2022 5th Information Technology for Education and Development (ITED)

Enhanced Optical Double Phase Image Encryption Using Random Gaussian Noise

Kennedy Okokpujie
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
0000-0002-7594-276X

Damola Gideon Akinola
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
gideon.damolapgs@stu.cu.edu.ng

Innocent Nwokolo
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
innocent.nwokolopgs@stu.cu.edu.ng

Fredrick Olisaemeka
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
olisaemeka.isife@covenantuniversity.edu.ng

Oghorchukwuyem Obiazi
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
oghorchukwuyem.obiazipgs@stu.cu.edu.ng

Oghenetega Owivri
Dept. of Electrical and Information Engineering
Covenant University
Ota, Nigeria
oghenetega.owivripgs@stu.cu.edu.ng

***Abstract*—The advent of digitalization makes image security inevitable as a result of that, an asymmetric cryptography algorithm which is based on the improvement of double random phase encoding is proposed. This algorithm makes use of Gaussian random noise to boost the security of the existing method and was implemented on the MATLAB 2020a software application. The results obtained from the simulations show a slight decrease in the peak-to-signal ratio of 0.3304 and an increase in the mean square error when comparing the existing method with the enhanced method. An image encrypted using Enhanced Double Random Phase Encoding (EDRPE) has strong protection against intruders due to the introduction of the random Gaussian noise as one of the components of the masks in the encryption process. However, a slight noisy effect is produced on the recovered image which is not obvious to the receiver. The simulation result validates the algorithm's potential against security attacks but does not eliminate the presence of noise.**

Keywords—Images, Enhanced Double Random Phase Encoding, Cryptography, Asymmetric, Gaussian Noise

I. Introduction

The advent of digitalization makes the transmission of data or information from one point to another possible and effective, this data could be in the form of voice, text, images, etc. However, this information often encounters security challenges during transmission and may not get to its destination or receiver. Information security is of great importance as the development of multimedia data and communication becomes rapid [1], [2]. Any information security algorithm must be able to meet up with the National Institute of Standards and Technology (NIST) core objectives which include confidentiality, integrity and availability[3] [16]. Confidentiality implies that an authorized disclosure of the information is not permitted, and modification of the information's content without authorization is guarded against which means integrity and availability means that access is not restrained from authorized users. Image encryption is one of the algorithms used in information security that completely changes the sent image into a format that does not represent the nature of the sent image [4] [17]. Image encryption ensures image protection from all sorts of security challenges and can find its application mostly in multimedia systems, medicine, the military, etc. in order to implement an image encryption algorithm techno known as cryptography is used. Cryptography is a process of securing data from intruders during transmission by enhancing its properties or characteristics. The primary aim of cryptography is to protect the original image known as plaintext from third parties or eavesdroppers trying to access the original image[5][18]. The various cryptography algorithms used in image encryption can be categorized into two, these categories include:

- Symmetric or Secret Key Algorithm Cryptography.
- Asymmetric or public key Algorithm Cryptography.

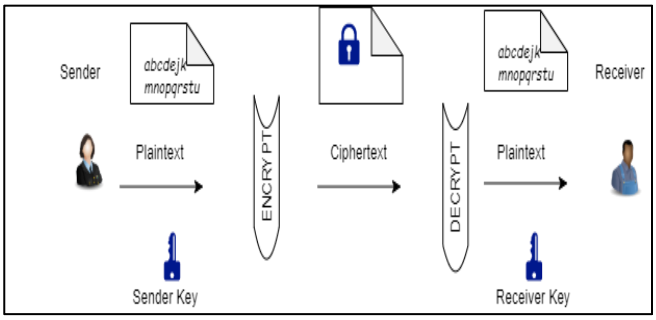


Fig.1: Symmetric key Algorithm

In a symmetric key Algorithm, as shown in Fig. 1, the same key is used by both the sender and receiver to encrypt and decrypt the data respectively while in an Asymmetric key algorithm as shown in Fig.2, two different keys are used, one of the keys is used by the sender to encrypt the data while the other key is used to decrypt the data by the receiver. One major problem encountered in the secret key algorithm is lack of proper management of the key, this problem is solved in the Asymmetric Keys Algorithm due to more keys.

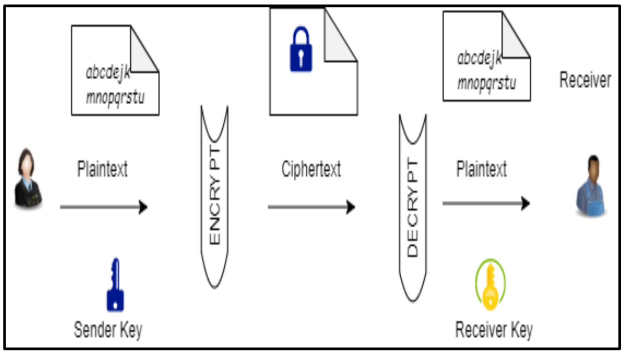


Fig.2: Asymmetric Key Algorithm

Double random phase encoding Algorithm is an example of Asymmetric form of Cryptography. The main idea of this approach depends on inserting two encoding keys (random phase) in a setup called 4f [6]. The setup is an optical system consisting of two cascaded lenses separated by two focal lengths with each of the input and output image planes one focal length outside the lens system from different directions. The decryption process uses the same Fourier Random Phase Mask in the encryption process to recover images.

This paper proposes enhanced method of image encryption using double random phase encoding. The encryption process of the traditional image encryption algorithm is improved with random Gaussian noise function whereby improving on the existing image encryption transmission security.

II. LITERATURE REVIEW

A. *Related Works*

The idea of optical image encryption based double random phase encoding(DRPE) was initiated by Refreiger and Javidi, this asymmetric key algorithm combined two masks to encrypt an image[6], [7]. In this scheme, the input image was covered with a phase mask first and then transformed the resulting output using Fourier transform, for the decryption process, inverse Fourier transformation was performed on the amplitude truncated output of the encrypted to recover the original image[1].The necessity of enhancing their research work stem for the advantages embedded in implementing different image encryption algorithms[4]. The research work carried out by Song and others showed that a single mask or phase encryption algorithm is prone to security attack[8].

An improvement was carried out on the double phase random encoding encryption algorithm[9], this algorithm used discrete cosine transform in place of Fourier transform as the second mask for encryption and inverse discrete cosine transform as a replacement for the inverse Fourier transform. This improved method makes verification of encrypted images convenient. The double random phase encoding can also be strengthen against brute force attack by multiplying the input image's matrix with a quadratic phase factor before performing the encryption[10]. Another method to improve DRPE as implemented by [11] is to encrypt the output of DRPE with the orthogonal matrix . Watermarking algorithms can also be deployed to protect digital media[12],this approach aids clarification of ownership of digital images between senders. Furthermore, implementation of double random encoding using linear canonical transform showed that image encryption algorithms can be strengthen against unauthorized attackers with the introduction of many keys in the encryption process [13].

B. *Existing Double Random Phase Image Encryption (DRPE) Algorithm*

The existing DRPE cryptography algorithm technique makes use of two masks, the first mask i.e., generated from the phasor representation of the image as in equation (1) is used to multiply the original image. The Fourier transform of the scalar multiplication is taken as in equation (2). In order to generate the second mask as in equation (3), scalar multiplication of the phasor representation of the original image and the original image. The inverse Fourier inverse of the resulting output is taken to conclude the encryption process. The original image recovery or decryption process involves two processes, taking the Fourier transform of the encrypted image and performing an inverse Fourier transform on the resulting image as in equation (4).

$$\mathrm{M1}(u, v) = I\,(x, y) * e^{j\,(2\pi n\,(x,y)} \qquad (1)$$

$$C\,(x, y) = FT\,\{\mathrm{M1}(u, v)\} \qquad (2)$$

$$\mathrm{M2}(u, v) = IFT\,\{I\,(x, y) * \mathrm{rand}\,(e^{j\,(2\pi n\,(x, y)})\} \qquad (3)$$

$$\mathrm{P}(x, y) = IFT\{FT\{\mathrm{M2}(u, v) * C(x,y)\}\} \qquad (4)$$

Where:

$I\,(x, y)$ = Amplitude of the original Image,

$\mathrm{M1}(u, v)$ = First generated phase mask,

$e^{j\,(2\pi n\,(x,y)}$ = Phasor equation,

rand() = Random function generator

$\mathrm{M2}(u, v)$ = Second generated phase mask,

$C\,(x, y)$ = Encrypted Image,

$\mathrm{P}(x, y)$ = Decrypted Image

C. *Application of Gaussian Noise in Image Encryption*

In digital image processing, one of the techniques used is the application of noise. These noise functions change the properties of a digital image. Gaussian function generates Gaussian noise that adds noise effect with its probability density function equal to its normal distribution[14][19][20]. The effect of Gaussian's noise is majorly felt on the gray part of an image[15][21][22].

$$f(g) = \left(\sqrt{\frac{1}{2\pi\sigma^2}\,e}\right)^{-(g-\mu)^2/2\sigma^2} \qquad (5)$$

The mathematical model of Gaussian noise as shown above in equation (5) combines the gray value, mean value, and standard deviation value of a digital image. This Gaussian is added to the original image signal to enhance it encryption before the image signal is transmitted.

Where $f(g)$ = Gaussian's noise,

g = image gray value,

μ = mean value,

σ = standard deviation,

e = Euler's number,

π = Mathematical constant

III. METHODOLOGY

In this research work, a new technique that makes use of random Gaussian noise as a replacement to the conventional random signal in DRPE is introduced. The encryption process is strengthened with random Gaussian noise as the component of the second mask as shown in equation (6). The decryption process remains as that of the existing algorithm.

$$M2(u, v) = IFT\ \{I\,(x, y) * \text{rand} * \ f(g) \ * \ (e^{j\,(2\pi n\,(x,\, y))})\} \qquad (6)$$

Fig.3 and Fig.4 depict the models of encryption and decryption processes of the Enhanced optical double image encryption using random Gaussian noise.

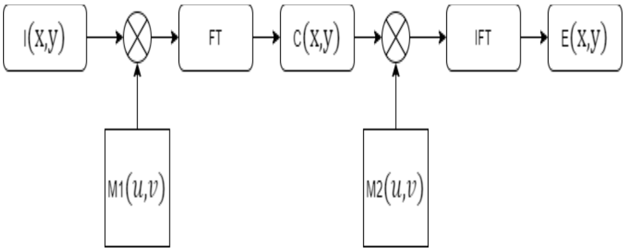


Fig.3: Encryption Process

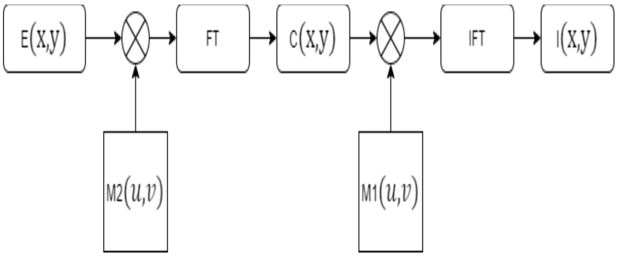


Fig.4: Decryption Process

C. *Simulation*

The implementation of enhanced image encryption using optical double random phase encoding algorithm was carried out using MATLAB 2020a application software graphical user interface. The programming of the algorithm is summarized into three parts:

- Image reading.
- Image encryption.
- Image decryption.

D. *Algorithm of the proposed enhanced method*

The following steps are involved in encrypted process:

Step 1: The input image $I(x, y)$ is multiplied with a random phase mask M1(u, v).

Step 2: The output in Step 1 is Fourier transformed to produce $C(x, y)$.

Step 3: The transformed image $C(x, y)$ is further multiplied with another mask M2(u, v) that has gaussian noise component.

Step 4: The encrypted image E(x, y) is formed by taken the inverse Fourier transform of the output of Step 3.

The following steps are involved in decryption process:

Step 5: The encrypted image E(x, y) is multiplied with the phase mask M2(u, v).

Step 6: The output in Step 5 is Fourier transformed to produce $C(x, y)$.

Step 7: The transformed image $C(x, y)$ is further multiplied with another phase mask M1(u, v).

Step 8: The inverse Fourier transform of the Step 7's output is taken to recover the original image $I(x, y)$.

Fig. 5 give the detail information on how the experiment was carried out in a flowchart.

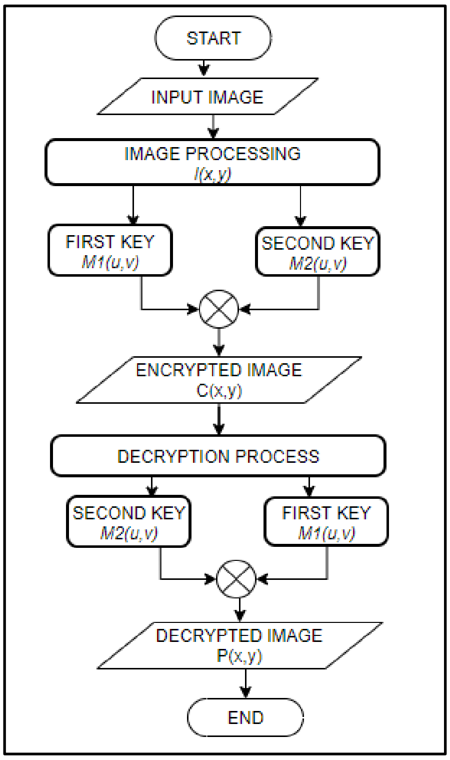
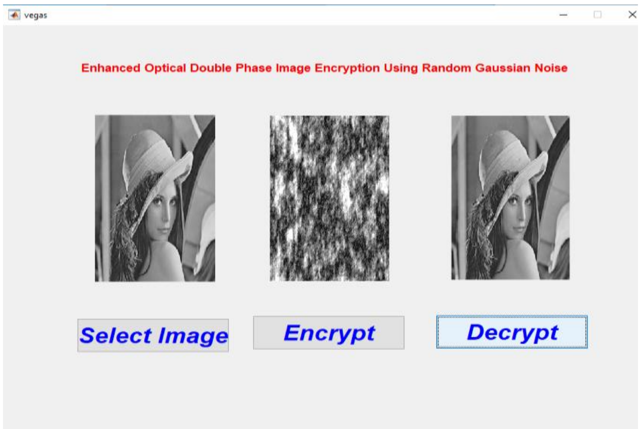


Fig.5: The Flowchart of the proposed methodology

IV. SIMULATION RESULTS AND ANALYSIS

The enhanced asymmetric cryptography algorithm was implemented on MATLAB 2020a's GUIDE integrated development environment. The graphical user interface accepts RGB images of any dimension from the user and resized its dimension into 400 x 256 pixels. For efficient image processing, the resized RGB image was converted to a binary image as shown in Fig.6. Encryption and decryption processes were carried out on the processed image and performance metrics of the processes were evaluated for both the existing method and the proposed method.



Enhanced Optical Double Phase Image Encryption Using Random Gaussian Noise

Fig.6: Implemented enhanced optical double phase encryption using random Gaussian Noise cryptography algorithm on MATLAB.

Fig.6 show the selection, encryption and decryption interface of the simulated processes. While Fig.7 depict the corresponding histogram plots are (a) original image, (b) encrypted image, and (c) decrypted image respectively of the Fig.6.

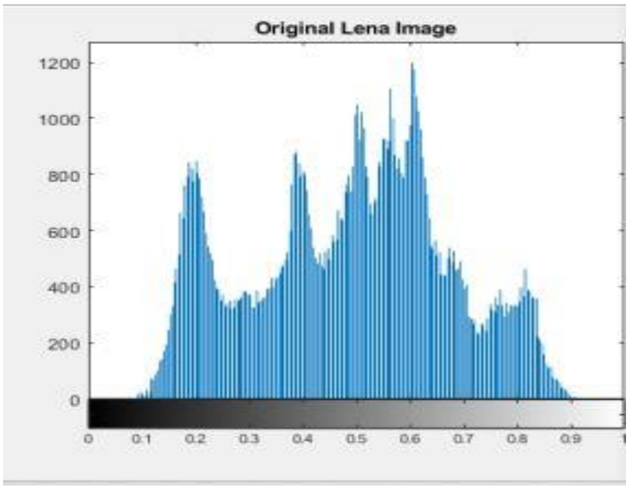


Fig.7: Histogram plots (a) original image

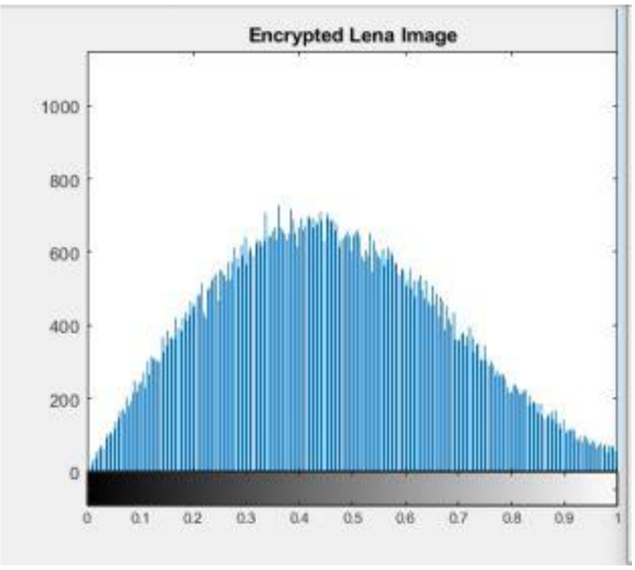


Fig.7: Histogram plots (b) encrypted image.

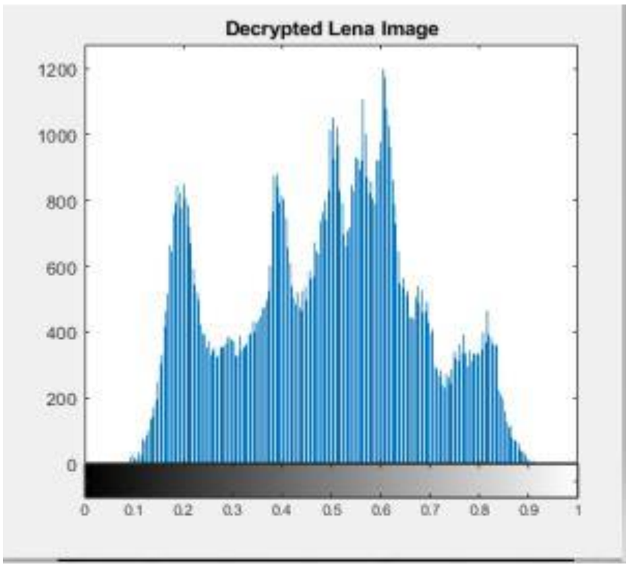


Fig.7: Histogram plots (c) decrypted image.

Fig.7: Histogram plots (a) original image ,(b) encrypted image, and (c) decrypted image.

The performance metrics obtained show a slight decrease in the peak-to-signal ratio of 0.3304, and an increase in the mean square error when comparing the existing method with the enhanced method. The entropy and the structural similarity index measure remain the same as shown in TABLE I.

TABLE I. PERFORMANCE ANALYSIS OF THE ENCRYPTION AND DECRYPTION ROCESSES.

Cryptography Algorithms	**Parameters**				
	Input Image	***Peak-Signal Noise Ratio***	***SSIM***	***Entropy***	***MSE***
DRPE	LENA[a]	313.2970	1	7.4468	$4.68.6X10^{-32}$
EDRPE	LENA	312.9666	1	7.4468	$4.7832X10^{-32}$

V. Conclusion

The enhanced algorithm of DRPE using Gaussian random noise introduces a slight noisy effect on the existing algorithm but maintains the same degree of disorderliness and structural similarity index. An image encrypted using enhanced DRPE has strong protection against intruders due to the introduction of the Gaussian noise as one of the components of the masks. However, a slight noisy effect is produced on the recovered image which is not obvious to the receiver. The simulation result validates the algorithm's potential against security attacks but does not eliminate the presence of noise. In the future, other digital noise other than gaussian noise could be considered for the enhancement of the image encryption algorithm. Furthermore, this algorithm can be improved by applying wavelet transform.

ACKNOWLEDGMENT

We acknowledge the part sponsorship of Covenant University Center for Research and Innovation and Development (CUCRID), Ota, Ogun State, Nigeria.

REFERENCES

[1] H. Singh. (2016, December). Asymmetric image encryption scheme by using random phase masks in Fourier transform domain. In *International Conference on Fibre Optics and Photonics* (pp. W3A-4). Optica Publishing Group., doi: 10.1364/PHOTONICS.2016.W3A.4.

[2] K. Zhou, J. Fan, H. Fan, and M. Li, "Secure image encryption scheme using double random-phase encoding and compressed sensing," Opt. Laser Technol., vol. 121, no. May 2019, p. 105769, 2020, doi: 10.1016/j.optlastec.2019.105769.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice. 2014.

[4] A. Oad, H. Yadav, and A. Jain, "A Review : Image Encryption Techniques and its Terminologies," Int. J. Eng. Adv. Technol., vol. 3, no. 4, pp. 373–376, 2014.

[5] H. Delfs and H. Knebl, Information Security and Cryptography Introduction to Cryptography. 2015.

[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, no. 7, p. 767, 1995, doi: 10.1364/ol.20.000767.

[7] K. Nakano and H. Suzuki, "Analysis of singular phase based on double random phase encoding using phase retrieval algorithm," Opt. Lasers Eng., vol. 134, no. June, p. 106300, 2020, doi: 10.1016/j.optlaseng.2020.106300.

[8] W. Song, X. Liao, D. Weng, Y. Zheng, Y. Liu, and Y. Wang, "Cryptanalysis of phase information based on a double random-phase encryption method," Opt. Commun., vol. 497, no. May, p. 127172, 2021, doi: 10.1016/j.optcom.2021.127172.

[9] Z. Liu, M. L. Yang, and W. Q. Yan, "Image encryption based on double random phase encoding," Int. Conf. Image Vis. Comput. New Zeal., vol. 2017-Decem, pp. 1–6, 2018, doi: 10.1109/IVCNZ.2017.8402486.

[10] P. Yadav, "IMAGE ENCRYPTION USING FRACTIONAL FOURIER," vol. 5, no. 5, pp. 650–655, 2016.

[11] H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," J. Opt. Soc. Korea, vol. 18, no. 3, pp. 201–206, 2014, doi: 10.3807/JOSK.2014.18.3.201.

[12] R. Wolfgang and E. Delp, "Overview of image security techniques with applications in multimedia systems," Proc. SPIE Int. Conf. Multimed. Networks Secur. Displays, Termin. Gateways, Nov, pp. 3228pp297-308, 1997.

[13] A. Sangwan and H. Singh, "A Secure Asymmetric Optical Image Encryption Based on Phase Truncation and Singular Value Decomposition in Linear Canonical Transform Domain," Int. J. Opt., vol. 2021, doi: 10.1155/2021/5510125.

[14] A. Swain, "Noise in Digital Image Processing," pp. 1–9, 2018.

[15] A. Boyat and B. Joshi, "A Review Paper: Noise models in digital image processing," Signal Image Process. An Int. J., vol. 6, no. 2, pp. 63–75, 2015, doi: 10.5958/2455-7110.2018.00010.1.

[16] Omoruyi, O., Okereke, C., Okokpujie, K., Noma-Osaghae, E., Okoyeigbo, O., & John, S. (2019). Evaluation of the quality of an image encrytion scheme. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *17*(6), 2968-2974. DOI: http://doi.org/10.12928/telkomnika.v17i6.10488

[17] Chinonso, O., Omoruyi, O., Okokpujie, K., & John, S. (2017). Development of an Encrypting System for an Image Viewer based on Hill Cipher Algorithm. *Covenant Journal of Engineering Technology*.

[18] O. Kennedy, A. O. Chiamaka, , O. I. Princess, and O. Julius-Olatunji, (2022, April). Implementation of an Embedded Masked Face Recognition System using Huskylens System-On-Chip Module. In 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON) (pp. 1-7). IEEE.

[19] K. Okokpujie, E. Noma-Osaghae, S. N. John, C. Ndujiuba, and I. P. Okokpujie, (2021). Comparative analysis of augmented datasets performances of age invariant face recognition models. Bulletin of Electrical Engineering and Informatics, 10(3), 1356-1367.

[20] K. Okokpujie, S. John, C. Ndujiuba, J. A. Badejo, and E. Noma-Osaghae, (2021). An improved age invariant face recognition using data augmentation. Bulletin of Electrical Engineering and Informatics, 10(1), 179-191.

[21] K. Okokpujie, and S. Apeh, (2020). Predictive modeling of trait-aging invariant face recognition system using machine learning. In Information Science and Applications (pp. 431-440). Springer, Singapore.

[22] K. Okokpujie, S. John, C. Ndujiuba, and E. Noma-Osaghae (2020). Development of an Adaptive Trait-Aging Invariant Face Recognition System Using Convolutional Neural Networks. In Information Science and Applications (pp. 411-420). Springer, Singapore.