Hybrid Facial Chaotic-based Graphical Encryption Technique for Cloud Environment

A. Manikandan
Research Scholar, Department of Computer Science and Engineering, VISTAS, Pallavaram, India.
E-mail: mani.se@velsuniv.ac.in

R. Anandan
Professor, Department of Computer Science and Engineering, VISTAS, Pallavaram, India.
E-mail: anandan.se@velsuniv.ac.in

Received September 19, 2021; Accepted December 16, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19240

Abstract

Pictographic representations are everywhere in this digital world. IoT, Cloud, Fog, and 5G systems are becoming data transfer boosters for each user. In a real-world situation, secure data transmission is critical through open networks. Many conventional cryptosystems are inadequate for graphical data privacy in terms of computational overhead, latency, and more sensitive to the unknown attacks. In this paper, the secured and low-complex chaotic-based facial image cryptosystem has been developed for computer vision image data. The proposed crypto system utilizes the facial features, Lorentz chaotic maps for private keys production during the encoding process and the same is decrypted using the diffusion process. Facial depictions are merged with chaotic maps that are segmented and decrypted with mutual keys. The performance of the proposed hybrid cryptosystem is validated using the standard facial datasets and NCPR, UACI metrics are measured. Entropy and adjacent pixels correlation metrics also evaluated through proposed cryptosystems.

Keywords

Chaotic Maps, Cryptosystems, Facial Expression, Image Encryption, Security Mechanisms.

Introduction

The rapid and increasing growth of computer vision data sharing Reliable and comprehensive security measures are required to ensure the confidentiality of content and prevent unauthorized access over open networks and the Internet. Using data encryption Lin, C.Y.; Yu, H.H.; Zeng, W, is the most important method today. A security mechanism is an algorithm that stores data (text, images, voice, etc.). During processing to render it

inaccessible, transparent, or impermeable. Data encryption is now utilized in a wide range of applications, and numerous cryptographic keys have been developed with the intention of protecting confidential material by increasing its protection and discretion Phillips, I.E.B.; Ornstein, S. The majority of the research focuses on improving encryption efficiency, reducing execution time, and increasing security robustness against attacks. Chaos-based encryption schemes have outperformed conventional encryption schemes, demonstrating the potential to provide enhanced protection and privacy by using variable keys Azzaz, M.S.; Tanougast, C.; Sadoudi, S.; Bouridane, A Several associations have used chaotic maps to encrypt textual material. Ekhlas et al. Albhrany, E.A.; Jalil, L.F.; Saleh, H.H suggested an unstructured textual method based on block cryptographic and chaotic maps in particular. Their algorithm primarily used possible combination and replacement of the byte in S-box to encode and decode an 8*8 bytes array. Despite the fact that their system uses a wide key space, it has a low entropy. Murillo et al. Murillo-Escobar, M.; Meranza-Castillón, M.; López-Gutiérrez, R.; Cruz-Hernández, C. A suggested A symmetric text crypto rulebook based entirely on chaos. Custom logistic maps with 128-bit mystery keys, pseudo-random sequences, plain text properties, and optimal permutation spread were spherical all used in their scheme. The method has a limited computational cost, although it has a fast encryption speed. Another scheme, Lou et al. Luo, H.; Ge, B. Idevised a scheme to protect picture contents when being accessed. For the diffusion and permutation of pixels, they had been using a Deoxyribonucleic acid (DNA) method and 2D Henon Sine card (2D HSM). Their approach was highly conductive, despite low entropy analysis. Various researchers are also investigating video encryption. Gnash et al. In particular, Ganeshkumar, D.; Suresh, A.; Manigandan, K. Created a three-tiered chaotic video cryptosystem. Approximate cryptographic measurements were optimized with a combination of logistic and tent (LTS) cards, using permutations and spreading rounds. Their approach showed excellent time literacy, but limiting congestion was a disadvantage. Due to the limitations of related work, chaos systems have been used to create effective multimedia data encryption systems. Traditional chaos-based cryptosystems are good for text data, but not enough for voice data protection. The high redundancy of the audio signal and the large amount of data function are mainly involved in this. Some chaos-based graphical symmetric ciphers have security gaps such as z, which imposes additional restrictions on the selection of system parameters for inverted rectangular transformations Ibrahim Yasser, Mohamed A, Ahmed S. Samra, Fahmi Khalifa.To address these limitations, we developed a secured chaotic based low-complex facial image encoding technique for computer vision data transmission. The significant contribution of the proposed model comprises of three steps (i) Initially, facemask features are extracted from various depictions using standard extraction algorithm(ii) The extracted features are merged

with lorentz chaos values in order to generate the security keys at different segment(iii) Finally, the encrypted facial depictions are decoded using the diffusion process under mutual concern of sender and receivers. Section 3 details the proposed encryption model for computer vision data.

Related Works

Otoo-Arthur et al. proposed Now that ubiquitous technology is becoming an integral part of distance learning, the big data paradigm has the potential to be integrated into higher education. It also provides a general outlook for big data sources in higher education. Our job is to provide a high level framework data flow of big data in scalable higher education tailored to context-specific systems. The BiDeL framework provides high performance in terms of memory distribution and parallelism. BiDeL leverages numerous big data tools and algorithms in the Spark MLlib library to enhance the online learning user experience. D. Otoo-Arthur and T. L. van Zyl, Abdullah et al. utilized the chaotic maps for image encryption process in Hikmat N. Abdullah, Hamsa A. Abdullah Encryption and recovering the images are very difficult in real-time due to their dimentionality. The proposed image encryption algorithm adopted the chaotic maps in two distinct categories such as Arnold maps, and Henonand maps for recovering the encrypted images. The encoding process is initialized with confusion phase where pixels are combined with random chaotic values and recovered at the final phase using the diffusion process. Hybrid encoding process is mainly targeted on 2D images which is not much sufficient for recent portraits.

I. Yasser et al. proposed a discomposure based encoding and decryption framework for media data. Media data (i.e. text, video, audio, and image) are encrypted using chirikov chaotic maps in four distinct models Yasser, I.; Khalifa, F.; Mohamed, M.A.; Samrah, A.S The proposed 2D alteration encryption scheme includes hybrid algorithm were chaotic maps are generated at both confusion and diffusion process. Chaos maps are shuffled with text as symmetric key model, and highly sensitive to unknown attacks. The limitation of the proposed fusion chaos system requires high-end hardware source such as cloud, fog computational servers for both encryption and decryption that leads to high-cost and storage. Garcia-Mata et al. developed chaos signatures in terms of quantum size and statistically derived the chaos structures using “Lyapunov exponent”. The proposed quantum chaos maps are applied for out-of-time ordered correlator Ignacio Garc´ıa-Mata, Marcos Saraceno, Rodolfo A. Jalabert, Augusto J. Roncaglia, Diego A. Wisniacki. Arnold cat maps are used for generation of confusion states in encryption process. Jaideep Pathak et al. proposed a prediction model based on supervised learning approach for forecasting the chaotic dynamic structures. Chaos are very random in nature that requires the efficient

technique to predict its variations during transmission. The proposed hybrid model It consistently outperforms component reservoirs or knowledge-based model prediction methods in its ability to accurately predict both the Lorenz system and the spatiotemporal chaos Kuramoto-Shibasinsky equation Jaideep Pathak, Alexander Wikner, Rebeckah Fussell, Sarthak Chandra, Brian R. Hunt, Michelle Girvan, Edward Ott Fusen Wang et al. developed a supervised convolution neural network (CNN) and multistage decryption model for image encryption technique. The proposed neural networks are mainly used for diffusion process and specifically targeted on known-plaintext attacks method on chaotic cryptosystems Fusen Wanga, Jun Sanga, Qi Liua, Chunlin Huanga, Jinghan Tan MNIST database is used for validation process and multistage CNN is trained with combined pairs of "plaintext-cipertexts". Ruiping Li et al. developed a new image encryption framework which is based on the user fingerprints. Images are encrypted using merhap maps in terms of fingerprints and decrypted only by the authentic user. The fingerprint based encoding technique enhances the security and free from key storage, plaintext attacks, choose text attacks etc. Blockchain storage is also mentioned in the proposed encryption framework for storage of multiple fingerprints Ruiping Li. Haiyun Ma et al. developed a privacy technique for IoT devices which is depended on the cloud environment Haiyun Ma, Zhonglin Zhang. The proposed encoding scheme is segmented based model where privacy data is sliced into distinct segments before encryption initiated. Acquisition time and data properties are focused during the segmentation of private information and encoded using the chaotic maps Stream cipher and dual key algorithms for complete non-destructive conversion between plaintext and ciphertext to ensure the integrity of encrypted information. Deebak et al. created a single user privacy mechanism for medical data privacy B. D. Deebak, Fadi Al-Turjman, Anand Nayyar. Chebyshev chaotic maps are produced with addition and product operations in order to generate the security keys. The proposed single user privacy is focused on medical data which is protected using the symmetric keys.

Proposed Methodology

In this paper, security technique is proposed for computer vision data. Each image is encoded with facial encryption and decrypted using the diffusion process. The developed privacy framework is a hybrid process where logistic chaotic maps are combined with facial features in order to protect the media messages (i.e. images and videos). Figure.1 illustrates the proposed structure with workflow of privacy technique.

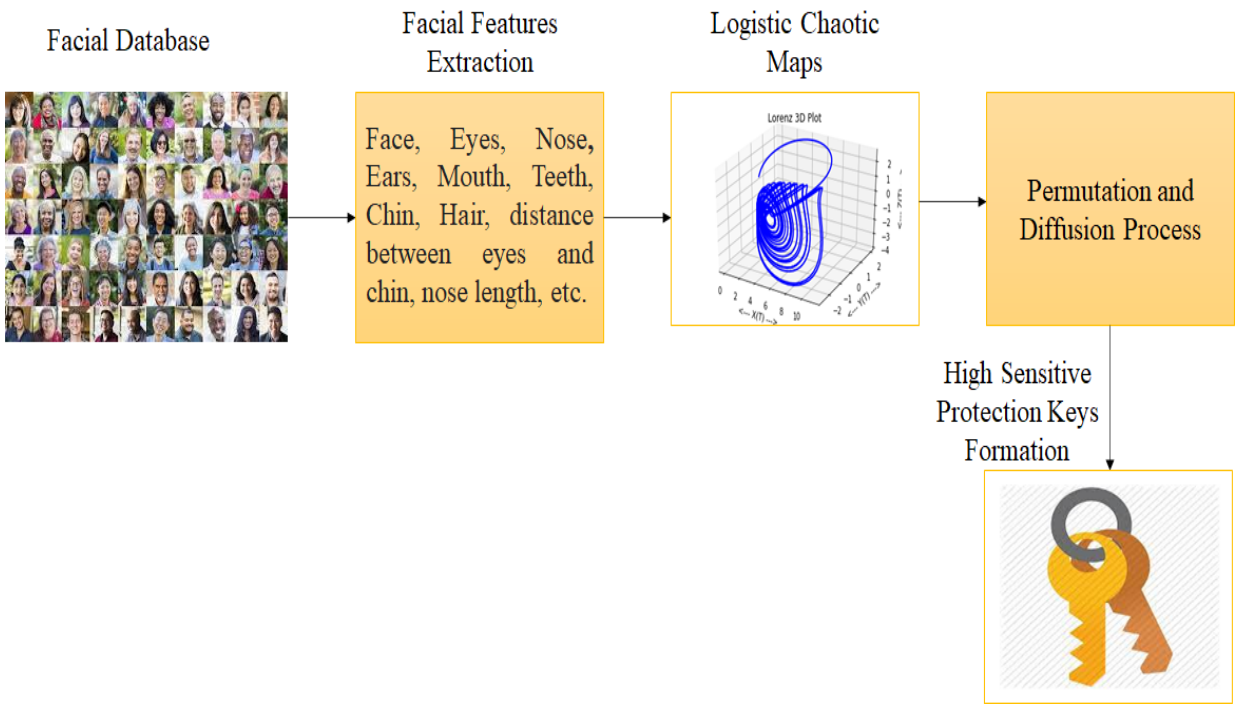

Fig. 1 Proposed structure with workflow of Image encryption process

1. Facial Features Extraction

Various cryptosystems have used the facial expressions for security key generation due to its massive features and different points among each facemask images. Initially, the facial features are extracted in terms of "face size, nose length, eyes shape, jaw distance, ears, teeth, and distance between nose to mouth", etc. These features are collected from random appearances and merged with chaos values before encryption procedure. Figure. 2 illustrate the workflow of facemask feature extraction.

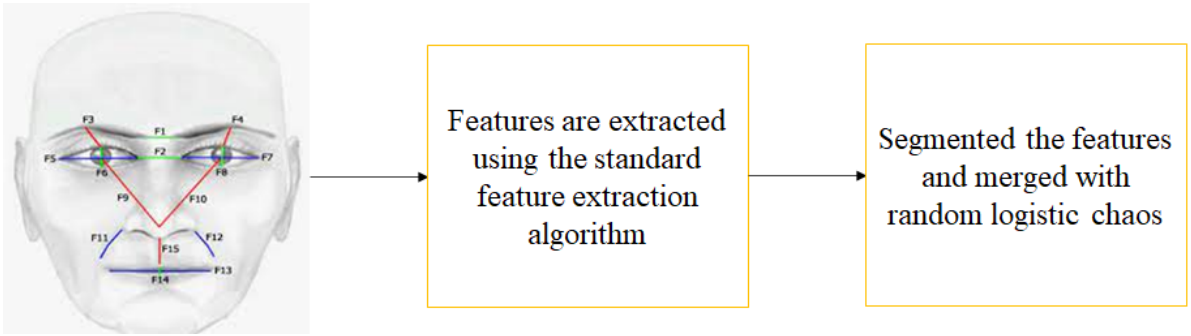

Fig. 2 Feature extraction and segmentation process

The proposed algorithm with a block size of 8 bits applies a wavelet transform to each block for image compression and a 256-bit private key for image encryption. Each merged images are segmented into 3*3 slices for encoding key generation.

2. Proposed Model

- **Hybrid Chaos based Facial Image Encryption and Decryption**

Among the 3 dimensional chaotic maps, the paper makes use of the three-D Lorentz logistic maps for the countermeasure methods. The differential equations for the three-D logistic that are given as comply with as dx/dt = s(y-x) (1)

$$dy/dt = -xz + gy \quad (2)$$
$$dz/dt = -gx + yd \quad (3)$$

in which numerical answers for s= 10, g=20 d=35 offers the chaotic traits of the above equations. The chaotic traits acquired for one of a kind values of s, g and d are proven in figures nine and 10.

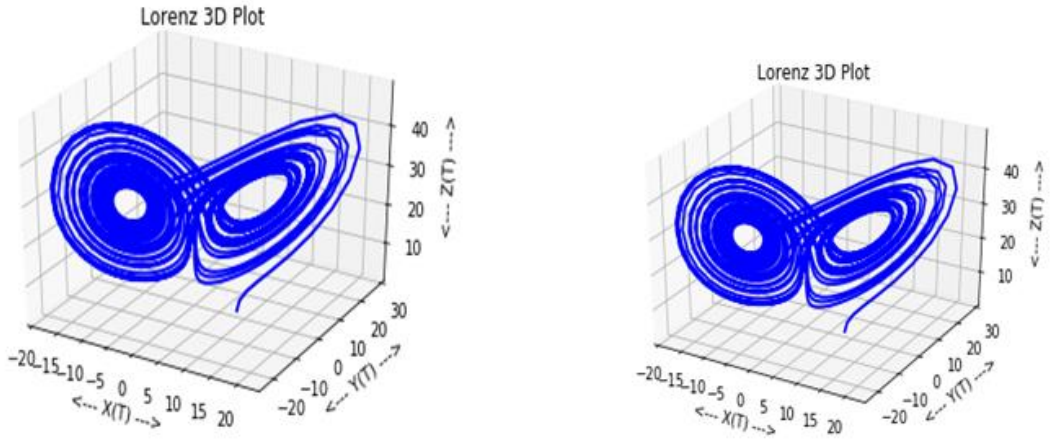

Fig. 3 Logistic Chaotic Maps using Proposed Model

Compared to logistic maps, quantum logistic maps have many superior properties.

(1) Larger key space with 3D system.
(2) Distribute the output more evenly Therefore, the aperiodicity and randomness of the chaotic sequence are improved.

Algorithm 1. Encryption Process using chaos-based facial encryption technique
Step 1: Enter the normal / face image X used for transfer and convert it to a gray scale image (bits) of size M x N
Step 2: Generate a 3D logistic map

Step 3: Perform first level encryption using input images array using permutation process to obtain cipher keys G=(g1,g2,g3,……g_L).
Step 4: Again the Cipher Data are formulated with G matrix which is formed along with the Input Image matrix data using permutation and diffusion to form the High Secured Encrypted Data

Experimental Setup

In this work, facial prints are utilized for confusion process and it has been removed through chaotic maps diffusion procedure. The facial depictions are adopted from standard database called "FERET [25]", "FDDB [26]".

1. FERET Dataset Description

Between August 1993 and July 1996The FERET database was collected in 15 sessions. The database contains a total of 14,126 images, including 1564 image sets, 1199 people and 365 duplicate image sets. The duplicate set is the second set of photos already in the database taken by someone another day. The purpose of the FERET scheme was to create an extensive database of facial images collected independently of the algorithm developer.

George Mason University's Wechsler et al. were chosen to lead the database array. Wechsler and Phillips et al. worked together on the database array. These photos were taken in a semi-controlled environment.

- **FDDB Dataset Description**

FDDB dataset comprises of "2845" This database has a total of 5171 faces and contains images with various problems such as masking, difficult poses, low resolution faces and blurred faces. Specify the area of the face as an elliptical area. Both gray scale and colour images.

Fig. 3 Sample Images adopted from Berg database

Fig. 4 Facial Images used for validation of proposed model

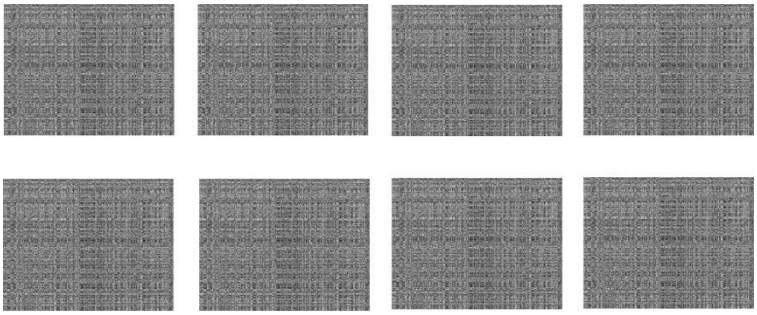

Fig. 5 Encrypted Images obtained using proposed model

Figure.4 illustrates the sample portraits used for evaluation and figure.5 represents the observed encrypted results obtained using the proposed chaotic based image encoding privacy technique. These images are decoded by the authenticated receivers with the mutual authentication keys at the end of diffusion process.

2. Results and Discussion

The developed image encoding technique performance is measured using standard security metrics called "Number of pixels change rate-NCPR", and "unified-average changing Intensity-UACI", and entropy error values are observed for various input facial expressions.

$$NCPR = \sum_{j,i} \frac{O(j,i)}{D_N} * 100\% \quad (1)$$

$$UACI = \sum_{j,i} \frac{|L^1(j,i) - L^2(j,i)|}{(B.D_N)} * 100\% \quad (2)$$

Adjacent Pixels correlation Formulation

$$T(u) = \frac{1}{D_N} \sum_{j=1}^{D_N} u_j \quad (3)$$

$$P(u) = \frac{1}{D_N}\sum_{j=1}^{D_N}\left[u_j - T(u)\right]^2 \quad (4)$$

$$Cov(u,v) = \frac{1}{D_N}\sum_{j=1}^{D_N}\left[u_j - T(u)\right] - \left[v_j - T(v)\right] \quad (5)$$

$$P_{uv} = \frac{cov(u,v)}{\sqrt{P(u)}\sqrt{P(v)}} \quad (6)$$

Entropy Error

$$W(u) = -\sum_{j=1}^{D_N} u_j \, log_2 \, u_j \quad (7)$$

Table 1 Results Observed for Facial Image-1

NPCR and UACI for Mammacial facial Images-1m–Normal Images		
No of Bits Change	NPCR(%)	UACI
10%	99.65%	32.45
20%	99.267%	33.00
30%	99.56	33.23
40%	99.163	33.20
50%	99.64%	33.19
60%	99.64	33.19
70%	99.65	33.15
80%	99.65%	33.14
90%	99.65%	33.12
100%	99.65%	33.10

Table 2 Results obtained for Facial Image-2

NPCR and UACI NPCR Mammacial facial Images-1m –Normal ImagesBenign Images		
No of Bits Change	**NPCR(%)**	**UACI**
10%	99.65%	32.45
20%	99.267%	33.00
30%	99.56	33.23
40%	99.163	33.20
50%	99.64%	33.19
60%	99.64	33.19
70%	99.65	33.15
80%	99.65%	33.14
90%	99.65%	33.12
100%	99.65%	33.10

Table 3 Results obtained for Facial Images

NPCR and UACI for Mammogram MalignNPCR and UACI fo facial Images-3m –Normal Images ant Image s		
No of Bits Change	**NPCR(%)**	**UACI**
10%	99.30%	32.45
20%	99.56%	33.00
30%	99.40%	33.23
40%	99.34%	33.20
50%	99.25%	33.19
60%	99.10%	33.19
70%	99.12%	33.15
80%	99.5%	33.14
90%	99.2%	33.12
100%	99.0%	33.10

Table 4 NCPR and UACI observation for Facial Image-4

NPCRFacial aal facial Images-4 –Normal nd UACI for MRI Ima		
No of Bits Change	**NPCR(%)**	**UACI**
10%	99.0%	29.45
20%	99%	27.67
30%	98.5%	28.9
40%	98%	29.4
50%	99%	29.5
60%	99%	29.4
70%	99.01%	29.5
80%	98.4%	29.6
90%	98.5%	29.8
100%	99%	29.9

Table 5 Results observed for Tumor Depictions

NPCR and UACI for MRI Tumor Images facial Images-5Normal		
No of Bits Change	**NPCR(%)**	**UACI**
10%	99.1%	29.43
20%	99.0%	27.66
30%	99.0%	28.82
40%	98.45%	29.39
50%	99.0%	29.5
60%	98.45%	29.32
70%	99.01%	29.42
80%	98.4%	29.54
90%	98.4%	29.82
100%	98.4%	29.89

Table 6 Results observed for lena depictions

NPCR and UAal facial Images-6 –Normal CI for Lena Images		
No of Bits Change	**NPCR(%)**	**UACI**
10%	98.5%	27.45
20%	98.46%	27.3
30%	98.32%	27.6
40%	98.45%	27.5
50%	98.4%	27.4
60%	98.2%	27.3
70%	98.2%	27.2
80%	98.1%	27.2
90%	98%	27.12
100%	98.%	27.10

Table 7 Results observed for facial images

NPCR and UACI Baboon al facial Images-7Images		
No of Bits Change	**NPCR(%)**	**UACI**
10%	98.5%	27.45
20%	98.46%	27.3
30%	98.32%	27.6
40%	98.45%	27.5
50%	98.4%	27.4
60%	98.2%	27.3
70%	98.2%	27.2
80%	98.1%	27.2
90%	98%	27.12
100%	98.%	27.10

Table 8 NCPR and UACI values obtained for facial depictions

NPCR and UACI Vegetable facial Images-8 images		
No of Bits Change	**NPCR(%)**	**UACI**
10%	98.5%	27.45
20%	98.46%	27.3
30%	98.32%	27.6
40%	98.45%	27.5
50%	98.4%	27.4
60%	98.2%	27.3
70%	98.2%	27.2
80%	98.1%	27.2
90%	98%	27.12
100%	98.%	27.10

Table 9 Adjacent Pixels Correlation Estimation Obtained for proposed privacy model

Image_details	Plain Images			Cipher Images		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Facial Images-1	219.45	109.89	110.567	0.2333	1.6779	2.9000
Facial Images-2	220.67	108.45	101.46	0.03445	0.56778	0.7889
Facial Images-3	89.890	108.67	85.56	0.00900	1.456	3.9090
Facial Images-4	219.45	109.89	110.567	0.2333	1.6779	2.9000
Facial Images-5	220.67	108.45	101.46	0.03445	0.56778	0.7889
Facial Images-6	89.890	108.67	85.56	0.00900	1.456	3.9090
Facial Images-7	90.788	90.444	90.23	0.03445	0.56778	0.7889
Facial Images-8	89.890	89.00	85.56	0.00900	1.456	3.9090

Table 10 Entropy results estimation for 8-facial Images

S.no	Input Image	Entropy
01	Facial Images-1	7.992
02	Facial Images-2	7.992
03	Facial Images-3	7.993
04	Facial Images-4	7.992
05	Facial Images-5	7.993
06	Facial Images-6	7.993
07	Facial Images-7	7.992
08	Facial Images-8	7.994

Conclusion

Since there are no apparent symmetry or periodicity requirements in a chaotic process, it is far more precise in decision making, Suitable for encrypting personal information. Chaos is characterized by a rich hierarchical structure. This white paper takes full advantage of Chaos technology to improve security in image encoding and decryption process. Multimedia, computer vision graphical data privacy are requires the most efficient cryptosystems that is addressed by the proposed chaotic-based facial model. Initially, the facial illustrations are collected from standard database and various features are extracted. The extracted features are merged with logistics maps in order to produce different private keys for encryption purpose. Finally, the encoded images are decrypted using the diffusion process after mutual keys verification. The performance of proposed chaotic-based facial encoding technique is validated with benchmark called FDDB and FEERT facemasks. NCPR, UACI, entropy, adjacent pixels changing metric is estimated using the proposed

low-complex encryption technique. The proposed model achieved better results compared to the traditional algorithms.

References

Ng, T.T., Chang, S.F., Lin, C.Y., & Sun, Q. (2006). Passive blind image forensics. Chapter 15, Multimedia Security Technologies for Digital Rights Management, edited by Zeng, W., Yu, H., and Lin, C.Y.

Phillips, I.E.B., & Ornstein, S. (2011). *Securing Digital Content System and Method.* U.S. Patent 7,979,697B2.

Azzaz, M.S., Tanougast, C., Sadoudi, S., & Bouridane, A. (2013). Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption. *Communications in Nonlinear Science and Numerical Simulation*, *18*(8), 2035-2047.

Hasheminejad, A., & Rostami, M. J. (2019). A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. *Optik*, *184*, 205-213.

Yu, J., Guo, S., Song, X., Xie, Y., & Wang, E. (2020). Image parallel encryption technology based on sequence generator and chaotic measurement matrix. *Entropy*, *22*(1), 76.

Yousif, B., Khalifa, F., Makram, A., & Takieldeen, A. (2020). A novel image encryption/decryption scheme based on integrating multiple chaotic maps. *AIP Advances*, *10*(7).

Albhrany, E.A., Jalil, L.F., & Saleh, H.H. (2016). New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps. *Int. J. Sci. Res. Sci. Eng. Technol. (IJSRSET)*, *2*, 67-73.

Murillo-Escobar, M.A., Meranza-Castillón, M.O., López-Gutiérrez, R.M., & Cruz-Hernández, C. (2020). A Chaotic Encryption Algorithm for Image Privacy Based on Two Pseudo randomly Enhanced Logistic. *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, *884*, 111–136.

Luo, H., & Ge, B. (2019). Image encryption based on Henon chaotic system with nonlinear term. *Multimedia Tools and Applications*, *78*(24), 34323-34352.

Ganeshkumar, D., Suresh, A., & Manigandan, K. (2019). A New One Round Video Encryption Scheme Based on 1D Chaotic Maps. *In 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 439-444.

Yasser, I., Mohamed, M.A., Samra, A.S., & Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. *Entropy*, *22*(11), 1253.

Otoo-Arthur, D., & van Zyl, T.L. (2020). A Scalable Heterogeneous Big Data Framework for e-Learning Systems. *In International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, 1-15.

Abdullah, H.N., & Abdullah, H.A. (2017). Image encryption using hybrid chaotic map. *In International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, 121-125.

Yasser, I., Khalifa, F., Mohamed, M.A., & Samrah, A.S. (2020). A new image encryption scheme based on hybrid chaotic maps. *Complexity*, *2020*.

García-Mata, I., Saraceno, M., Jalabert, R.A., Roncaglia, A.J., & Wisniacki, D.A. (2018). Chaos signatures in the short and long time behavior of the out-of-time ordered correlator. *Physical review letters*, *121*(21).

Pathak, J., Wikner, A., Fussell, R., Chandra, S., Hunt, B.R., Girvan, M., & Ott, E. (2018). Hybrid forecasting of chaotic processes: Using machine learning in conjunction with a knowledge-based model. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *28*(4).

Wang, F., Sang, J., Liu, Q., Huang, C., & Tan, J. (2021). A deep learning based known plaintext attack method for chaotic cryptosystem. *arXiv preprint arXiv:2103.05242*.

Li, R. (2021). Fingerprint-related chaotic image encryption scheme based on blockchain framework. *Multimedia Tools and Applications*, *80*(20), 30583-30603.

Ma, H., & Zhang, Z. (2020). A new private information encryption method in internet of things under cloud computing environment. *Wireless Communications and Mobile Computing*, *2020*. https://doi.org/10.1155/2020/8810987

Deebak, B.D., Al-Turjman, F., & Nayyar, A. (2021). Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. *Multimedia Tools and Applications*, *80*(11), 17103-17128.