A Partial Face Encryption in Real World Experiences Based on Features Extraction from Edge Detection

https://doi.org/10.3991/ijim.v17i07.38753

Raghad Abdulaali Azeez[1(✉)], Abeer Salim Jamil[2], Mohammed Salih Mahdi[3]
[1] Collage of Education Ibn-Rushed for Human Science, University of Baghdad, Baghdad, Iraq
[2] Department of Computer Technology Engineering, Al-Mansour University College, Baghdad, Iraq
[3] Business Information College, University of Information Technology and Communications, Baghdad, Iraq
raghad.azeez@ircoedu.uobaghdad.edu.iq

Abstract—User confidentiality protection is concerning a topic in control and monitoring spaces. In image, user's faces security in concerning with compound information, abused situations, participation on global transmission media and real-world experiences are extremely significant. For minifying the counting needs for vast size of image info and for minifying the size of time needful for the image to be address computationally. consequently, partial encryption user-face is picked. This study focuses on a large technique that is designed to encrypt the user's face slightly. Primarily, dlib is utilizing for user-face detection. Susan is one of the top edge detectors with valuable localization characteristics marked edges, is used to extract features vectors from user faces. Moreover, the relevance of the suggested generating key is led to a crucial role in security improvement by producing them as difficult to intruders. According to PSNR values, the recommended encryption algorithms provided an adequate outcome in the encryption, they had a lower encrypting duration and a larger encrypting impact.

Keywords—dlib, partial encryption, Susan, user face

1 Introduction

As an outcome of the exponential extension of communication technologies, magnificent progresses in connectedness have happened in modern ages; media connection has rapidly be an essential channel of information exchange. However, in terms of network sharing, it shows a serious concealed danger to multimedia networking. As an outcome, image anonymity and protection have been grown in crucial [1-6]. Due to images are a vital side of our lifestyles, and thousands of trillions of images are made, processed, and transferred once a day, image encryption is one of the generality dynamic image authentication manners [7-11]. Image data protection is vital, particularly in the IoT, manufacturing, and health sections. Image encryption is an ultimate exceed-

ingly utilized manners for protecting image transmits[10, 12-17]. Regrettably, celebrated ciphers like GOST, Blowfish, DES, and AES consider as four of the top encryption manners obtainable, however these were not suitable for image encryption. Due to these encryption manners are expensive to compute, they make it impossible to meet the instance for electronic images transmits with vast volumes of data [18-22]. Image is made up of linked items. Encrypting just the linked zone of image is functional than encrypting the integral image that it guides to minimizes processing time [8, 23-27]. The suggested manners may be utilized to improve the secrecy of portable identities for personnel working in offices that call for a top scale of authorisation to register them., When the individual enters the security office, image in identification ought to be encrypted and not vulnerable to modification or adjustment, by the fabricator., to obtain inter permit, the suggested manners decrypts of own image The residue of this search is regulated as follows: portion two debates related working in face detection. Portion three debates dlip and Susan Edge Detector. Portions four and five debates Partial Face Encryption. Portion six debates outcomes. Finally, portion seven, conclusion is debated.

2 Related work

With the growing necessity for security of user face, distinct scientific people have developed distinct encryption manners in this sector. In [25], detected user face utilizing PCA, FFNN and Viola-Jones manner. In [28], as a feature extraction utilized PCA and holistic manner with integral user face, whilst histogram equalization and LBP are disordered manner that utilizes the distinct of local texture descriptors through integral user face [29]. Distinct searches depended on an individual feature as PCA, like [30], that denote user face are turned in Eigen value, that can recognize people facial acts. In [31], they detected user face utilizing SVD and PCA in [32] detected user face utilizing LBP and Gabor. lately, deep learning manners, particularly DCNN, have seen significant success in creating user face identification systems. utilizing MTCNN for trouble of the closed user face detection [33-35], however, utilizing Google Face Net and SVM [36] utilizing augmentation and CNN as a brilliance manner for detecting user face. For encrypting user face, focus on a several distinct investigations: in [37] utilizing LFSR and Haar Wavelet. utilizes the models of chaotic user face [38] utilizing MK-RDA to sympathize peculiar arrangements from chaotic manner, by means of a salience mode, in shuffle and scrambled zone, combining random strategy to run model of chaotic user face. utilizing Homomorphic encryption for keeping the human particularity and dodge data leak from the patterns in [35, 39, 40] utilizing HOG feature and SVM with two kernels (linear and Gaussian) for user face recognition manners. Hiding user face utilizing the complexion people skin detection manner, cluster and YCbCr [41].

3 User face detection

The suggested manners take the master features of user face zone and utilizes them for encrypting user face. The suggested manner's development step covered of two

points: As 1st point, Dlib manner is applied for user-face detection more exactly and rightly; this manner identifies zone of user face from the surroundings. As 2nd point, Susan edge detectors is applied to extract features vectors from user faces [42, 43].

3.1 Dlib face Detection

Dlib is source python package for face Detection and consider as a Facial orientation guessing in agreement with the fundamental thought via discovering 68 landmarks on user face. such as the top portion of the chin, the inner edge of the brows, the outer edge of the eye, the lower point of the nose, and so on as shown in Figure 1 [42-45].

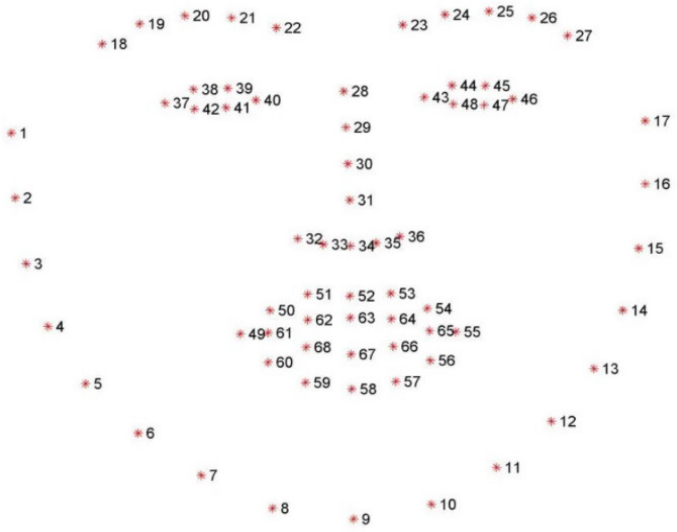


Fig. 1. Dlib Facial Orientation [43]

3.2 Susan edge detectors

Edge Detectors minimizes image info while retaining crucial properties for utilize in subsequent image processes [46]. The strategies for detecting Susan "Smallest Univalue Segment Assimilating Nucleus" edges are the percentage of model with intensity by "nucleus" threshold. SUSAN manner corner is concentration established, that is applied via an orbicular filter of 37 pixels nearly a nucleus for each pixel on image, with no necessity to derivatives of image. When the intensity of each pixel inside a filter is matched to the intensity of the filter's nucleus, zone of the filter with the comparable intensity as the nucleus might be specified. Explain Figure 2, which depicts a black rectangle on a blank backdrop with 5 circle filters in various places on the straightforward image. Corners can be determined according to on the USAN zone. When the zone of USAN is up to the tiny, like status "a," the nucleus is within the corner [44, 46-49].

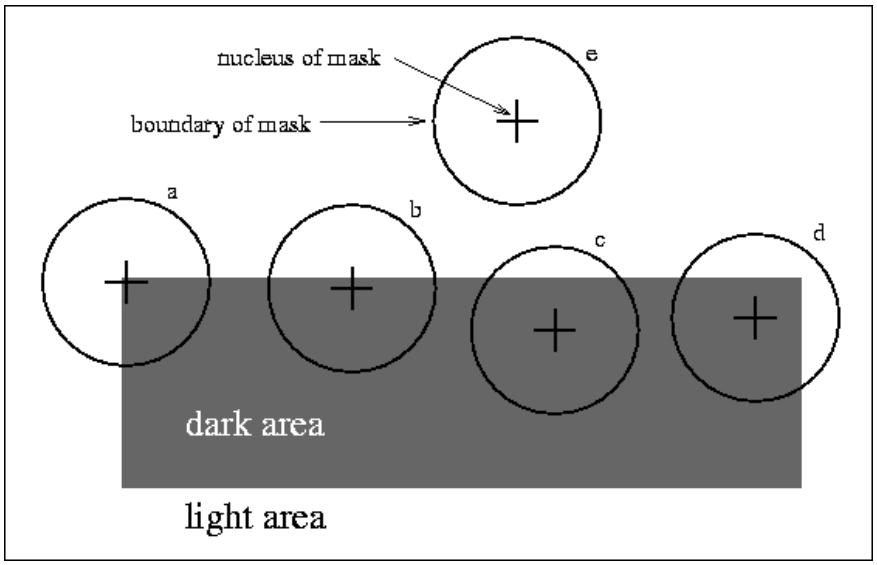


Fig. 2. Four orbicular Filters for explaining Susan Corner

Equation 1 acts an identical comparison task among each pixel on the filter and the filter's nucleus for corners detector.

$$c(r,r0) = \begin{cases} 1, & |I(r) - I(r0)| \le t; \\ 0, & otherwise. \end{cases} \tag{1}$$

r0 is nucleus's ranges and r is the ranges of other pixels on the filter; I(r) is the gray-scale value, c (r, r0) is the comparing outcome t is grayscale distinction threshold that locates the anti-arbitrary capability and the tiny inequality that being extracted via SU-SAN manner. Equation 2 is overwhelmingly utilized due to its adequacy.

$$c(r,r_0) = exp\left(-\left(\frac{I(r)-I(r0)}{t}\right)^6\right) \tag{2}$$

The volume of USAN zone is explain in Equation 3. elementary reply to corners is acquire from Equation 4, that is an appropriate the rule of SUSAN, the tiny USAN zone, the top elementary reply to corners.

$$n(r_0) = \sum_{r \in c(r_0)} c(r,r_0) \tag{3}$$

$$R(r_0) = \begin{cases} g - n(r_0), & n(r) < g \\ 0, & n(r) \ge g \end{cases} \tag{4}$$

g refers to geometric threshold that locates the sharp scale of corner. ultimately, corners being establish via non-maximum inhibition [46, 48-50].

4 Suggested method

A partial facial encryption manner in real world experiences is offered in the suggested manner function. It is ordinarily renowned that with partial encryption, only the relevant zones are specified, and that are purely diffusional. The concept of suggested manner is to encrypt user facial images utilizing colour image intensity. Utilizing dlib detection manner for human face zone. Extraction manner is utilized to detect edge patterns retrieved via Susan manner that utilized to distributed zone concern to gained top feature vector. Suggested strategy increases the eligibility of the encryption manner and decreases the volume of time encryption owing to partial user face encryption. As well, a modern manner for making arbitrary keys is produced for encrypting image. The suggested manner is utilized a relatively massive confidential keys established as volume 16 -16 matrix. In image encrypting, these keys are utilized in feature extraction alteration and replacement procedures for fulfilling an ideal diffusion and confusion features. The diagram Figure 3 below depicts the major phases of the suggested user facial partial encryption manner:

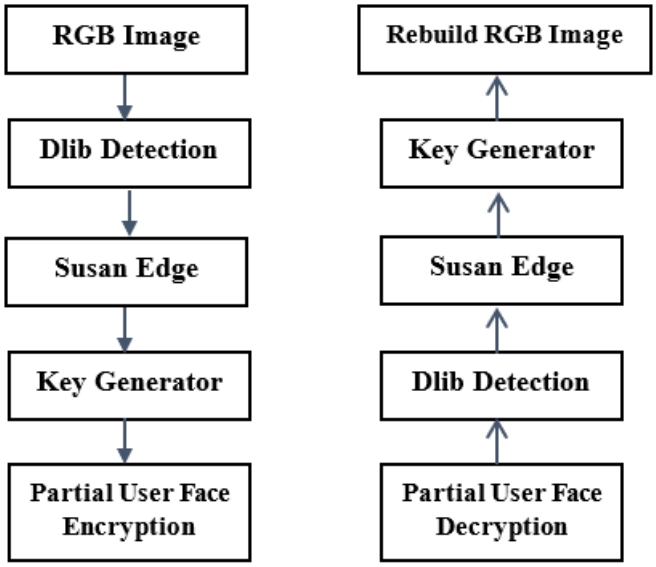


Fig. 3. Suggested User Facial Partial Encryption Manner

In suggested manner, detecting user face zone via applying dlib detection on chosen cases of images as depicts the in Figure 4.

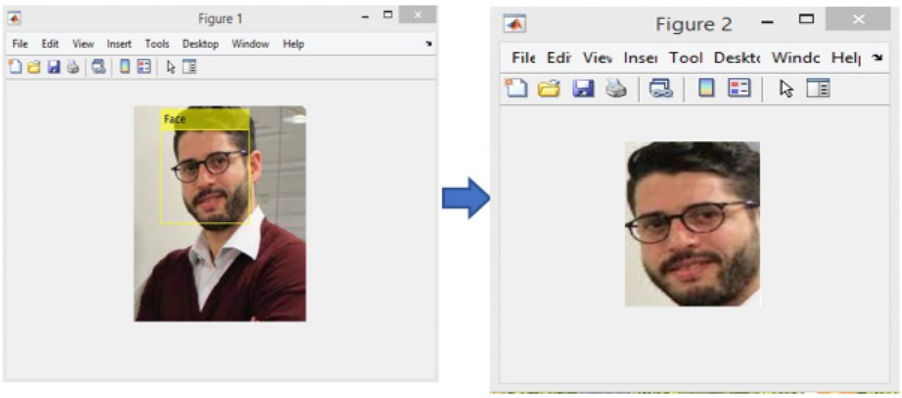


Fig. 4. User Face Zone utilizing Dlib Detection

Susan manner is utilized to locate feature edge due to it is an ideal at extracting criterion information from a variety of visible objects whereas ultimately reducing the volume of info to be address. Utilizing the Susan manner, the lighted pixel is acted as a matrix of feature extraction as depicts in Figure 5.

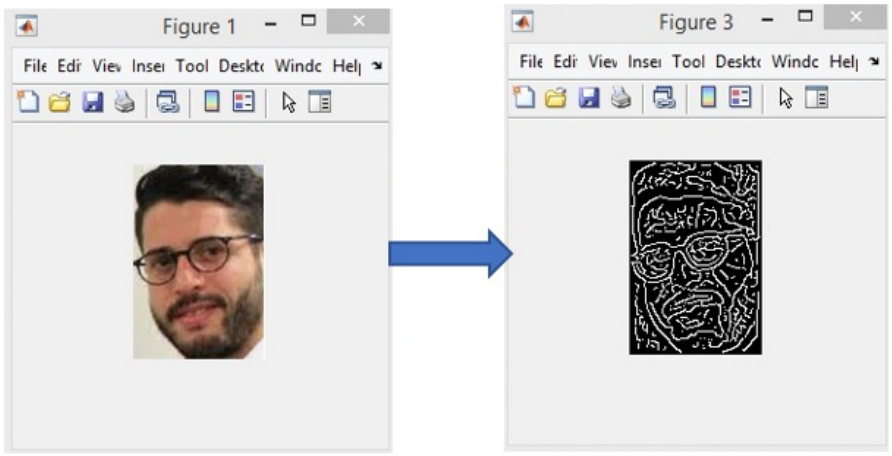


Fig. 5. User Face Zone (Left) and Susan (Right)

In agreement with distinct security investigations, the top worthy part of the encryption procedure for making arbitrary keys, due to an arbitrary make massive keys. As an outcome, rough to break and keep. The crypto key is generated arbitrary from the Susan feature vector; Algorithm 1 depicts making key generation procedures. Randomness tests are utilized to validate the making key. To ensure if the produced key is arbitrary, the outcome of tests was validated and given, demonstrating which created key override arbitrary test and unexpected 0,1 sequences and consequently being utilized strongly.

Algorithm 1 (Generation of Keys)
Susan Edge as Input of Algorithm 1
Keys as Output of Algorithm 1
Start
1. Transform output of Susan Edge image to 0,1 matrix of as 2D.
2. Split 0,1 matrix into windows of equal volume, every window corresponds to 9 items.
3. every window in 0,1 matrix is transformed to decimal value.
4. Make 1-D vector for keeping keys.
Stop

The key is formed from Susan edge manner in the 1st layer of encryption, partial user facial encryption seems after the position of information of the encrypted face zone is combined in the 2nd layer of encryption. Algorithm 2 depicts the processes of partial user facial encryption.

Algorithm 2 (Partial of user Facial Encryption)
Keys as Input of Algorithm 1
Encryption of user Face as Output of Algorithm 1
Start
1. Transform each integer number in output of Algorithm 1 as Follows:
   - From 1 to 149 = Red
   - From 150 to 299=Green
   - From 300 to 511=Blue
2. combine position of encrypted zone user's face.
Stop

5 Results

Suggested manner is be utilized for encrypting images of RGB of whatever volume or form. Depicted in Figure 6, 4 cases images of RGB addressed via suggested manner.

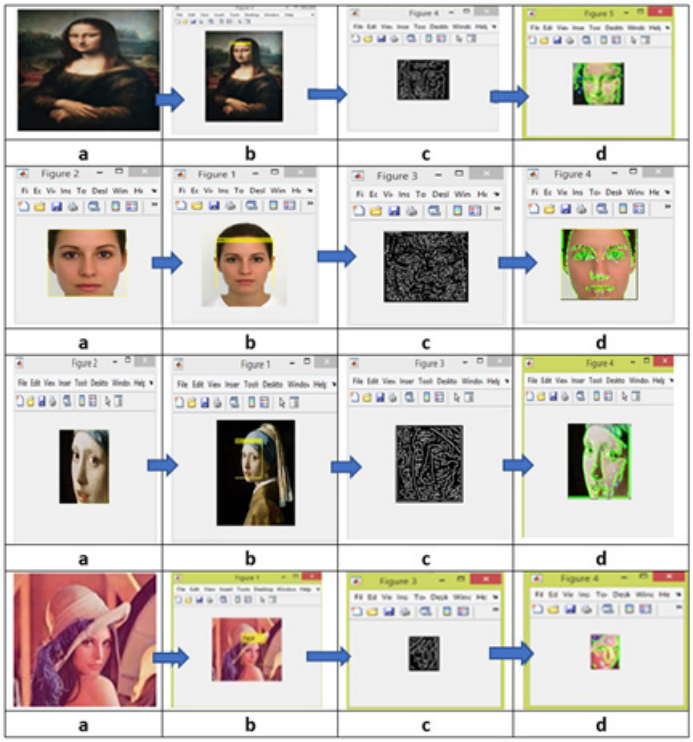


Fig. 6. a-Cases of RGB Images, b-Dlib Face Detection, c- Susan Edge Detector d-Partially User Face Encryption

The usual tests used to evaluate suggestion interpretation: encrypting time of image user face integral and partial. Entropy, and Peak Signal to Noise Ratio (PSNR) as specified in form 5 and 6 respectively [48-52].

$$Entropy = \sum(E(x))\left(\log\frac{1}{E(X)}\right) \tag{5}$$

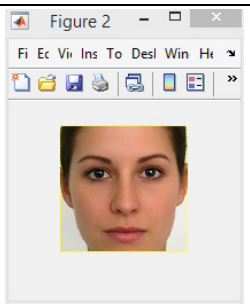
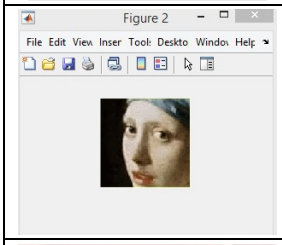
Where E is the probability of an enumeration of x_{th} grayscale.

The greatest conceivable pixel for an 8-bit image is 256 gray-scale, suggesting that complete arbitrary, as predicted in an encrypted image, may take place in the analysed image. that is only possible if each pixel in user face image has a similar probability of being assigned a value range 0 and 255.

$$PSNR = 10 \times \log_{10}\left[\frac{P \times Z255^2}{\sum_{p-1} \mathrm{P} \sum_{z-1} \mathrm{Z} |\int \mathrm{f}(p.z) - \int \mathrm{d}(p,z)|^2}\right] \tag{6}$$

Where, f refers to the main image, d refers to image decrypting. Table 1 depicted usual tests, and entropy and PSNR values for distinct cases of images with a premier user face and distinct of user facial encryption.

Table 1. Usual tests for encryption images

Case of Image	(Integral user Face Encryption Time (Second)	Partial user Face Encryption Time (Second)	Entropy (Encryption Image)	MSE of Image Encryption	PSNR (Image Encryption)	PSNR (Image Decryption)
	6.56	1.87	7.42	66.84	19.6	86.3
	9.87	1.98	7.65	70.60	20.34	83.76
	7.45	1.32	7.60	69.44	20.9	85.82
	9.12	2.30	7.84	69.4	21.34	84.76

6 Conclusion

User confidentiality protection is a theme in overlooking and privacy real world experiences. User face encrypting is being increasingly worthy. The intent of search is encrypting human user face by utilizing user facial partial encryption for rising security

of individual treatment of whatever office in agreement with dlib, Susan to locate encrypted points in user face. The suggested manner utilized feature points for making keys, outcoming in a safer and more efficient encryption. The suggested manner is especially functional ever after it rises security while lowering encryption times, and it is rightly due to it obtains a low PSNR among main and encrypting images.

7 References

[1] S. Zhu and C. Zhu, "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," *Entropy,* vol. 22, no. 7, p. 772, 2020. https://doi.org/10.3390/e22070772

[2] N. F. Hassan, A. Aladhami, and M. S. Mahdi, "Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps," *Iraqi Journal of Science,* pp. 830-842, 2022. https://doi.org/10.24996/ijs.2022.63.2.36

[3] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2021. https://doi.org/10.21533/pen.v10i1.2577

[4] N. F. Hassan, R. A. Azeez, and M. S. Mahdi, "Video Watermarking, Theories and Robustness Issues," *Journal of Al-Ma'moon College,* no. 36, 2021.

[5] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[6] H. T. Salim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[7] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy,* vol. 21, no. 3, p. 319, 2019. https://doi.org/10.3390/e21030319

[8] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," *Periodicals of Engineering Natural Sciences,* vol. 8, no. 4, pp. 2138-2145, 2020.

[9] H. K. Tayyeh, M. S. Mahdi, and A. A. AL-Jumaili, "Novel steganography scheme using Arabic text features in Holy Quran," *Int. J. Electr. Comput. Eng,* vol. 9, no. 3, p. 1910, 2019. https://doi.org/10.11591/ijece.v9i3.pp1910-1918

[10] M. S. Mahdi and N. F. Hassan, "Design of keystream Generator utilizing Firefly Algorithm," *Journal of Al-Qadisiyah for computer science mathematics,* vol. 10, no. 3, pp. Page 91-99, 2018. https://doi.org/10.29304/jqcm.2018.10.3.441

[11] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 2, pp. 12-20, 2022.

[12] S. Zhu, C. Zhu, and W. Wang, "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy,* vol. 20, no. 9, p. 716, 2018. https://doi.org/10.3390/e20090716

[13] M. Mahdi and N. Hassan, "A suggested super salsa stream cipher," *Iraqi Journal for Computers Informatics,* vol. 44, no. 2, pp. 5-10, 2018. https://doi.org/10.25195/ijci.v44i2.51

[14] C. Fu, G.-y. Zhang, M. Zhu, Z. Chen, and W.-m. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," *Security*

and Communication Networks, vol. 2018, pp. 1-13, 2018. https://doi.org/10.1155/2018/2708532

[15] a. N. F. H. Mohammed Salih Mahdi, "Proposed an Efficient Secure Healthcare IoE," *University of Technology, PhD Thesis, Baghdad, Iraq,* 2019.

[16] C. Revanna and C. Keshavamurthy, "A new partial image encryption method for document images using variance based quad tree decomposition," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 1, pp. 786-800, 2020. https://doi.org/10.11591/ijece.v10i1.pp786-800

[17] M. S. Mahdi and N. F. Hassan, "A proposed lossy image compression based on multiplication table," *Kurdistan Journal of Applied Research,* vol. 2, no. 3, pp. 98-102, 2017. https://doi.org/10.24017/science.2017.3.34

[18] A. Kadhim and M. Salih, "Proposal of new keys generator for DES algorithms depending on multi techniques," *Engineering Technology Journal,* vol. 32, no. 1 Part (B) Scientific, 2014.

[19] A. Farhan and M. Mahdi, "Proposal dynamic keys generator for DES algorithms," *islamic college university journal,* vol. 29, pp. 25-48, 2014.

[20] M. MS, "Proposed block cipher algorithm with cloud computing based on keys generator," *MS Thesis, University of Technology, Iraq,* 2013.

[21] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[22] A. S. Mohamad, "Data encryption for bank management system: Data encryption for bank management system," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 4, pp. 14-20, 2022.

[23] A. M. Duhaim, S. O. Al-Mamory, and M. S. Mahdi, "Cheating detection in online exams during COVID-19 pandemic using data mining techniques," *Webology,* vol. 19, pp. 1-26, 2021. https://doi.org/10.14704/WEB/V19I1/WEB19026

[24] R. a. M. Al_airaji, I. A. Aljazaery, and A. H. M. Alaidi, "Automated Cheating Detection based on Video Surveillance in the Examination Classes," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 8, 2022. https://doi.org/10.3991/ijim.v16i08.30157

[25] N. T. Deshpande, S. J. A. i. C. S. Ravishankar, and Technology, "Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN," vol. 10, no. 5, pp. 1173-1189, 2017.

[26] J. Kh-Madhloom, "Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 2, pp. 21-33, 2022.

[27] J. Q. Kadhim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET),* vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[28] A. F.-. Dubois, "recognition using deep neural networks," *Master Thesis,* 2018.

[29] S. I. Mohammed, N. A. Jaafar, and K. M. Hussien, "Face Recognition Based on Viola-Jones Face Detection Method and Principle Component Analysis (PCA)," *Iraqi J. Comput. Commun. Control Syst. Eng,* vol. 18, no. 3, pp. 52-59, 2018. https://doi.org/10.33103/uot.ijccce.18.3.6

[30] Q. Zhang, H. Li, M. Li, and L. Ding, "Feature extraction of face image based on LBP and 2-D Gabor wavelet transform," *Math. Biosci. Eng,* vol. 17, no. 2, pp. 1578-1592, 2020. https://doi.org/10.3934/mbe.2020082

[31] P. Anusha, K. Prasad, G. Kumar, E. Lydia, and V. Parvathy, "Facial detection implementation using principal component analysis (pca)," *Journal of Critical Reviews,* vol. 7, no. 10, pp. 1863-1872, 2020.
[32] M. S. Mahdi, "Computer aided diagnosis system for breast cancer using ID3 and SVM based on slantlet transform," *QALAAI ZANIST JOURNAL,* vol. 2, no. 2, pp. 142-148, 2017. https://doi.org/10.25212/lfu.qzj.2.2.16
[33] F. Ayiah-Mensah, L. Asiedu, F. O. Mettle, and R. Minkah, "Recognition of augmented frontal face images using FFT-PCA/SVD algorithm," *Applied Computational Intelligence and Soft Computing,* vol. 2021, pp. 1-9, 2021. https://doi.org/10.1155/2021/6686759
[34] B. H. Majeed, "Effect of Augmented Reality Technology on Spatial Intelligence among High School Students," *International Journal of Emerging Technologies in Learning (Online),* vol. 17, no. 24, p. 131, 2022. https://doi.org/10.3991/ijet.v17i24.35977
[35] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," *Wasit Journal of Computer and Mathematics Science,* vol. 1, no. 3, 2022.
[36] P. Wu, "Masked face recognition using convolutional neural network," 2022. https://doi.org/10.1109/ICCSI55536.2022.9970601
[37] Z. Pei, H. Xu, Y. Zhang, M. Guo, and Y.-H. Yang, "Face recognition via deep learning using data augmentation based on orthogonal experiments," *Electronics,* vol. 8, no. 10, p. 1088, 2019. https://doi.org/10.3390/electronics8101088
[38] H. R. Shakir, L. E. George, and G. K. Tuma, "Partial encryption for colored images based on face detection," *International Journal,* vol. 5, no. 8, 2015.
[39] R. Jiang, S. Al-Maadeed, A. Bouridane, D. Crookes, and M. E. Celebi, "Face recognition in the scrambled domain via salience-aware ensembles of many kernels," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 8, pp. 1807-1817, 2016. https://doi.org/10.1109/TIFS.2016.2555792
[40] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018: IEEE, pp. 1-10.
[41] M. Kitayama and H. Kiya, "HOG feature extraction from encrypted images for privacy-preserving machine learning," in *2019 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, 2019: IEEE, pp. 80-82. https://doi.org/10.1109/ICCE-Asia46551.2019.8942217
[42] H. A. Hosni Mahmoud and H. A. Mengash, "A novel technique for automated concealed face detection in surveillance videos," *Personal and Ubiquitous Computing,* vol. 25, pp. 129-140, 2021. https://doi.org/10.1007/s00779-020-01419-x
[43] H. Zhou, P. Chen, and W. Shen, "A multi-view face recognition system based on cascade face detector and improved Dlib," in *MIPPR 2017: Pattern Recognition and Computer Vision*, 2018, vol. 10609: SPIE, pp. 37-42. https://doi.org/10.1117/12.2282829
[44] Y. Feng, J. Zhang, and S. Wang, "A new edge detection algorithm based on Canny idea," in *AIP Conference Proceedings*, 2017, vol. 1890, no. 1: AIP Publishing LLC, p. 040011. https://doi.org/10.1063/1.5005213
[45] N. Boyko, O. Basystiuk, and N. Shakhovska, "Performance evaluation and comparison of software for face recognition, based on dlib and opencv library," in *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, 2018: IEEE, pp. 478-482. https://doi.org/10.1109/DSMP.2018.8478556
[46] J. Chen, L.-h. Zou, J. Zhang, and L.-h. Dou, "The Comparison and Application of Corner Detection Algorithms," *Journal of multimedia,* vol. 4, no. 6, 2009. https://doi.org/10.4304/jmm.4.6.435-441

[47] S. M. Smith and J. M. Brady, "SUSAN—a new approach to low level image processing," *International journal of computer vision,* vol. 23, no. 1, pp. 45-78, 1997. https://doi.org/10.1023/A:1007963824710

[48] A. S. Jamil, R. A. Azeez, and N. F. Hassan, "An Image Feature Extraction to Generate a Key for Encryption in Cyber Security Medical Environments," *International Journal of Online & Biomedical Engineering,* vol. 19, no. 1, 2023. https://doi.org/10.3991/ijoe.v19i01.36901

[49] A. S. Jamil, R. A. Azeez, A. Al-Adhami, and N. F. Hassan, "Multibiometric System with Runs Bits Permutation for Creating Cryptographic key Generation Technique," *Iraqi Journal of Science,* pp. 452-468, 2023. https://doi.org/10.24996/ijs.2023.64.1.40

[50] A. S. Jamil and A. M. S. Rahma, "Image Encryption Based on Multi-Level Keys on RC5 Algorithm," *iJIM,* vol. 16, no. 17, p. 101, 2022. https://doi.org/10.3991/ijim.v16i17.34335

[51] D. Salomon, *Data compression: the complete reference*. Springer Science & Business Media, 2004.

[52] S. E. Umbaugh, *Digital image processing and analysis: human and computer vision applications with CVIPtools.* CRC press, 2010. https://doi.org/10.1201/9781439802069

8 Authors

Assist. Prof. Dr. Raghad Abdulaali Azeez received BSc degree in computer science in 1987 from university of technology, department of computer science. Her MSc. in Computer Science from Information Technology Unit, Collage of Education Ibn-Rushed for Human Science, University of Technology, Iraq, 2002 and PhD. in Computer Science from Iraqi Commission for Computers and Informatics / Institute for Postgraduate Studies, 2006. She has around 25 years of teaching experience. Her areas of interest's are computer security, steganography and image processing.

Assist. Prof. Dr. Abeer Salim Jamil received the MSc. and PhD. in Computer Science from University of Technology, Iraq, 2004 and 2015 respectively. She has around 24 years of teaching experience and 11 years teaching in Cisco Network Academic (CISCO). Her areas of interests are Digital Image Processing, Video Processing, Security, software Engineering, Networking and artificial intelligence applications. She can be contacted at email: abeer.salim@muc.edu.iq.

Assist. Prof. Dr. Mohammed Salih Mahdi is currently Asst.Prof.Dr. in Business Information College, University of Information Technology and Communications, Iraq. His BSc degree in hiding data in 2010 and his MSc degree in a security of cloud computing in 2012 and his PhD degree in a security of IoE in 2019 from Computer Science department, University of Technology, Iraq. His research interests include Data Security, steganography, Image Processing, Data Compression, Artificial Intelligence, Data Mining, Machine Learning, Deep Learning, Internet of Things, Cloud Computing, Quantum Computing and blockchain technology.

Article submitted 2023-01-17. Resubmitted 2023-03-02. Final acceptance 2023-03-05. Final version published as submitted by the authors.