

* *Corresponding Author*

Abstract: The usage of the cameras in facilities in the energy sector is becoming more and more common. In addition, with the widespread use of SCADA and the increase in automation of camera-based applications, ensuring security in video data communication has become more and more important. In this study, methods that have been successful in providing image security in previous studies in Ref.[1] have been improved to ensure the security of video data communication. These methods use Kurt-Modified Chua's Circuit (KMCC) as random number generator. Proposed algorithms are efficient for energy sector secure video communication because of using hyperchaotic random number generator and also bit level scrambling, diffusion encryption to each frame of video.

Keywords: *Bit level scrambling, Chaotic sequence, Decryption, Energy video, Modified Chua's circuit*

Cite this paper as: Kurt, E., & Mülayim, S., A New hyper chaotic algorithm for energy video communication security. *Journal of Energy Systems 2022; 6*(4): 583-593, DOI: 10.30521/jes.1160773

1. INTRODUCTION

Video-based applications, which have become widespread in all areas of life such as business, entertainment and military, reveal security requirements. This situation has led to the need for many segments to produce solutions in this field, from personal data security to industrial data security [2-4]. The security of in-plant video images, which are critical in data communication between facilities in the energy sector, is becoming increasingly important. For this purpose, the use of encryption processes on images of energy systems has begun to increase [5,6]. In the literature, there are traditional some encryption methods such as DES [7], IDEA [8], RSA [9] and AES [10]. However, while these methods are successful for plain text and binary data encryption, they are not suitable for direct use for video encryption due to several reasons. One of the reasons is that video data mostly has large size and requires real time processing, such as image displaying, seeking time, frame modify, bit rate control and recompression. The other reason is that the videos consist of consecutive frames and the difference between these frames will be a few pixels. Traditional methods will not be sufficient to encrypt the visible information containing these few pixels of information.

Considering these situations, different studies have been put forward [11,12]. Some of them followed the zig-zag permutation algorithms [13] and some of them followed the encryption method by compressing the video files with DCT [12]. Some studies for encrypt MPEG video files contain I, P and B pictures, just by using I intraframes and DCT (Discreate Cosine Transform), Huffman entropy coding and quantization in order to compress the mpeg video file [14]. In addition, the video compression techniques are divided into 2 groups as lossy and lossless. Lossless compression doesn't sacrifice visual content or detail either. However, in this case, the compression process is more limited than lossy compression. Lossless compression should be preferred if the loss of information in the compression process causes so much damage. Huffman algorithm and run length coding can be given as examples of lossless compression algorithms. In lossy compression, on the other hand, unnecessary information that users cannot see and does not affect image quality is removed, results in a higher compression ratio than lossless compression [15]. However, the point to be noted here is that the data removed during the compression process cannot be recovered. Therefore, although the losses will be unnecessary and will not affect the image, it should still be considered whether the losses in the video to be compressed are critical or significant.

Another issue that is as important as compression techniques in the processing of the video file to be encrypted is that the encryption technique should be quite strong, as the variation between frames is low in video encryption, as mentioned above. There are many different algorithms in the literature on encrypting colored images. One of them is a successful study using the method of scrambling and diffusion at the bit level [16] and this study presents efficient and fast color image algorithms that can be used in video encryption. Besides, another important factor in encryption is the random number generator to be used in the encryption map. The more unique and complex the randomness of the number generator, the more advantageous the encryption algorithm is against attacks. This situation has increased the interest in implement chaotic theory to the encryption algorithms [17]. Because, chaotic number generators are not iterative. Therefore, any external source will not be enough to decrypt random data. Of course, this system has one disadvantage, which is that the chaotic generators in the encryption circuit and the decryption circuit must be synchronized.

Kurt-Modified Chua’s Circuit (KMCC) is used in this study because it is a very powerful random number generator which exhibits hyperchaotic behavior under certain parameters [16]. In addition, the frames generated from video files are encrypted at the bit level with scrambling and diffusion methods in Refs [1,16]. Therefore in the present work, we aim to combine the hyperchaotic feature with the advanced ciphering/deciphering techniques to prove the efficiency of the technique in video cryptography field.

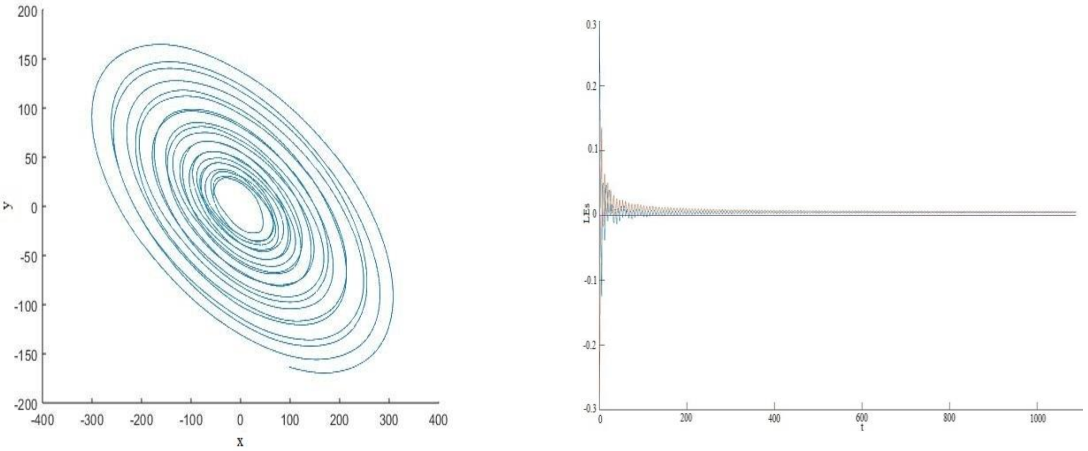
In Sec. 2, the determination of the hyperchaotic circuit namely KMCC will be presented. Sec. 3 gives the methology of the present work. Sec. 4 gives the experimental findings of the proposed video cryptology technique. The security analyses on the ciphered images are given in detail in Sec. 5. Finally, the paper ends with a conclusion section where the concluding remarks are highlighted.

2. HYPERCHAOTIC SYSTEM DEFINITION

In this study, chaotic random numbers are needed to provide high security video encryption/decryption. Therefore KMCC is used to generate the random numbers required for encryption/decryption. Because with certain initial parameters, this circuit generates hyperchaotic data and the circuit has a strong randomness in the phase space. The equations of the circuit are as follows [17]:

$$\begin{cases} \dot{x} = y - bx - \frac{1}{2}(a-b)[|x+\sin(z)| - |x-\sin(z)|]\,, \\ \dot{y} = -\beta(y+x) + f sin(v)\,, \\ \dot{z} = \emptyset\,, \\ \dot{v} = \omega \end{cases} \tag{1}$$

Here, the control parameters are a, b, $\emptyset$, β, ω and f. The tangent of the nonlinear diode is described by the parameters a and b for the threshold regions of three-segmented-structure. The parameter β is the parameter including capacitance, inductance and the conductivity. The parameter f includes excitation amplitude in volts, β and segment location in voltage - current characteristics of the diode (see details at Refs. [18,19]).



(a) (b)

Figure 1. (a) 2D attractor of random number generator circuit with the parameters of a=-4.2, b=-0.31, β=0.3, Ø=-15.9, ω=-4.2, f=9.1, (b) Lyapunov spectrum of this circuit.

Lyapunov spectrum represented in Fig. 1(b) shows that this system is hyperchaotic because of two positive exponents. Also, 2D attractor of KMCC is presented in Fig. 1(a).

3. METHODOLOGY

In this paper, the image encryption procedure in Refs. [16,18,19] is adapted to video encryption. Besides, the secret key generation and initial value definition are used in Refs. [16,18,19]. However, we explain some changes such as frame generating and encryption modifies. In our technique, initially a video file is converted to the frame structures. The frames are created as png (Portable Network Graphic) format because of lossless and highest compress ratio jpg format is better than png with compress ratio but jpg is a lossy format and this loss causes disruptions in the recovered frames of the video. After the frame creation SHA-256 secret key, chaotic numbers and key matrix generated, respectively for first frame of video. This method does not make a weakness in encryption because our number generator KMCC generates hyperchaotic data and we apply scramble and diffusion in bit level. Afterwards, application of the encryption for each frame is made.

Fig. 2 presents the first stage of algorithm creating secret key, chaotic numbers and key matrix for the encryption. Unlike previous study in Refs. [16,18,19], in this study, key matrix is produced with a different method. This method depends on creating two arrays with using frame *x* and *y* dimension and create a new array with crossing those two arrays. These two arrays include random numbers generated from KMCC. This method allows generating key matrix with fewer iterations and hence less chaotic numbers, but this method allows higher quality frames to be encrypted at the encryption time in Refs. [16,18,19].

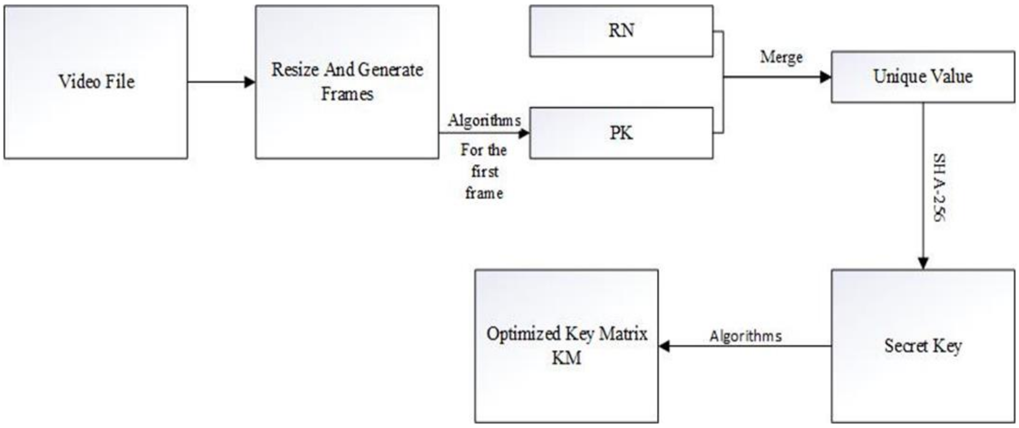


Figure 2. Flow chart of key matrix and secret key generate.

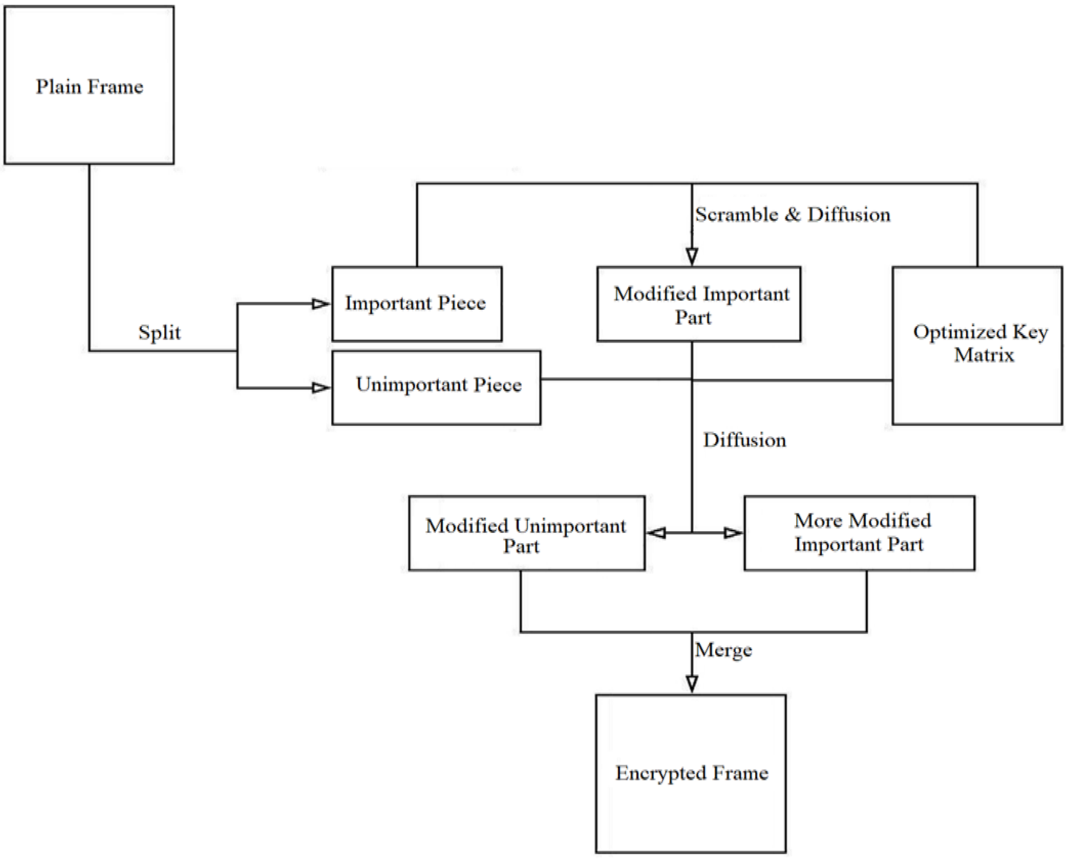


Figure 3. Flow chart of encryption process.

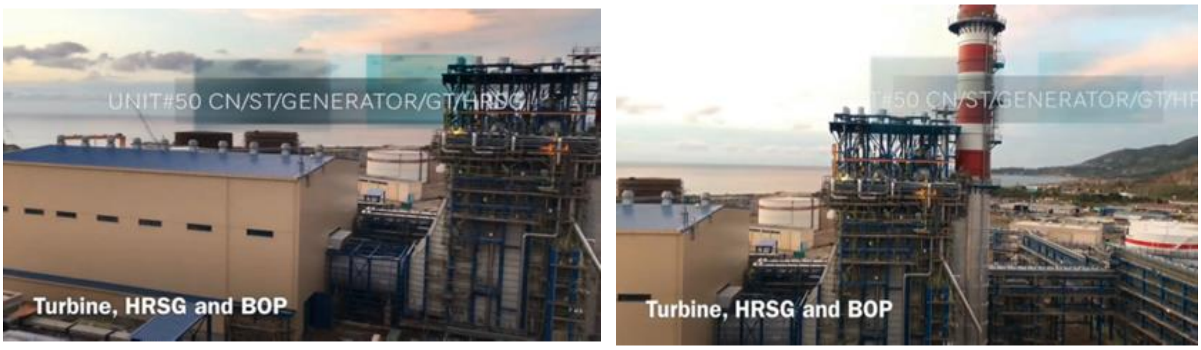
Fig. 3 presents encryption algorithm. This algorithm split the frame into 2 different pieces shown in Fig. 3. This feature of Ref. [16,18,19], which was previously mentioned in image encryption and which is different from the algorithms in the literature, was used in the present study. However, in this study modified important part splitted 4 pieces while scramble & diffusion apply. This method is necessary for use Key Matrix which created with new method. The encryption process presented in Fig. 3 was applied to each frame. This process is applied after the process presented in Fig. 2. This approach speeds up the encryption, especially in applications such as real-time webcams. For the deciphering process, vice-versa of this algorithm is used.

4. EXPERIMENTAL RESULTS

The initial parameters of KMCC for the generation of secret key and random numbers are a=-4.2, b=-0.31, β=0.3, ∅=-15.9, ω=-4.2, respectively. The circuit dynamics exhibit a hyperchaotic scenario for $f \geq 9.1$ as also stated in Ref. [18]. The sample secret key is,

F815BA4402FF42A3FE8ACCBC9FC0490C0EFDCF54E0F34612940169672FA8B64C.

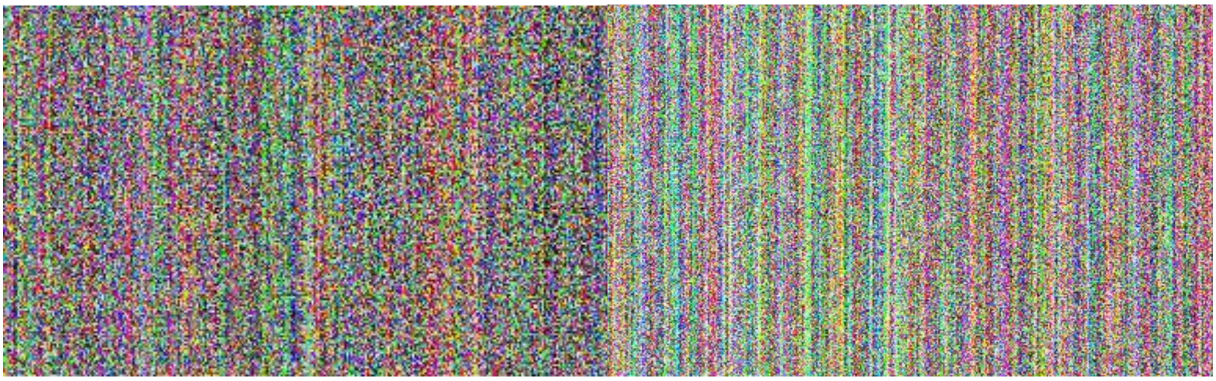
With using this secret key and control parameters stated in Eq. (1), the initial state variables of KMCC are obtained. Driving amplitude *f* is also obtained. These procedure is similar in Ref. [1,16]. Some frames of the raw video are presented in Fig. 4(a,b). Here, 2 sample frames belong to an energy plant video are presented, indeed the video itself has 200 frames in total.



(a) *(b)*

Figure 4. Sample frames from the energy plant video for the encryption/decryption: (a) is the first frame and (b) is the 180th frame.

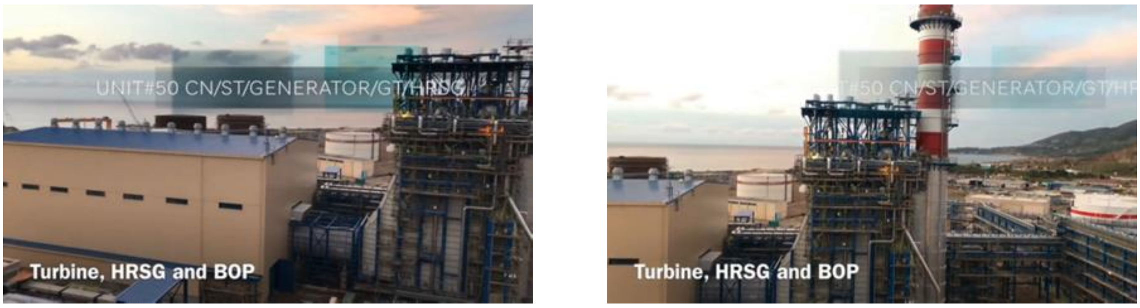
Fig. 5 (a,b) presents the ciphered frames respectively with using algorithm in Fig. 3.



(a) *(b)*

Figure 5. The ciphered stages of the frames shown in Fig. 4(a,b).

It is obvious with a naked eye that the ciphering procedure works well. On the other hand, some security test should be applied to ensure to what extend the ciphering is strong. Many security tests applied in this study to be at the safe side. In the meantime decrypted frames are presented in Fig. 6(a,b), respectively.



(a) *(b)*

Figure 6. The decrypted energy plant video frame samples: (a) the first frame and (b) the 180th frame of decrypted video.

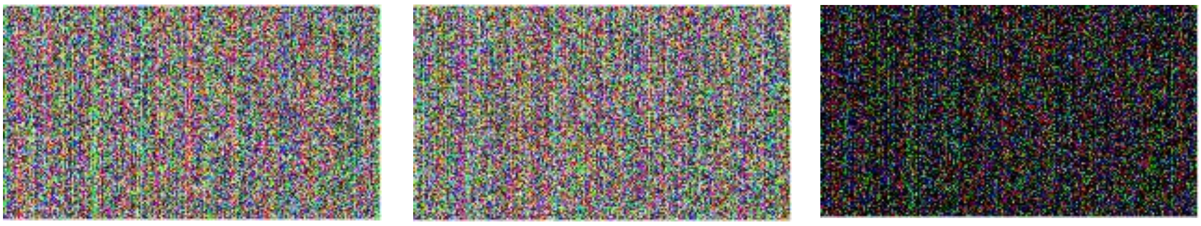
5. SECURITY TESTS

5.1. Key Space Analysis

A strong key space can neutralize the brute-force attacks. The encryption key consists of initial values given by (x_1, y_1, z_1, v_1) and f as initial parameter stated in Ref. [1,16]. Therefore, initial conditions of the chaotic characteristic precision must be as high as possible. To be more precise on the initial values we should apply 15 digits after the comma [20]. In that case, the key space is $S = 10^{70} \cong 2^{232} > 2^{100}$ [20], thereby it means that our cryptosystem and algorithms has resistance to the brute-force attacks.

5.2. Key Sensitivity Test

As mentioned earlier, our secret key generation is only done at the beginning of the entire process and this secret key depends on generated has value of the plain frame and added noise. Therefore, if there exists a slightly change caused in the initial condition, that causes differences at the encrypted frame. In Fig. 7(a,b,c), the encrypted first frame with a slightly changed secret key frame, encrypted frame and the difference between these two frames are represented, respectively.



(a) *(b)* *(c)*

Figure 7. Sensitivity of secret key in encryption process.

Note that here, the changed key for the second frame (i.e. Fig. 7(b)) is defined as, F815BA4402FF42A3FE8ACCBC9FC0490C0EFDCF54E0F346129401696727A8B64C

5.3. Differential Attacks

In the image encryption terminology, the encrypted image must be different from the plain image (i.e. unencrypted image). In the literature, this difference is evaluated by a criteria called NPCR [21] and UACI [22]. Tables 1 and 2 show the NPCR and UACI test results in this manner.

Table 1. Average, minimum and maximum values of UACI (%) by using proposed algorithm.

Frame	R			G			B		
index	Max	Mean	Min	Max	Mean	Min	Max	Mean	Min
1	34.103	33,456	32.810	34.865	34.207	33.550	34.980	34.500	34.010
180	34.450	33.430	32.400	34.200	33.400	32.590	34.960	34.060	33.160

Table 2. Average, minimum and maximum values of NPCR (%) by using proposed algorithm.

Frame	R			G			B		
index	Max	Mean	Min	Max	Mean	Min	Max	Mean	Min
1	99.280	99.225	99.170	99.370	99.308	99.247	99.480	99.423	99.367
180	99.340	99.335	99.330	99.400	99.245	99.091	99.500	99.447	99.395

5.4. Resisting Noise Attack Analysis

Different noises in the transmission channels used in the transmission of the image may affect the transmitted image. Therefore, the algorithm should be designed to ensure that the transmitted encrypted image is resistant to these noises applied in an external manner. The criterion for how well the decrypted image meets this requirement is Peak Signal-to-Noise Ratio (PSNR). The PSNR value is calculated by the following formula [23]:

$$PSNR = 10\left[\log_{10}\left(\frac{(255)(255)}{MSE}\right)\right](dB) \tag{2}$$

$$MSE = \frac{1}{ab}\sum_{k=1}^{x}\sum_{k=1}^{y}\|J_1(k,m) - J_2(k,m)\|^2 \tag{3}$$

The MSE presented in Eq. (3) is the mean square error between the original frame ($J_1(k,m)$) and the recovered frame ($J_2(k,m)$). Those frames have a size of a×b. In this study, Gaussian and salt paper noised applied and tested proposed algorithms. Fig. 8 shows the results of the salt pepper noise test in this regard. For this test, the 180th frame of the video is exposed to salt pepper noise. PSNR, MSE and correlation values in presented in Table 3. The PSNR values under 30 dB but quite near 30 dB and the correlation is very high. As can be seen from the results in Table 3, the proposed algorithm is resistant to the noise attacks.

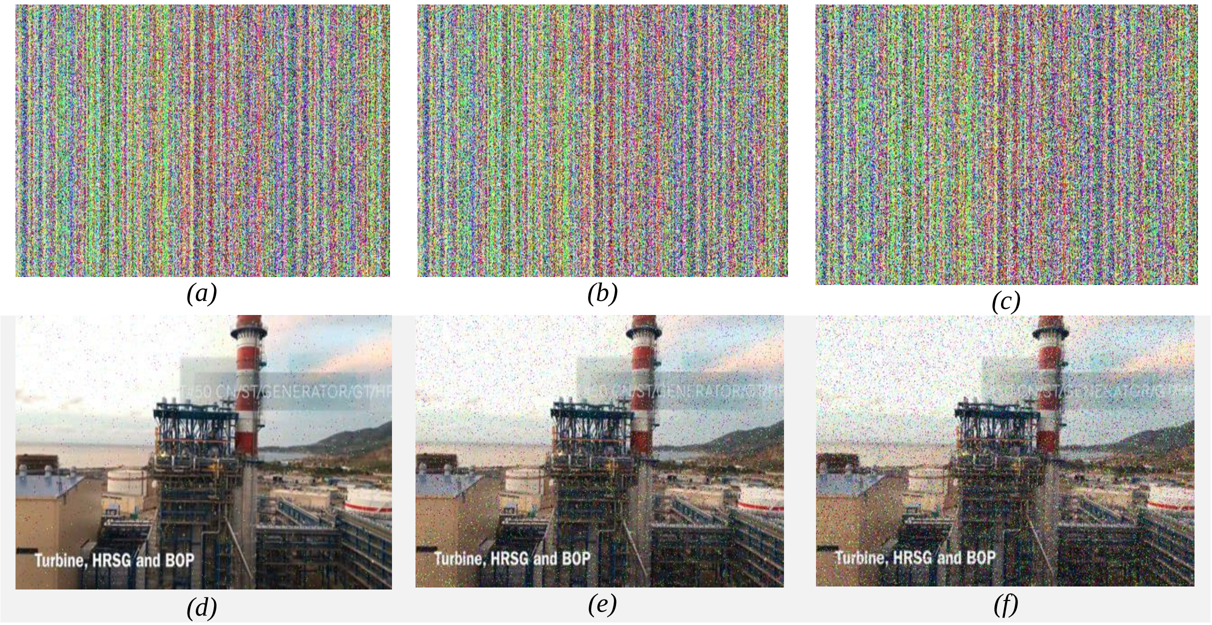


Figure 8. The 180th decoded frame of the video and the salt-and-pepper noise-encoded forms are: (a) and 0.01 intensity noise (d); (b) and 0.05 intensity noise (e); (c) and noise of 0.1 intensity (f).

Table 3. MSE, PSNR and correlation values of Fig. 8 for each noise density.

Frame	Noise		MSE			PSNR			Correlation	
index	Density	R	G	B	R	G	B	R	G	B
180	0.01	115	110	112	27.539	27.703	27.638	0.9948	0.9941	0.9954
	0.05	543	552	564	20.785	20.710	20.617	0.9752	0.9697	0.9746
	0.1	1106	1118	1121	17.695	17.645	17.635	0.9435	0.9429	0.9472

5.5. Information Entropy Analysis

Information entropy is the measurement of the arbitrary distribution for an image. The information entropy formula is calculated as follows [24]:

$$H(m) = \sum_{i=1}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)} \tag{4}$$

According to Ref. [25], this value should be close to 8 for an encrypted image. Table 4 shows the results and values are quite close to 8 by using Eq. (4).

Table 4. Information entropies of the decrypted images.

Frame index	RGB Components		
	R	G	B
1	7.9869	7.9833	7.9697
180	7.6984	7.7613	7.8277

5.6. Correlation Coefficient Analyses

Statistical attacks use the relationship between of neighboring pixels in original frame image. To counteract this attack encrypted frame image must have lower relationship in neighboring pixels. To calculate this correlation value, following formulation used [26]:

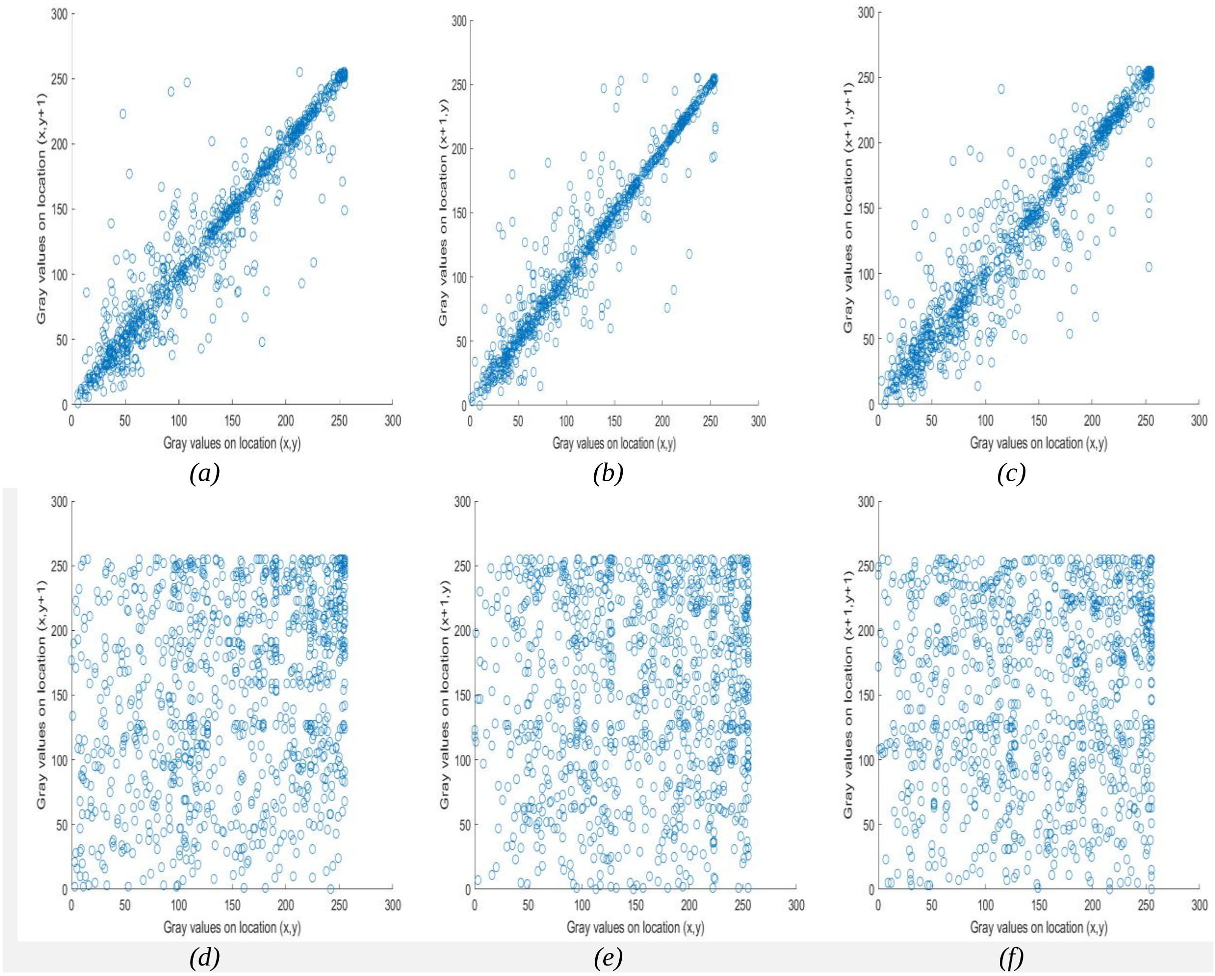
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

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

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{7}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \tag{8}$$

Fig. 9 shows the vertical, horizontal and diagonal correlation distributions of two adjacent pixels of the encrypted and plain frame. In Fig. 9, it can be clearly seen that the correlation between two neighboring pixels has decreased significantly. Table 5 shows the detailed values of the correlation coefficient analyses.



(a) (b) (c)

(d) (e) (f)

Figure 9. Correlation distributions of two adjacent pixels of the plain frame (a),(b),(c) are vertical, horizontal and diagonal respectively and correlation distributions of two adjacent pixels of the encrypted frame (d),(e),(f) are vertical, horizontal and diagonal respectively.

Table 5. Encrypted and plain frame correlation values.

Frame index	Directions	Original			Encrypted		
		R	G	B	R	G	B
1	Diagonal	0.9409	0.9407	0.9256	-0.0012	0.0349	0.0107
	Vertical	0.9738	0.9702	0.9681	0.1244	0.1150	0.0258
	Horizontal	0.9677	0.9659	0.9704	0.0657	0.0749	0.0411
180	Diagonal	0.9601	0.9564	0.9515	0.0882	0.0703	0.0732
	Vertical	0.9663	0.9774	0.9713	0.2298	0.1557	0.1199
	Horizontal	0.9733	0.9763	0.9769	0.0504	0.1250	0.0287

5.7. Histogram Analysis

In the literature, histogram is used to obtain the pixel distribution values of an image. While a plain frame has several and different peak value, encrypted frame has quite nearly constant distribution. This situation is shown in Fig. 10.

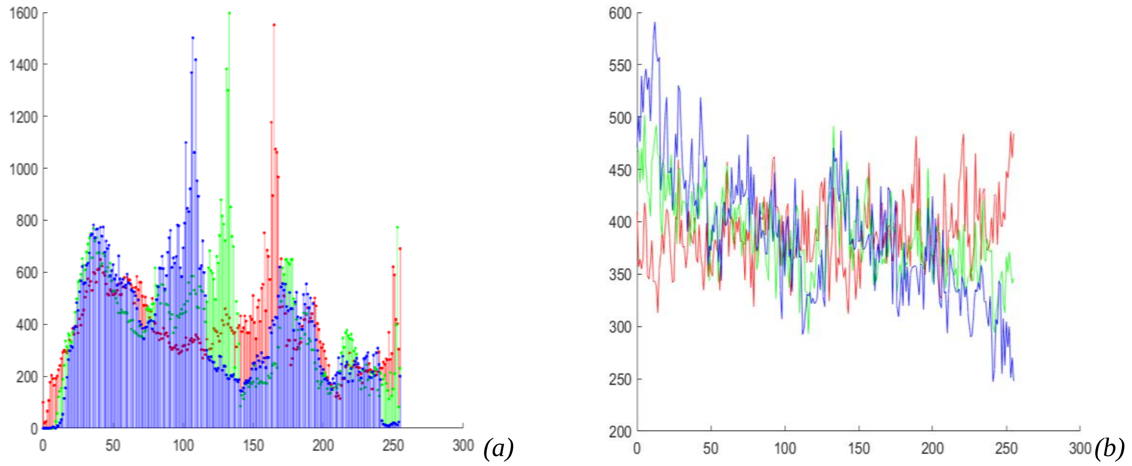


Figure 10. The histograms of (a) the first raw frame of the video and (b) the encrypted form of the same frame, respectively.

5.8. Speed Analysis

In addition to encryption security, speed is also an important factor. Since in this study focused on increasing the level of security, DCT and other compression techniques that developed to increase speed have not been implemented yet. Therefore, the speed performance is not satisfactory. The video used in this study is 6 s length and the encryption time for the video is 12 s. The system used for the present work is AMD RYZEN 3900x CPU, 16 GB 3200MHz RAM, SSD and MatLab 2017b.

6. CONCLUSION

In this study, a new hyperchaotic algorithm has been developed for the energy sector video data communication security. The strong and new secure video ciphering has been obtained with bit level scrambling and diffusion encrypting algorithm and also used KMCC as the random number generator. In order to ensure the ciphering secure capability, some security tests are applied to the ciphered frames and tests proved that the proposed system can be used for energy sector video data secure communication. To improve the ciphering speed performance, a coding/encoding video compression/decompression technique such as DCT (Discrete cosine transform) will be applied to this system and also the algorithms will be improved for speed up process for the future work.

REFERENCES

[1] Kurt, E., Arpacı, B., A new tool for energy security and secure energy communication. *Journal of Energy Systems* 2021; *5*(4): 376-389, DOI:10.30521/jes.1003454.

[2] Wassim Hamidouche, Mousa Farajallah, Naty Ould-Sidaty, Safwan El Assad, Olivier Déforges. Real-Time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension. *Signal Processing: Image Communication, Elsevier* 2017; 58: 73-86. DOI: 0.1016/j.image.2017.06.007.

[3] C. N. Raju, G. Umadevi, K. Srinathan and C. V. Jawahar. Fast and Secure Real-Time Video Encryption. In: 2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing; 16-19 December 2008, Bhubaneswar, India, pp. 257-264.

[4] Matin, A., Wang, X. Video encryption/compression using compressive coded rotating mirror camera. *Sci Rep* 2021; *11*: 1-11, DOI: 10.1038/s41598-021-02520-8

[5] Kang, D. J., Lee, J. J., Kim, B. H., & Hur, D. Proposal strategies of key management for data encryption in SCADA network of electric power systems. *International Journal of Electrical Power &amp; Energy Systems, Elsevier BV* 2011; *33*(9): 1521–1526, DOI: 10.1016/j.ijepes.2009.03.004.

[6] Oğraş, H. & Tür, M. R. An Effective Image Encryption Algorithm Using Bit Reversal Permutation and a New Chaotic Map. *Gazi University Journal of Science* 2022; *35*(2): 542-556. DOI: 10.35378/gujs.872818

[7] Biryukov, Alex & Cannière, Christophe. Data encryption standard (DES). In: Henk C. A. van Tilborg, Sushil Jajodia, editors. Encyclopedia of Cryptography and Security. New York, USA: Springer, 2005. pp. 129-135

[8] Almasri, O., & Jani, H. M., Introducing an Encryption Algorithm based on IDEA. *International Journal of Science and Research (IJSR)* 2013; *2*(9): 334-339.

[9] Zhang, S., A Brief Introduction to RSA Encryption. *Advances in Computer, Signals and Systems* 2021; *5*(1): 95-97, DOI:10.23977/acss.2021.050115.

[10] Stinson, D.R., Paterson, M., Cryptography: Theory and Practice. Florida, United States: CRC Press, 2005.

[11] Subraja, K., Geetha, N., & Mahesh, Dr. K., BITS – A Novel Video Encryption Algorithm. International *Journal of Innovative Technology and Exploring Engineering* 2020; *9*(8): 101–105, DOI:10.35940/ijitee.h6196.069820.

[12] Kadam, K, Deshmukh, A. Video Frame Encryption Algorithm using AES. *International Journal of Engineering Research* 2016; *5*(6): 588-591, DOI: 10.17577/IJERTV5IS060670.

[13] Abomhara, M. & Zakaria, O. & Khalifa, O., An Overview of Video Encryption Techniques. *International Journal of Computer Theory and Engineering* 2010; *2*: 103-110, DOI:10.7763/IJCTE.2010.V2.123.

[14] Changgui, C, Bhargava, B. Efficient MPEG video encryption algorithm. In: Proceedings Seventeenth IEEE Symposium on Reliable Distributed Systems; 20-23 October 1998, West Lafayette, IN, USA, pp. 381 - 386.

[15] Babatunde, A, Gbenga, J, Abikoye, O, B., Isiaka. Survey of Video Encryption Algorithms. *Covenant Journal of Informatics & Communication Technology* 2017; *5*(1): 65-80.

[16] Arpacı, B., Kurt, E., Çelik, K., Ciylan, B., Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit. *Journal of Electrical Engineering & Technology* 2020; *15*: 1413-1429, DOI: 10.1007/s42835-020-00393-x.

[17] Xiao, D, Liao, X, Wei, P. Analysis and improvement of a chaos-based image encryption algorithm. *Chaos, Sol. & Fractals* 2009; *40*(5): 2191-2199, DOI:10.1016/j.chaos.2007.10.009.

[18] Arpacı, B, Kurt, E, Çelik, K. A new algorithm for the colored image encryption via the modified Chua's circuit. *Engineering Science and Technology, an International Journal* 2020; *23*(3): 595-604. DOI: 10.1016/j.jestch.2019.09.001.

[19] Kurt, E. Nonlinearities from a non-autonomous chaotic circuit with a non-autonomous model of Chua's diode. *Physica Scripta* 2006; *74*(1): 22-27, DOI:10.1088/0031-8949/74/1/005.

[20] Arpacı, B, Kurt, E. An Innovative Tool for the Chaotic Image Encryption, Decryption and Security Tests. In: ICECCE 2020 Int. Conf. Electr., Commun. Computer Engin. *;* 12-13 June 2020, IEEE, Istanbul, Turkey, pp. 1-8. DOI: 10.1109/ICECCE49384.2020.9179274

[21] Li Y, Wang C, & Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering* 2017; *90*: 238–246, DOI: 10.1016/j.optlaseng.2016.10.020.

[22] El Assad S, Farajallah M. A new chaos-based image encryption system. *Signal Processing Image Communication* 2016 ; *41*:144–157, DOI:10.1016/j.image.2015.10.004.

[23] X. Chai, Z. Gan, M. Zhang, A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimedia Tools and Applications* 2017 ; *76*(14) :15561–15585, DOI:10.1007/s11042-016-3858-4.

[24] Vaidyanathan S, Akgul A, Kaçar S, Çavuşoğlu U., A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography. *European Physical Journal Plus* 2018 ; *133*(2):46-64, DOI: 10.1140/epjp/i2018-11872-8.

[25] Akgul A, Pehlivan I. A new three-dimensional chaotic system without equilibrium points, its dynamical analyses and electronic circuit application. *Technical gazette* 2016 ; *23*(1):209–214, DOI: 10.17559/TV-20141212125942.

[26] Norouzi B, Seyedzadeh SM, Mirzakuchaki S, Mosavi MR. A novel image encryption based on row-column, masking and main diffusion processes with hyperchaos. *Multimedia Tools and Applications* 2015; *74*(3):781–811, DOI: 10.1007/s11042-013-1699-y.