ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20231210183347

Original scientific paper
Received: 2023-12-10, Accepted: 2024-01-15

Detect People's Faces and Protect Them by Providing High Privacy Based on Deep Learning

Mauj Haider AbdAlkreem, Ruaa Sadoon Salman*, Farah Khiled Al-Jibory

Abstract: Facial privacy is essential in our time due to the violations that occur due to the proliferation of social media and people's primary dependence on it. Facial features can be exploited to identify, track, or other matters without obtaining prior consent. This is increasingly important due to the increasing use of facial recognition technologies. Protecting the face and privacy is a challenging task, as the entire world is very widely connected through social networking sites in an uncensored manner, especially in countries with no electronic governance or oversight. Therefore, there is an urgent need to provide systems or research that focuses on the issue of facial privacy. In this paper, a system for providing privacy for people was proposed using the WIDER FACE data set, considered the most important among the data sets. The system aims to provide privacy for people by determining the destination that must be preserved and provided with privacy through three technical. The approach goes through several steps: The processing process of the image is achieved by enhancement of the images that are input in the training stage and then dividing the data into a test and training set, and the training stage through the YOLOv6 algorithm (looks only once), and privacy operations including encryption, decryption, mask and blurring in the test part of the data, and conducting an external test for personal photo. The final results of the proposed system were as follows: accuracy = 0.98 in training and 0.96 in testing.

Keywords: deep learning; facial; image; privacy; YOLOv6

1 INTRODUCTION

The privacy of people's faces in images is one of the essential topics that researchers are working on at present and shortly due to the increasing use of social networking sites, the Internet and various programs [1]. Various cases of privacy violations have emerged, including impersonation of people by changing facial images and through fake videos as well, as well as cases of security breaches by tracking people through their published images, or it is possible to use people's details such as faces in biometric fingerprints in very high-resolution photos, and on the other hand [2]. It violates privacy on social networking sites and programs when sending images [3]. Therefore, all of these reasons were enough to make researchers work on how to provide privacy for people in pictures. Facial privacy refers to the right to exercise authority over collecting, using, and disclosing personal data obtained from an individual's facial features. This includes both facial images and facial recognition data, which refers to a mathematical depiction of an individual's face that can be used for identification purposes [4]. The increasing prevalence of facial recognition technology has raised concerns about protecting facial privacy [5]. Facial recognition technology is currently used in many fields, such as law enforcement, surveillance, and marketing. However, facial recognition technology raises several privacy concerns [6]. The concern is that facial recognition technologies can surreptitiously monitor individuals without consent. This dramatically limits the ability to move and express oneself, which may cause feelings of fear or intimidation [7]. Another problem arises from the possibility that facial recognition systems engage in discriminatory practices. Facial recognition technologies have shown less accuracy in identifying individuals of colour. This may result in individuals from marginalized racial and ethnic groups being subject to a greater degree of scrutiny and discrimination by law enforcement or facing barriers to accessing essential services. There is a legitimate concern that facial recognition data may be vulnerable to hacking or misuse. This could lead to identity theft or other types of damage. Given these issues, there are increasing efforts to protect individuals' facial privacy [8]. Many jurisdictions have implemented legislation or regulations limiting the use of facial recognition technology. California legally mandates that companies obtain consent before collecting or using facial recognition data [9]. This paper proposes a method to provide privacy by relying on face protection using three protected image techniques to provide face privacy through a deep learning algorithm (YOLOv6). This paper has been organized with clarification sections around how to detect faces and how the protection process is carried out through the face in the image, and a section that highlights the most important previous studies that had high citations and high results. The last section of the paper is an integrated part that is the proposed approach and the method for evaluating the results and drawing conclusions from this.

2 FACE RECOGNITION

Face recognition is a technique that involves recognizing or confirming the identification of a person by analyzing their facial features [10]. Face recognition systems can identify individuals in photographs, videos, or real-time. Mobile devices can be utilized by law enforcement to identify individuals during police stops [11]. However, face recognition data is susceptible to inaccuracies, which might falsely incriminate individuals for crimes they did not commit. Facial recognition software exhibits significant deficiencies in accurately identifying African Americans, other ethnic minorities, women, and young individuals [12]. It frequently misidentifies or fails to recognize these groups, disproportionately impacting specific demographics.

Moreover, facial recognition technology has been employed to specifically identify individuals who are participating in activities that are safeguarded under the right to freedom of speech. Face recognition technology is

expected to become increasingly prevalent shortly [13]. It can be utilized to monitor the activities of humans in the outside world, similar to how automatic license plate scanners track vehicles based on their plate numbers [14]. Face recognition systems employ computer algorithms to identify unique and distinguishing characteristics of an individual's face. Subsequently, these specific characteristics, such as the intraocular distance or the contour of the chin, are transformed into a mathematical depiction and juxtaposed with information from other facial profiles stored in a face recognition database [15]. A face template refers to the specific data about a face [16]. It is different from an image as it is specifically created to contain just certain information that can be utilized to differentiate one face from another [17]. Specific facial recognition systems are programmed to compute a probability match score between an unidentified individual and particular face templates recorded in the database rather than providing a definitive identification [18]. These systems will provide multiple potential matches, arranged in order of the probability of accurate identification, instead of only delivering one outcome [19]. Face recognition systems exhibit variability in their capacity to accurately identify individuals under challenging circumstances, such as inadequate illumination, low image resolution, and unfavourable viewing angles (e.g., a snapshot taken from above, capturing an unfamiliar person) [20].

3 PERSONAL PRIVACY VIOLATIONS IN IMAGES

Personal privacy in images is the right to control the collection, use and disclosure of photos that contain personal information about a person [21]. This includes physical images, such as photographs and videos, and digital images, such as those stored on computers and smartphones. The matter is fraught with numerous hurdles and obstacles, which can be succinctly where Facial recognition technology enables the identification and monitoring of individuals in public spaces and the ability to track their movements and unlock their mobile devices [22]. This technology can be employed to surveil individuals' actions, namely to tailor advertisements to them or trace their movements for illicit intentions. Facial recognition technology can potentially discriminate by targeting individuals based on their colour, ethnicity, gender, or other legally protected attributes [23]. For instance, it can be employed to restrict individuals' entry to employment, housing, or other advantageous prospects.

Furthermore, Cyber-attacks target recognition data, such as faces or bodily parts, due to their high value. In the event of data theft, the stolen information might be exploited for purposes such as identity impersonation, fraudulent activities, or even stalking [24]. Insufficient transparency is frequently, individuals are uninformed of the fact that their bodily components are being subjected to scanning or tracking. The absence of transparency might provide challenges for individuals in understanding the utilization of their data and safeguarding their privacy [7].

4 RELATED WORK

There are many studies on this topic, and the following are the most important studies related to the topic [25]. This study explores when users openly release photographs and videos of others to address privacy concerns. A mechanism for recognizing and filtering human traits in public photographs and videos is presented to safeguard privacy. The suggested method uses face filtering to improve privacy without affecting image sharing by considering visual content. The suggested system first recognizes a person's facial shape in a digital image or video. The software compares specified facial traits to its facial vector database. After face recognition, the suggested approach removes unrecognized people from the image. (Convolutional Neural Network - CNNs) have been utilized for face detection, whereas deep learning face embedding has been employed for face recognition. Both methods have high accuracy and are practical. Time. Gaussian face filtering, significantly blurring, is standard. For fast-processing applications, this approach is famous for its real-time performance. Users can also adjust distortion levels. Experimental results on three datasets show that the system can accurately identify faces in images and movies. Improved CNNs for facial detection achieve 91.3 % accuracy. The system uses the K-Nearest Neighbor (KNN) technique for facial recognition and scored 96.154 % on the I Privacy dataset. In ref. [24] a basic image privacy system and an improved disturbance generation network algorithm are introduced. Experiments show that generative networks may efficiently create adversarial perturbation while maintaining image quality. Candidate region filters during generative network training reduce interference from bad training samples and improve adversarial sample detection protection. Maintain image quality by cleverly preventing Deep Neural Network (DNN) detectors from detecting sensitive information like human features. Create an image privacy method by training and creating adversarial samples for each image to defend DNN detectors. Consider training an adversarial perturbation generative network to improve the prior model instead of training for each Image. Comparing the technique to others using mean average precision, average distortion, and time expended on a more extensive face dataset. The study found that the method upsets DNN detectors without affecting image quality. Additionally, the upgraded model generates adversarial perturbations faster. In ref. [26], a reversible facial recognition privacy method is proposed. Before uploading face photos to the cloud, apply a mosaic and train an encoder to create protected images using the original facial data. We'll train another classifier with protected photos for facial expression detection and create a decoder to restore the original facial images. Using protected images in cloud services limits malicious attackers' identifying information. The classifier can help low-privilege users conduct computer vision tasks with protected images. Authorized users' average facial photo use will not change after content recovery. Experimental results show that the facial image restoration method works. Furthermore, shielded images perform similarly in typical computer vision

tests. In ref. [27] proposed artefact removal Privacy-preserving blurring (DartBlur) uses a DNN architecture for feature blurring. DartBlur hides facial privacy and detection artefacts. It includes four training objectives to improve review and enhance the detection of artefact suppression. Add it to a second-order optimization pipeline and adversarial training scheme. WIDER FACE allows DartBlur to surpass the current face-replacement method in review convenience, accessibility, and training artefact suppression compared to blur-based methods. Tab. 1 summarises the related work mentioned above.

Table 1 Summarized of Previous Studies.

Year & RF.	Employed method	Method dataset	Aim of paper	Result of system
2020 [25]	- CNN (detect the face region) - (Determined Maximum Likelihood -DML) was used for the feature extraction stage - (Support Vector Machine-SVM) and (KNN) were used for the face classification	- Grimace - FEI - I-Privacy - WIDER face	Use real-time facial recognition and blurring. OpenCV was used to create facial recognition algorithms. A CNN algorithm was pre-trained to identify facial regions. Pre-trained Deep Metric Learning (DML) extracted features next. Face recognition employs SVM and KNN for classification.	SVM accuracy = 88.462 %, and KNN accuracy = 96.154 %
2021 [24]	- Faster R-CNN with (Visual Geometry Group -VGG-16 as the feature extractor - Deep neural network (DNN) detectors from detecting private information	- PASCAL VOC - visual object - WIDER face(set 100 randomly selected images in the simple verification set as test data set to verify the effectiveness of the improved algorithm)	Present an approach to prevent deep neural network (DNN) detectors from recognizing private information, such as human faces, while maintaining image quality. Specifically, provides an image privacy protection algorithm by training and creating adversarial samples for each image to defend the DNN detector.	- PASACL VOC mAP = Original image = 90 Gaussian blur = 89 Mosaic = 81 - WIDER face mAP = Original image = 83 Bose model = 35
2021 [26]	- Face detection (YOLO) - CNN AS classifier - Encoder and decoder both use U-Net	- CelebA for training - WIDER FACE (training YOLO for face detection) - (Labeled Faces in the Wild Home -LFW) for testing only	Transforms original photographs into protected images with face information before uploading to the cloud. Cloud photos can be used for facial expression recognition and restored to original photographs; attackers cannot identify individuals.	Accuracy Original image = 93.0702 % Protected Images = 92.9864 %
2023 [27]	- YOLOv5 - PyramidBox	- WIDER FACE - FDDB - Crowd Human	The blur-based DartBlur approach balances accessibility, review convenience, and artefact suppression. According to experiments, DartBlur meets design goals and generalizes well across datasets and systems.	PyramidBox DartBlur per. Fid = 95.18 Post-hoc Fid = 75.16 Cycle Fid = 24.68 YOLOv5 DartBlur per. Fid = 96.17 Post-hoc Fid = 91.72 Cycle Fid = 37.15

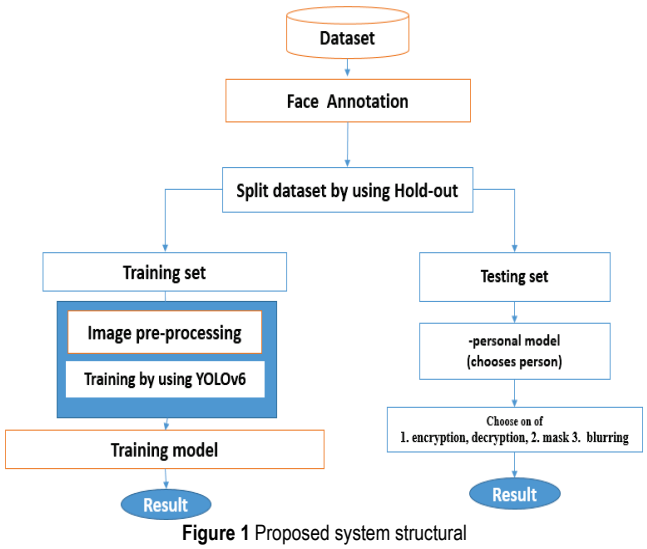

Figure 1 Proposed system structural

5 PROPOSED SYSTEM

Providing protection and privacy for the human face was the goal of the proposed system, where the number of faces in the images is distinguished and determined, and specific people are selected from within the group to provide them with privacy through the faces, and this is done using the (YOLOv6) algorithm. The proposed system chooses one method out of three to provide privacy during the prediction phase. Relying on the most famous types of global data sets is challenging for researchers due to its characteristics, most notably the many faces, close and very far. Fig. 1 illustrates the details of the proposed system.

5.1 Dataset

A WIDER facial is a popular facial detection algorithm benchmark. In "WIDER FACE: A Face Detection Benchmark" by Shuo Yang et al. [28], 32,279 Flickr pictures with over 80,000 faces tagged were used. Events, including sports, concerts, and street scenes, are represented by 61 event classes in the dataset. WIDER FACE helps face detection algorithm developers and researchers. WIDER FACE dataset, which uses images from the publicly available WIDER dataset, has been used to benchmark state-of-the-art face detection algorithms and drive the development of new and improved methods. The WIDER FACE dataset has 61 event classifications. The following Fig. 2 shows an example of the event of the image in the dataset [28].

Figure 2 Example of the event of the image in the WIDER FACE dataset

Face annotations in the WIDER FACE dataset provide each image's face location, size, and occlusions. Face detection algorithm training and evaluation require these annotations. Text files with dataset photos contain these annotations. Each image has a text file with each face's bounding box and occlusion label. The WIDER facial dataset has excellent facial annotations. Because expert annotators painstakingly created the annotations. The annotators thoroughly inspected each image and categorized each face per standards. Face detection algorithms must be trained and evaluated using WIDER FACE's high-quality annotations. Annotations tell algorithms where and how big faces are in photos. The algorithms can be trained to detect faces better with this data. Annotations can also evaluate face detection systems. This is done by comparing algorithm detections against ground truth annotations. Best-performing algorithms have high detection rates and low false favourable rates. Many cutting-edge face detection algorithms have been trained and tested using WIDER FACE dataset face annotations. The dataset has spurred facial detection technology advancements. The data was divided using the holdout method, widely regarded as the most suitable approach for massive datasets. Keras is an integrated, robust, user-friendly, open-source Python toolkit designed to develop and assess deep learning models. It is an integral component of the TensorFlow library, enabling the concise definition and training of neural network models.

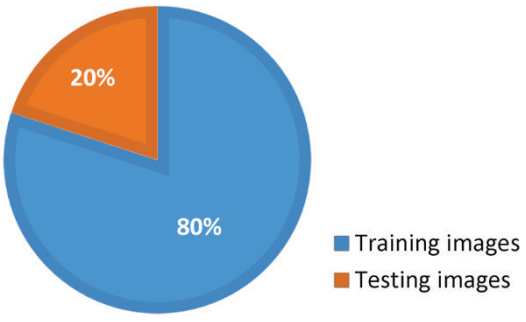

Figure 3 Split dataset in the proposed system

Keras library using in (splitting dataset in the training set and testing set in topic Holdout). Fig. 3 shows the percentage of splitting datasets in the proposed system.

Table 2 Splitting dataset to training and testing in the proposed system

Training images	12888
Testing images	3222

5.2 Training and Privacy Stage

The proposed system uses YOLOv6 because the algorithm is an innovative real-time object detection method that combines the precision of previous models with substantial enhancements in inference speed. It is based on the framework of YOLOv5 but has other novel characteristics that improve its overall performance. The advantage of this algorithm that chooses in the proposed system can summarized in the following point:

- Enhanced Precision: YOLOv6 exhibits superior accuracy on standard datasets compared to its previous versions, showcasing its efficacy in diverse object detection assignments.
- Improved Velocity: YOLOv6 surpasses its previous versions regarding inference speed, allowing for real-time object detection in challenging situations.
- Hardware Efficiency: YOLOv6 is precisely engineered to optimize hardware performance, making it highly compatible with various computer platforms, such as mobile devices and embedded systems.
- Features: YOLOv6 includes various cutting-edge features, including Path Aggregation Network (PANet), Efficient Channel Attention (ECA), Cross Stage Attention (CSA), FPN with Shared Attention (FPN SA), Edge Attention Mechanism (SAM), and IoU Aware Anchor Refinement. These features significantly enhance the performance of YOLOv6.

YOLOv6's amalgamation of precision, swiftness, and hardware optimization renders it a flexible instrument suitable for many applications. Three summarized the layer of YOLOv6 that is used in the proposed system (Tab. 3).

Table 3 Layer of YOLOv6 in prosed system

Layer	Description
Mosaic	Resizes and crops images to a uniform size, improving training efficiency.
MixUp	Randomly blends two images during training, enhancing data augmentation and improving generalization.
AutoShape	Dynamically resizes the input image to a suitable size for the network, adapting to different image resolutions.
CSPDarknet53	The backbone network extracts features from the input image using a combination of residual connections and spatial attention modules.
PANet	Fuses feature from different network layers, providing context information for improved object detection.
SPP	Applies max pooling to features at different scales, enhancing the detection of objects at varying sizes.
YOLO Head	Performs object detection by predicting bounding boxes and class probabilities for each detected object.
NMS	Applies non-maximum suppression to filter out overlapping bounding boxes and retain only the most confident detections.

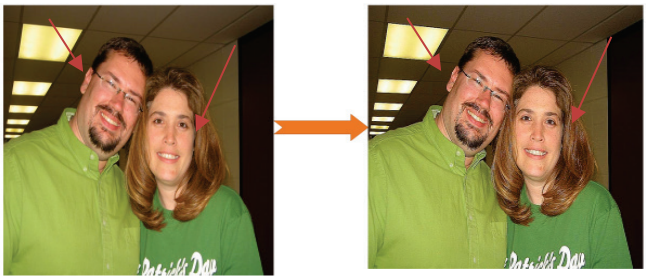

Figure 4 Example image to showing the difference before and after use

In the training stage, the enhancement image operation is used to set training data before input into the training algorithm. In generated images using (Python image library - edge enhance), OpenCV (Open Source Computer Vision Library) is a popular library for real-time computer vision. It provides various functions for detecting edges and enhancing the image, and programmers widely use it because of the actual improvement it provides. Figs. 4 and 5. This is an example image to show the difference before and after use.

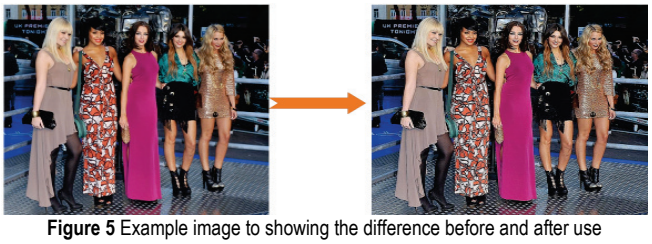

Figure 5 Example image to showing the difference before and after use

After completing the training process comes the testing phase, which is the phase that takes place through face detection, people selection, and privacy determination in the proposed system, where the trained model is called, and privacy operations are performed on the result of people identification and face identification, where in the proposed system three methods are performed. Separately, no choice. Including (encryption and decryption through an algorithm in which the data is encrypted using the Advanced Encryption Standard (AES) and decryption, which is a symmetric critical encryption method and is considered one of the modern encryption algorithms with the highest level of security as it is), (the mask method), and (the camouflage method). The following Figs. 6 and 7 show the final result of face privacy in the proposed system.

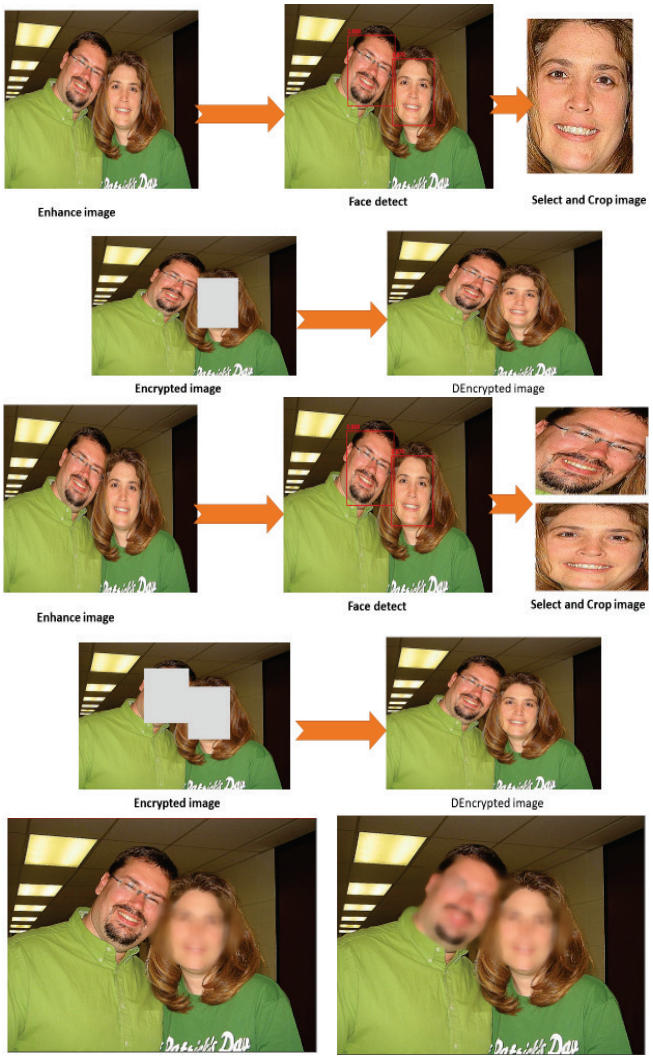

Figure 6 Example of (decryption and encryption) and (blurring) for one or more Pearson in the proposed system

6 EVALUATION THE RESULT

In the proposed system, a confusion matrix comprehensively represents the results obtained from a classification forecast. In the past, numbers were utilized to enumerate and categorize the quantity of precise and imprecise predictions based on class. The proposed evaluation approach will be employed to interpret the confusion matrix. A confusion matrix concisely summarises the frequency with which a classification model correctly or incorrectly anticipated outcomes. *TP* represents the number of actual positive cases, *TN* represents the number of true negative cases, *FP* represents the number of false positive cases, and *FN* represents the number of false negative cases. A confusion matrix is an invaluable tool for assessing the efficacy of a system. The specific fundamental indicators differ based on the four categories.

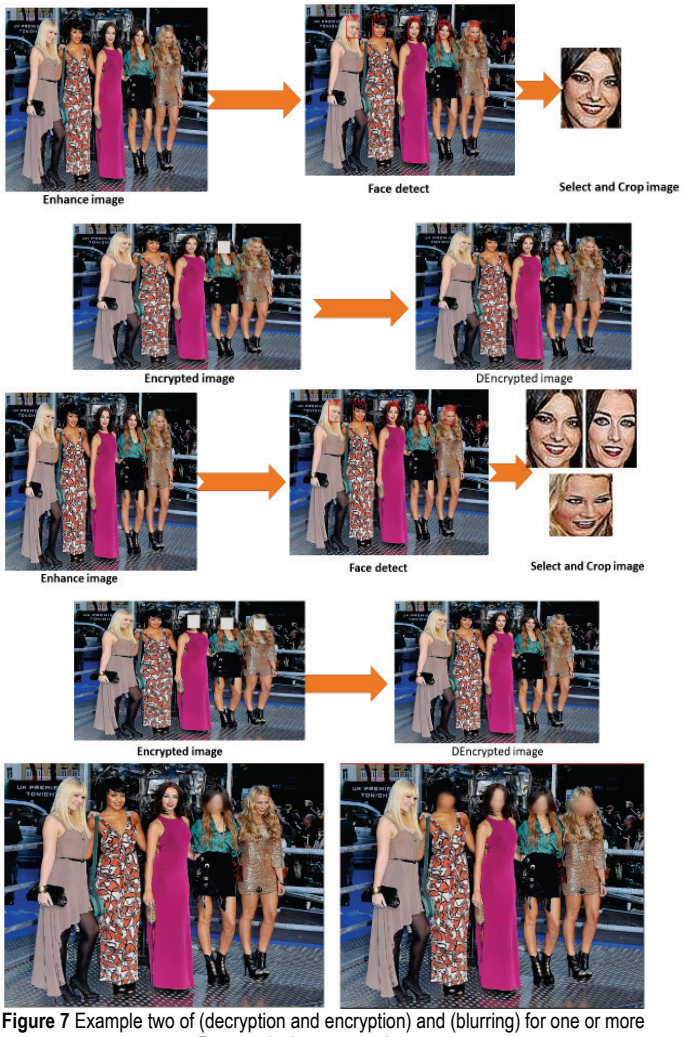

Figure 7 Example two of (decryption and encryption) and (blurring) for one or more Pearson in the proposed system

The following Figs. 8 and 9 are the results of the proposed system from the training and testing stage:

⇒ Training

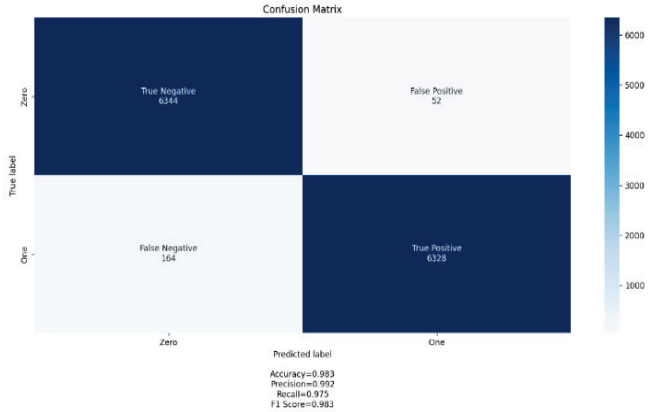

Figure 8 Confusion matrix for the training stage in the proposed system

Table 4 Result of confusion matrix in the proposed system in the training stage

TP = 6328	*FP* = 52	*FN* = 164	*TN* = 6344
Accuracy = (*True positives* + *True Negatives*)/(*True positives* + *True negatives* + *False positives* + *False negatives*)	0.983		
Precision = *True positives*/(*True positives* + *False positives*)	0.992		
Recall = *Recall* = *True positives*/(*True positives* + *False negatives*)	0.975		
Fl-score = 2 × [(*Precision* × *Recall*)/(*Precision* + *Recall*)]	0.983		

⇒ Testing

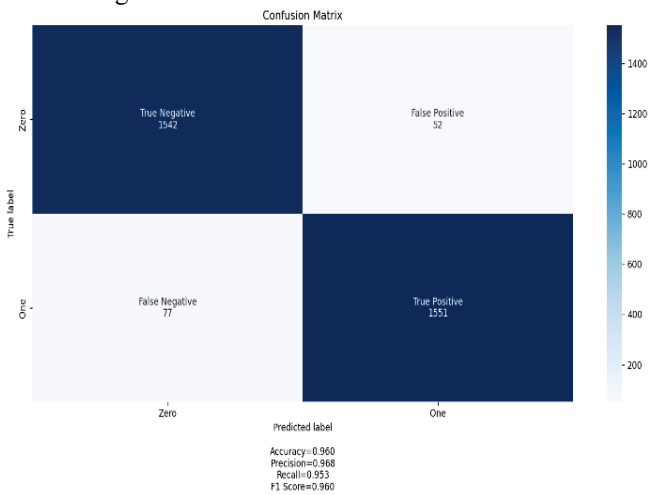

Figure 9 Confusion matrix for the training stage in the proposed system

Table 5 Result of confusion matrix in the proposed system in the training stage

TP = 1551	*FP* = 52	*FN* = 77	*TN* = 1542
Accuracy = (*True positives* + *True Negatives*)/(*True positives* + *True negatives* + *False positives* + *False negatives*)	0.960		
Precision = *True positives*/(*True positives* + *False positives*)	0.968		
Recall = *Recall* = *True positives*/(*True positives* + *False negatives*)	0.953		
Fl-score = 2 × [(*Precision* × *Recall*)/(*Precision* + *Recall*)].	0.960		

Based on the above results obtained as an output of the proposed system, the following Fig. 10 represents results in a curved way to show the difference between the test and training results.

7 CONCLUSION

Protecting the face or privacy is considered one of the challenges for researchers because it is developing rapidly due to the development of technology. In the research paper, work was done on employing artificial intelligence in privacy by building a model that relies on the deep learning method with an algorithm considered the strongest in detection, YOLOv6, and performing a simple processing process. However, it has a practical effect in improving images through a ready-made library and applying it to training images, and it also provides two important features. It selects

specific people from within a group and applies three operations to them separately. The results were promising and good. In future work, we will add another fourth method for diversity to experiment further and compare which method is most efficient in providing facial privacy protection.

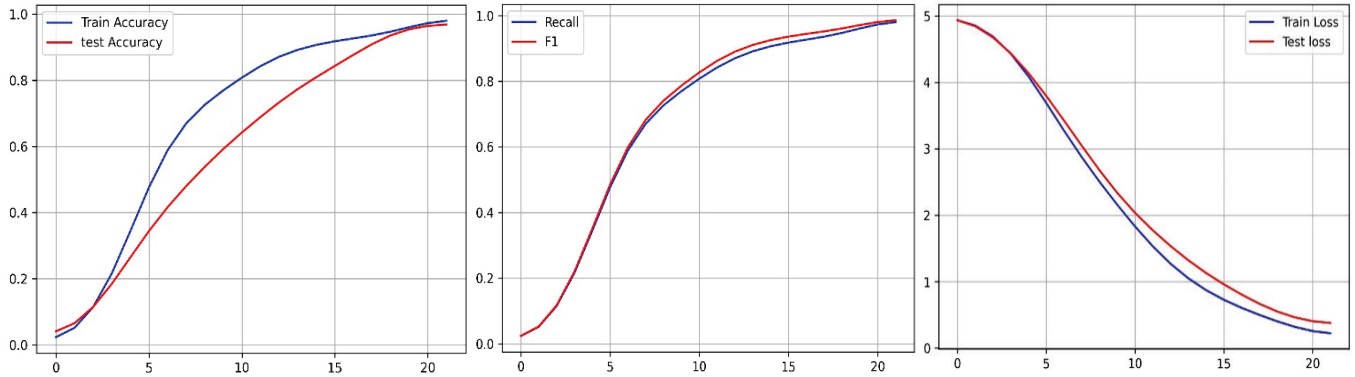

Figure 10 Result of the proposed system (training and testing)

8 REFERENCES

[1] Hosny, K. M., Zaki, M. A., Hamza, H. M., Fouda, M. M., & Lashin, N. A. (2022). Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection. *IEEE Access, 10*, 106750-106769. https://doi.org/10.1109/ACCESS.2022.3211657

[2] Chen, L., Zhao, G., Zhou, J., Ho, A. T. S., & Cheng, L. M. (2019). Face template protection using deep LDPC code learning. *IET Biometrics, 8*(3), 190-197. https://doi.org/10.1049/iet-bmt.2018.5156

[3] Korshunov, P. & Ebrahimi, T. (2013). PEViD: privacy evaluation video dataset. *Proc. SPIE 8856, Appl. Digit. Image Process. XXXVI*, p. 88561S. https://doi.org/10.1117/12.2030974

[4] Hu, S. et al. (2022). Protecting facial privacy: Generating adversarial identity masks via style-robust makeup transfer. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 15014-15023. https://doi.org/10.1109/CVPR52688.2022.01459

[5] Jiang, R., Bouridane, A., Crookes, D., Celebi, M. E., & Wei, H. L. (2016). Privacy-Protected Facial Biometric Verification Using Fuzzy Forest Learning. *IEEE Trans. Fuzzy Syst., 24*(4), 779-790. https://doi.org/10.1109/TFUZZ.2015.2486803

[6] Yang, J., Zhang, W., Liu, J., Wu, J., & Yang, J. (2022). Generating de-identification facial images based on the attention models and adversarial examples. *Alexandria Eng. J., 61*(11), 8417-8429. https://doi.org/10.1016/j.aej.2022.02.007

[7] Damer, N., López, C. A. F., Fang, M., Spiller, N., Pham, M. V., & Boutros, F. (2022). Privacy-friendly synthetic data for the development of face morphing attack detectors. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 1606-1617. https://doi.org/10.1109/CVPRW56347.2022.00167

[8] Qiu, Y., Niu, Z., Tian, Q., & Song, B. (2021). Privacy preserving facial image processing method using variational autoencoder. *International Conference on Big Data and Security*, 3-17. https://doi.org/10.1007/978-981-19-0852-1_1

[9] Andrejevic, M. & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learn. Media Technol., 45*(2), 115-128. https://doi.org/10.1080/17439884.2020.1686014

[10] Barnouti, N. H., Al-Dabbagh, S. S. M., & Matti, W. E. (2016). Face recognition: A literature review. I*nt. J. Appl. Inf. Syst., 11*(4), 21-31. https://doi.org/10.5120/ijais2016451597

[11] Lal, M., Kumar, K., Arain, R. H., Maitlo, A., Ruk, S. A., & Shaikh, H. (2018). Study of face recognition techniques: A survey. *Int. J. Adv. Comput. Sci. Appl., 9*(6), 42-49. https://doi.org/10.14569/IJACSA.2018.090606

[12] Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face recognition: Past, present and future (a review). *Digit. Signal Process. A Rev. J., 106*, p. 102809. https://doi.org/10.1016/j.dsp.2020.102809

[13] Kasar, M. M., Bhattacharyya, D., & Kim, T. H. (2016). Face recognition using neural network: A review. *Int. J. Secur. its Appl., 10*(3), 81-100. https://doi.org/10.14257/ijsia.2016.10.3.08

[14] Li, L., Mu, X., Li, S., & Peng, H. (2020). A Review of Face Recognition Technology. *IEEE Access, 8*, 139110-139120. https://doi.org/10.1109/ACCESS.2020.3011028

[15] Singh, S. & Prasad, S. V. A. V. (2018). Techniques and challenges of face recognition: A critical review. *Procedia Comput. Sci., 143*, 536-543. https://doi.org/10.1016/j.procs.2018.10.427

[16] Kong, S. G., Heo, J., Abidi, B. R., Paik, J., & Abidi, M. A. (2005). Recent advances in visual and infrared face recognition—a review. *Comput. Vis. Image Underst., 97*(1), 103-135. https://doi.org/10.1016/j.cviu.2004.04.001

[17] Oloyede, M. O., Hancke, G. P., & Myburgh, H. C. (2020). A review on face recognition systems: recent approaches and challenges. *Multimed. Tools Appl., 79*, 27891-27922. https://doi.org/10.1007/s11042-020-09261-2

[18] Wang, M. & Deng, W. (2021). Deep face recognition: A survey. *Neurocomputing, 429*, 215-244. https://doi.org/10.1016/j.neucom.2020.10.081

[19] Arya, S., Pratap, N., & Bhatia, K. (2015). Future of face recognition: a review. *Procedia Comput. Sci., 58*, 578-585. https://doi.org/10.1016/j.procs.2015.08.076

[20] Hassaballah, M. & Aly, S. (2015). Face recognition: Challenges, achievements and future directions. *IET Comput. Vis., 9*(4), 614-626. https://doi.org/10.1049/iet-cvi.2014.0084

[21] Payton, T. M., Claypoole, T. F., & Schmidt, H. A. (2014). Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. Corpus ID: 107112727. https://doi.org/10.5860/choice.52-0887

[22] Ke, T. T. & Sudhir, K. (2023). Privacy Rights and data security: GDPR and personal data markets. *Manage. Sci., 69*(8), 4389-4412. https://doi.org/10.1287/mnsc.2022.4614

[23] Pan, Z., Sun, J., Li, X., Zhang, X., & Bai, H. (2023). Collaborative Face Privacy Protection Method Based on Adversarial Examples in Social Networks. In: Huang, D. S., Premaratne, P., Jin, B., Qu, B., Jo, K. H., Hussain, A. (eds) *Advanced Intelligent Computing Technology and Applications.*

ICIC 2023. Lecture Notes in Computer Science, 14086. Springer, Singapore, 499-510. https://doi.org/10.1007/978-981-99-4755-3_43

[24] Tong, C., Zhang, M., Lang, C., & Zheng, Z. (2021). An Image Privacy Protection Algorithm Based on Adversarial Perturbation Generative Networks. *ACM Transactions on Multimedia Computing, Communications, and Applications, 17*(2), Article No. 43, 1-14. https://doi.org/10.1145/3381088

[25] Almansour, A., Alsaeedi, G., Almazroui, H., & Almuflehi, H. (2020). I-Privacy Photo: Face Recognition and Filtering. ICCDA 2020: *Proceedings of the 4th International Conference on Compute and Data Analysis*, 131-141. https://doi.org/10.1145/3388142.3388161

[26] You, Z., Li, S., Qian, Z., & Zhang, X. (2021). Reversible Privacy-Preserving Recognition. *The IEEE International Conference on Multimedia and Expo (ICME2021)*, Shenzhen, China, 1-6. https://doi.org/10.1109/ICME51207.2021.9428115

[27] Jiang, B., Bai, B., Lin, H., Wang, Y., Guo, Y., & Fang, L. (2023). DartBlur : Privacy Preservation with Detection Artifact Suppression. *The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR2023)*, Vancouver, BC, Canada, 16479-16488. https://doi.org/10.1109/CVPR52729.2023.01581

[28] Mamieva, D., Abdusalomov, A. B., Mukhiddinov, M., & Whangbo, T. K. (2023). Improved face detection method via learning small faces on hard images based on a deep learning approach. *Sensors, 23*(1), 502. https://doi.org/10.3390/s23010502

[29] Yang, S., Luo, P., Loy, C. C., & Tang, X. (2016). WIDER FACE: A Face Detection Benchmark. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR2016)*, Las Vegas, NV, USA, 5525-5533. https://doi.org/10.1109/CVPR.2016.596

Authors' contacts:

Mauj Haider AbdAlkreem
Ministry of Education, Administrative Affairs,
306-6, Baghdad, Baghdad Governorate, Iraq
maujhader7@gmail.com

Ruaa Sadoon Salman
(Corresponding author)
Ministry of Education,
Karkh Three Directorate of Education,
306-6, Baghdad, Baghdad Governorate, Iraq
ruaa.s.alkhafaji@gmail.com

Farah Khiled Al-Jibory
Ministry of Education,
Karkh First Directorate of Education,
306-6, Baghdad, Baghdad Governorate, Iraq
csd1b0037@gmail.com