Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1205–1214
DOI : 10.47974/JDMSC-1975

Convolutional-based variational autoencoders for face privacy protection in video surveillance

Mallepogu Sivalakshmi *
Department of Computer Science and Engineering
JNTUA College of Engineering
Ananthapuramu
Andhra Pradesh
India

K. Rajendra Prasad †
Department of Computer Science and Engineering
Institute of Aeronautical Engineering
Hyderabad
Telangana
India

C. Shoba Bindu §
Department of Computer Science and Engineering
JNTUA College of Engineering
Ananthapuramu
Andhra Pradesh
India

Abstract

The ubiquity of high-quality video surveillance owes much to advancements in imaging technology and data transmission. Presently, exposing an individual's face in photographs can infringe upon their right to privacy. Real-world face de-identification is a typical task beyond removing private information, considering the specific intent behind image usage. This paper introduces a novel deep learning model (NDLM) designed to safeguard facial

This research was conducted during the PhD with the support of JNTUA Ananthapuramu. Necessary laboratory infrastructure provided by the JNTUA for the work contributions

* *E-mail:* shivacse06@gmail.com (Corresponding Author)
† *E-mail:* krprgm@gmail.com
§ *E-mail:* shobabindhu.cse@jntua.ac.in

© Taru Publications

privacy in video surveillance, structured around two key phases: face detection and privacy protection. Initially, surveillance video data is collected from online sources. In the initial phase, face detection is achieved through the integration of a Hybrid Convolutional Neural Network (HCNN), which combines a convolutional neural network (CNN) and the improved Fire Hawks algorithm (IFHA) for optimal performance. IFHA assists in ensuring privacy protection. This integration incorporates service quality preservation into the loss function, facilitating the generation of facial images with controlled quality preservation. The approach effectively manages various service quality measures and is adaptable across diverse service contexts. The proposed methodology's effectiveness is evaluated to demonstrate its efficiency when compared to traditional methods.

Subject Classification: *94A60.*

Keywords: *Face identification, Privacy protection, Video surveillance, Convolutional neural network, Fire hawk's algorithm, Quality maintenance-variational autoencoders.*

1. Introduction

Video surveillance is ubiquitous in public places, capturing individuals' identities and behaviors [1]. While extensive monitoring has improved lives, the vast amount of image data stored, shared, and publicly accessible globally raises concerns about potential misuse [2]. The internet's unprecedented availability of image data has made images more accessible to users, enabling modern deep-learning algorithms to create intelligent applications [3], [4]. Once someone's visual information, mainly facial photos, becomes public, unauthorized collection and exploitation of this information for financial or political gain can lead to significant issues [5]. However, such actions can complicate data analysis [6] and given the frequent disclosure of private user information [7]. Traditional methods for safeguarding the privacy of face photographs involve actively altering or removing sensitive portions of the image, which can render the image useless and destroy its valuable information [8, 9]. The prevailing approach in face image privacy protection gently modifies the image's attributes, reducing the accuracy of potential facial recognition systems while maintaining its usability for social media [10]. Privacy protection is vital in social contexts, but preserving critical details like facial expressions [11] can significantly enhance information expression [12]. Several strategies have been proposed to safeguard facial privacy. Others employ differential privacy to shield facial privacy by introducing noise to features [13, 14]. These approaches struggle to balance accuracy and privacy protection in the experimental findings, demonstrating their vulnerability to strong reconstruction attacks. Furthermore, learning-based and frequency

domain-based procedures necessitate retraining the face recognition network, which may not apply to already deployed face recognition systems [15].

2. Background Study

This section summarizes pertinent initiatives related to face privacy protection and face identification. Zhen Zhong Kuang et al. [16] have presented a ground-breaking end-to-end privacy protection solution. Jingjing Yang et al. [17] have described a technique based on federated learning and ensemble models for safeguarding the privacy of facial images. A local facial recognition model was built using local face data training on the client side, and it was then fed into PcadvGAN during numerous training cycles. Uddagiri Sirisha et al. [18] have presented PPIE-ODLASC technique. The primary objectives of the PPIE-ODLASC algorithm were to categorize accident severity into different levels and send the accident photographs safely. The two fundamental mechanisms at work in the PPIE-ODLASC technique that is being given are encryption and severity categorization (high, medium, low, and normal). Ying Hu et al. [19] addressed feature selection challenges with numerous participants while protecting anonymity. To increase the functionality of the suggested algorithm, two unique operators that meet the criterion of privacy protection were developed. Mianjie Li and coworkers have argued in favor of data privacy protection [20].

3. Design of Proposed Architecture

The proposed architecture begins with a face detection system that identifies any faces within an image and provides the coordinates of bounding boxes for each detected face. It is essential to acknowledge that the face detection process can significantly vary as various face detection algorithms employ distinct methodologies. Facial Privacy Protection (FPP) techniques are also paramount in this landscape. They are dedicated to concealing an individual's identity from face detection systems, thus safeguarding their privacy from potential intrusions. This paper focuses on integrating face detection and privacy protection techniques. The architectural framework is illustrated in Figure 1.

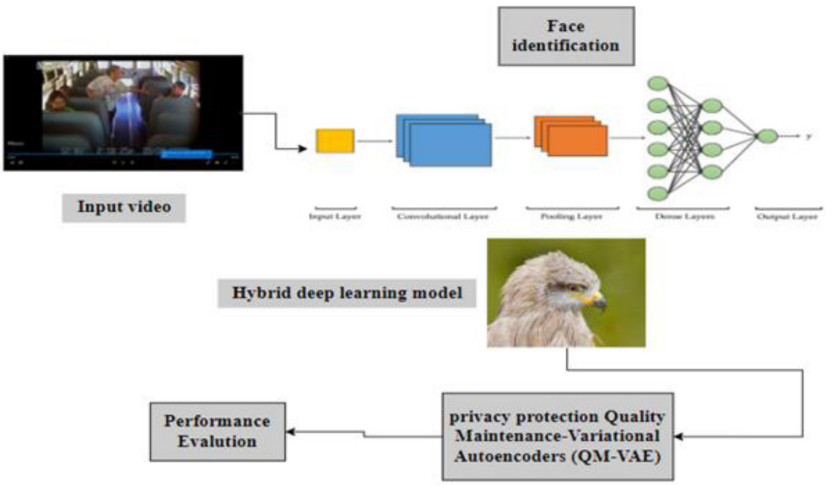

Figure 1

Block Diagram of Proposed Architecture

Levy Flight-based Fire Hawks Optimization

The fire hawk's algorithm is a metaheuristic approach for computing the optimal parameter of the CNN. This technique allows them to catch and control their prey, pick up hot sticks, and put them in various locations to start little fires. The mathematical formulation of FHO is presented in this section.

Step 1: Initialization

The location vectors of the prey and fire hawks are used as CNN parameters to initialize the number of solutions in this phase.

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_i \\ \cdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1^1 & x_1^2 & \ldots & x_1^j & x_1^d \\ x_2^1 & x_2^2 & \ldots & x_2^j & x_2^d \\ \ldots. & \ldots & \ldots & \ldots & \ldots. \\ x_i^1 & x_i^2 & \ldots & x_i^j & x_i^d \\ x_n^1 & x_n^2 & \ldots & x_n^j & x_n^d \end{bmatrix} \tag{1}$$

$$\begin{cases} i = 1, 2, \ldots, n \\ j = 1, 2, \ldots, d \end{cases} \tag{2}$$

Here, $x_{i,\max}^j$ is defined as the maximum bounds of the decision variable, $x_{i,\min}^j$ is defined as the minimum bounds of the decision variable,

$x_i^j(0)$ defines the initial position of the candidate solutions, $n$is the total number of potential solutions in the search area, x_i is referred to as the search space's candidate solution.

Step 2: Fitness Function

The objective function computation defines the selected optimization problem and is used to determine the locations of the fire hawks. The formula for the fitness function is as follows:

$$Y = \frac{1}{2}\sqrt{\frac{\Sigma_{i=0}^{n}(o-d)^2}{N}} \tag{3}$$

Step 3: Distance Computation

This computation computes the complete distance between prey and fire hawks. In the outcome[19], the closest prey to every bird is computed in the efficient distance. The distance function is computed as follows,

$$d_k^1 = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}, \begin{cases} l = 1,2,..,n \\ k = 1,2,..,m \end{cases} \tag{4}$$

Here, (x_1, y_1), and (x_2, y_2) is referred to as the prey and fire hawks' coordinates, $n$is the overall count of fire hawks in the search area.

Step 4: Attacking Behaviour

Consequently, two qualities are considered when upgrading a position in the FHO's main search criteria. This formulation is presented as follows,

$$fh_1^{new} = fh_1 + (R_1 \times gb - R_2 \times fh_{near}), l = 1.2,..,n \tag{5}$$

Here, R_1 and R_2 are defined as random numbers and it is uniformly distributed, fh_{near} is defined as the other fire hawks in the search location

Step 5: Movement of Prey

Each fire hawk's territory's prey movement and animal traits for the upgrading process are determined during this phase. This action is defined as the position upgrading process, and it is formulated as follows,

$$pr_q^{new} = pr_q + (r_3 \times fh_1 - r_4 \times sp_1), \begin{cases} l = 1,2,\ldots,n \\ q = 1,2,\ldots,r \end{cases} \tag{6}$$

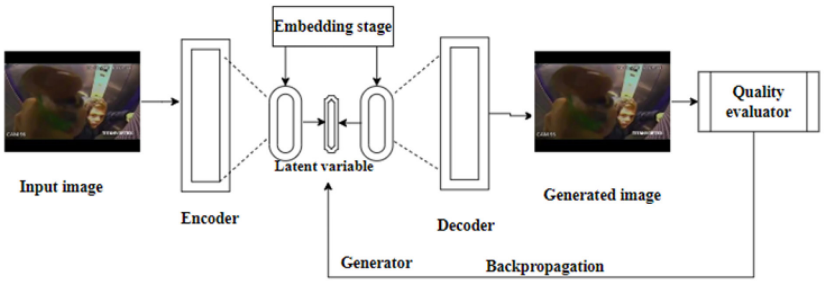

Figure 2

QM-VAE (Quality Maintenance- Variational Autoencoders)

This action is obtained in the position upgrading process by using below formulation,

$$pr_q^{new} = pr_q + (r_5 \times fh_{alter} - r_6 \times sp), \begin{cases} l = 1,2,\ldots,n \\ q = 1,2,\ldots,r \end{cases} \tag{7}$$

Here, R_3 and R_4 is defined as the random numbers and it is uniformly distributed, sp_1 is characterized as the secure location within the fire hawk's range,

$$sp_1 = \frac{\Sigma_{q=1}^{r} pr_1}{r}, \begin{cases} l = 1,2,\ldots,n \\ q = 1,2,\ldots,r \end{cases} \tag{8}$$

$$sp = \frac{\Sigma_{k=1}^{m} pr_k}{m}, k = 1,2,..,m \tag{9}$$

Step 7: Termination

It is the last phase; the termination condition is checked with the iteration count. This algorithm is designed for selecting optimal hyperparameters of the CNN. The face images in the input video are recognized using this algorithm. The chosen face images are used for privacy protection by considering QM-VAE, shown in Figure 2. As a result, the level of service is impacted. These issues are solved by using QM-VAE structure, and a solitary generative model is developed, which reduces the loss function consisting of service quality loss to manage the model learning. Initially, four protection techniques (mosaic, laplace, cartoon and blindfold) were considered for face images. From that, this proposed generative model is considered for service quality evaluation. The output picture quality is determined using the input data in the service condition during this training step, and the result is a loss function.

4. Performance Analysis

The performance measure are mentioned from Eqn. (10) to Eqn. (11)

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{\sqrt{MSE}} \tag{10}$$

$$SSIM = \frac{(2\times\bar{x}\times\bar{y}+c1)(2\times\sigma_{xy}+c2)}{(\sigma_x^2+\sigma_y^2+c2)\times((\bar{x})^2+(\bar{y})^2+c2)} \tag{11}$$

$$NC\ (input\ imge, reconstruct\ image) = \frac{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{ini,j} w_{rci,j}}{\sqrt{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{ini,j}{}^2}\sqrt{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{rci,j}{}^2}} \tag{14}$$

Abuse Arson Explosion

Robbery Shoplifting

Figure 3

Input Sample Videos

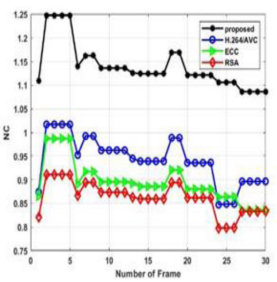

Figure 4

NC Validation

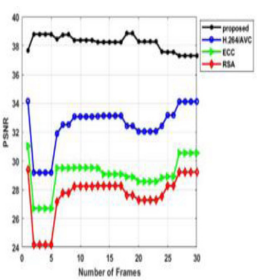

Figure 5

PSNR Validation

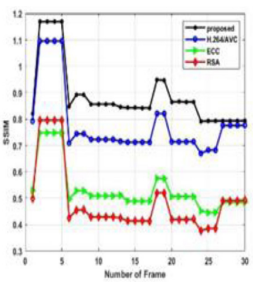

Figure 6

SSIM Validation

To validate the proposed approach, the benchmarked datasets of [21] are used in the experimental work. This dataset comprises real-time surveillance videos capturing various scenarios, including assault, vandalism, explosion, burglary, theft, arrest, abuse, robbery, fighting, shooting, accidents, arson, and shoplifting. The Normalized Correlation (NC) measure is computed and presented in Figure 4 to validate the proposed approach for Figure 3 image data. The optimal NC measure, which indicates the highest level of security enhancement, is achieved by our proposed approach. At the 10th frame, the proposed approach achieves a 0.98 NC measure, while conventional approaches reach 0.96, 0.92, and 0.84 NC. The PSNR measure is computed and presented in Figure 5 to validate proposed approach. The highest PSNR measure, indicative of superior security enhancement, is achieved by our approach. At the 15th frame, the proposed method obtains a PSNR of 34, whereas conventional approaches score 32.5, 29.5, and 27.15. The Structural Similarity Index Measure (SSIM) is calculated and presented in Figure 6 to validate proposed approach. In the 15th frame, proposed approach obtains an SSIM of 0.76, while conventional approaches score 0.71, 0.5, and 0.4.

5. Conclusion and Future Research

The proposed method operates in two fundamental phases: face detection and privacy protection. Initially, gathered surveillance video data from online sources. In the first phase, achieved face detection through the utilization of a Hybrid Convolutional Neural Network (HCNN), a combination of Convolutional Neural Network (CNN) and Improved Fire Hawks Algorithm (IFHA). Notably, the hyperparameters for the CNN were chosen with the assistance of IFHA. Subsequently, privacy protection was implemented using Quality Maintenance-Variational Autoencoders (QM-VAE), a technique that considers the trade-off between preserving service quality and safeguarding privacy. Performance metrics were employed to evaluate the proposed methodology comprehensively. The validation process conclusively showed that the proposed approach outperformed conventional methods across multiple dimensions, including PSNR, NC, SSIM, encryption time, and decryption time. Hence, this research has culminated in developing a robust and effective approach for face privacy protection in video surveillance, positioning it as a promising solution in security and privacy preservation in future research by extending the work for cloud based video system privacy.

References

[1] Li, Mianjie, Zhihong Tian, Xiaojiang Du, Xiaochen Yuan, Chun Shan, and Mohsen Guizani. "Power normalized cepstral robust features of deep neural networks in a cloud computing data privacy protection scheme." *Neurocomputing* 518 : 165-173 (2023).

[2] Khosravy, Mahdi, Kazuaki Nakamura, Yuki Hirose, Naoko Nitta, and Noboru Babaguchi. "Model inversion attack by integration of deep generative models: Privacy-sensitive face generation from a face recognition system." *IEEE Transactions on Information Forensics and Security* 17 : 357-372 (2022).

[3] Sun, Zhaodong, and Xiaobai Li. "Privacy-phys: Facial video-based physiological modification for privacy protection." *IEEE Signal Processing Letters* 29 : 1507-1511 (2022).

[4] Chen, Mingliang, Xin Liao, and Min Wu. "Pulse Edit: Editing physiological signals in facial videos for privacy protection." *IEEE Transactions on Information Forensics and Security* 17 : 457-471 (2022).

[5] Zhong, Yaoyao, and Weihong Deng. "Opom: Customized invisible cloak towards face privacy protection." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45, no. 3 : 3590-3603 (2022).

[6] Qiu, Yuying, Zhiyi Niu, Biao Song, Tinghuai Ma, Abdullah Al-Dhelaan, and Mohammed Al-Dhelaan. "A novel generative model for face privacy protection in video surveillance with utility maintenance." *Applied Sciences* 12, no. 14 : 6962 (2022).

[7] Zhang, Xing, Seung-Hyun Seo, and Changda Wang. "A lightweight encryption method for privacy protection in surveillance videos." *IEEE Access* 6 : 18074-18087 (2018).

[8] Lee, Donghyeok, and Namje Park. "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree." *Multimedia Tools and Applications* 80 : 34517-34534 (2021).

[9] Kumar, Ankit, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia, and Linesh Raja. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4 (2019).

[10] Andrew, Jane, and Max Baker. "The general data protection regulation in the age of surveillance capitalism." *Jnl of Business Ethics* 168 : 565-578 (2021).

[11] Hosni Mahmoud, Hanan A., and Hanan Abdullah Mengash. "A novel technique for automated concealed face detection in surveillance videos." *Personal and Ubiquitous Computing* 25 : 129-140 (2021).

[12] Cárdenas, Rolando J., Cesar A. Beltrán, and Juan C. Gutiérrez. "Small face detection using deep learning on surveillance videos." *Envi.* 2, no. 5 : 14 (2019).

[13] Manju, D., and V. Radha. "A novel approach for pose invariant face recognition in surveillance videos." *Procedia Computer Science* 167 : 890-899 (2020).

[14] Dong, Zuolin, Jiahong Wei, Xiaoyu Chen, and Pengfei Zheng. "Face detection in security monitoring based on artificial intelligence video retrieval technology." *IEEE Access* 8 : 63421-63433 (2020).

[15] Ullah, Rehmat, Hassan Hayat, Afsah Abid Siddiqui, Uzma Abid Siddiqui, Jebran Khan, Farman Ullah, Shoaib Hassan et al. "A real-time framework for human face detection and recognition in cctv images." *Mathematical Problems in Engineering* 2022 (2022).

[16] Kuang, Zhenzhong, Zhiqiang Guo, Jinglong Fang, Jun Yu, Noboru Babaguchi, and Jianping Fan. "Unnoticeable synthetic face replacement for image privacy protection." *Neurocomputing* 457 : 322-333 (2021).

[17] Yang, Jingjing, Jiaxing Liu, Runkai Han, and Jinzhao Wu. "Transferable face image privacy protection based on federated learning and ensemble models." *Complex & Intelligent Systems* 7, no. 5 (2021): 2299-2315.

[18] Davis, Simon. A recursion relation for the number of Goldbach partitions of an even integer, *Journal of Discrete Mathematical Sciences and Cryptography*, 27:1, 1–30 (2024), DOI: 10.47974/JDMSC-1188.

[19] Selikh, Bilel, Chillali, Abdelhakim, Mihoubi, Douadi & Ghadbane, Nacer. A new public key cryptosystem based on the non-commutative ring R, *Journal of Discrete Mathematical Sciences and Cryptography*, 27:1, 75–93 (2024), DOI: 10.47974/JDMSC-1573.

[20] Tuieb, Munthir Bahir, Serteep, Hind Jumaa & Ali, Doaa Muhsin Abed. Image steganography using Fresnelet transformations, stated coefficients and a pre-processed message, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:6, 1683–1689 (2023), DOI: 10.47974/JDMSC-1614.