Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 45 (2024), No. 5, pp. 1389–1399
DOI : 10.47974/JIOS-1711

Improved privacy protection technique for enhancing security of real-time video surveillance

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

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

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

Abstract

This research presents an effective way for protecting privacy in video surveillance data security. This technique integrates numerous critical challenges in order to generate a public stream and a private remnant erroneous the proposed approach distorted the protected, vulnerable portion. The proposed technique is built around the following three primary concerns: recognizing information that is cognizant of privacy, safeguarding anonymity, and maintaining confidential data through video encoding. In the first stage, the Privacy Region Mask Separation approach is used to identify the portion that is susceptible to protection. The sensitive part is located using this method. Then, the Adaptive Silhouette-Blur Guided Privacy Protection Scheme (ASBGPPS) is considered for privacy protection. An improved

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

version of the Coati optimization algorithm called SBGPPS and ICOA are both incorporated into it.. Lastly, the Storage-H.264/AVC approach is considered in order to accomplish the video encoding and secret sharing storage. Finally, we have completed the video restoration. In order to evaluate how well the proposed methodology works in comparison to more traditional methods, performance measurements are utilized.

Subject Classification: *68xx.*

Keywords: *Privacy protection scheme, Improved coati optimization algorithm (ICOA), H.264/AVC encoding, Privacy-sensitive portion, Privacy region mask separation.*

1. Introduction

Large-scale video surveillance systems are being employed in key locations like airports, city centres, residential areas, and public transportation. Despite its nature, the prevalent sense of insecurity at the turn of the century, with terrorist threats and rising criminality [1], makes the extensive use of video monitoring bearable. People, however, have a reasonable fear of this invasion of their privacy, which is limiting the acceptance of video surveillance devices [2]. Today, video surveillance systems are the most prevalent and widely used image systems in major cooperatives [3].

Machines and human agents routinely monitor sensitive information such as individual identities, activities, routes [4], and associations. While such information on suspicious visits is useful for security, misusing private information about trustworthy employees can hurt morale [5] and even lead to unneeded lawsuits. Therefore, it is necessary to develop privacy protection strategies that could shield particular people from prying eyes without compromising the level of security. Data encryption or scrambling methods are useless because it is no longer possible to see the protected video [6]. Simple image blurring may be acceptable to shield people's identities in television broadcasts, but it permanently changes surveillance videos, making them unsuitable for use as evidence in court [7,8].

Fortunately, current study findings indicate that new technologies with the ability to successfully protect privacy without impeding video surveillance duties are emerging [9,10]. These findings call into question the widely held belief that improved security entails a loss of privacy. However, despite widespread interest in the problem of privacy protection, detailed performance analysis is scarce [11]. It is critical, in particular, to validate suggested privacy protection methods against user and system

privacy needs. Furthermore, it is unknown if current privacy protection technologies can be integrated into existing monitoring architecture and deployed in large-scale systems [12, 13]. This study's objective is to determine a methodology for evaluating the ability of privacy protection technologies to conceal distinguishing facial information [14, 15].

2. Study of the Work

It is essential to study the video encoding-security enhancement in surveillance video applications. A few works are analysed and reviewed in this section. A multi-layer visual privacy-protected (VPP) coding approach was created by Hu Ying et al. [16] to visually obfuscate sensitive information in a video while minimizing the impact on the film's essential visual elements. As an outcome, the key frame determines the extraction's accuracy process in the future is guaranteed.

A federated feature selection method was initially introduced by prabhu et al. in [17]. Inspired by the idea of federated learning, the strategy involved establishing a trustworthy third participant the best feature subsets from several participants' submissions for processing and integration.

A Fractional-Ant Lion Optimisation Algorithm for Privacy Protection was introduced by Zhang et al. in [18]. The Fractional Calculus (FC) and Ant Lion Optimizer (ALO) algorithms were combined to develop the F-ALO algorithm, which offers superior data security. By using the mappers and reducers of the Map Reduce architecture and including the stages of privacy and information sharing, the shared data is protected. The suggested method uses standards like nakedness and sensitivity index to determine the appropriate coefficient. The proposed F-ALO algorithm outperformed other algorithms using the Hungarian database. This algorithm is proved with many parameters and useful in secured video surveillance applications.

Lightweight Encryption Method to the purpose of secured video surveillance was developed by Dave et al., [19]. Next, a layered cellular automata (LCA)-based light-weight encryption technique was created. By using this method, the restored ROIs were fed onto the starting state of a 8-layer by layer cellular automata, which was governed by randomly created rules for the state transformations of the LCA. As a result, each RoI underwent independent and concurrent encryption. Authenticated users can request access to the encrypted RoIs that were stored on the camera

side. The surveillance footage can be viewed in real-time by any web user without RoIs.

X. Ma et al. have presented an autonomous edge-fog node-based surveillance system suitable for intelligent house scenarios [20-24], with the goal of protecting people's privacy. As motion detection is used for finding intrusions that filter out suspected information in video surveillance. In this, its system becomes act as the best resource efficient system. To reduce service response times, benefits the work efficient distributed node system inorder to secure the protection, Abomhara et al., [24] have introduced a trust-aware task offloading mechanism (TOM) for video surveillance in edge computing enabled IoV. Technically, balanced job offloading solutions are found using SPEA2 (increasing the strength Pareto evolutionary algorithm).

No security of information strategy that has been proposed to ensure privacy while achieving its tracking purpose satisfies all of the aforementioned criteria. Reduction of images or videos is necessary for scrambled [22], while suppression methods, like those described in [15], are frequently difficult to implement and necessitate the storage of the original material in a different location. Methods that depend on encoding, such as those that are put forward in [21], are private; nonetheless, they jeopardize the authenticity of the data that comprises the original pixels. For example, relevant examples of simple procedures that cannot be reversed and are not secure.

3. Proposed Architecture

More surveillance cameras have been considered in recent years in various parts of our surroundings, including roads, airports, business buildings, and ATMs. With the widespread use of surveillance cameras, there is a particular concern about human privacy as these cameras are gathering a large number of films in a short amount of time. One of the primary topics for multimedia is the problem of visual tracking of human traits and protecting privacy. As a result, this essay develops an effective privacy protection system. Figure 1 shows the proposed schema.

Initially, surveillance videos are collected for the identification of privacy protection schemes. After that, the privacy region is identified with the consideration of privacy region mask separation. The privacy region is identified and sent to the protection scheme of ASBGPPS.

Based on that, the video was also reconstructed. The performances are evaluated by using measures.

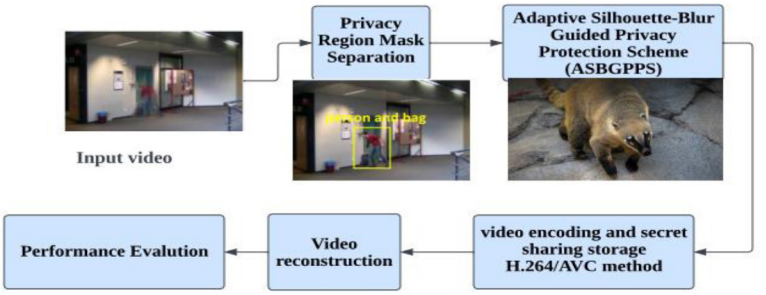


Figure 1

Proposed Schema

3.1 *Adaptive Silhouette-Blur Guided Privacy Protection Scheme*

The masking technique is used to separate the privacy-sensitive region. This separation portion is protected by considering ASBGPPS. This procedure is a combination of SBGPPS and ICOA. In the SBGPPS, the kernel parameter will be optimized by considering ICOA. Based on this process, the privacy region is identified and protected. In the process, the kernel size is optimally selected by considering ICOA. It is related to the residual errors. The residual error should be reduced by optimally choosing the kernel size.

3.1.2. Improved Privacy Protection Technique

The ICOA is taken into account while choosing the ideal kernel size in this proposed method. This algorithm is developed based on their coati behaviors. The coatis use this method to target iguanas and take advantage of their traits. Additionally, the predators' evasion tactics are taken into account [23, 24]. The population members of this metaheuristic algorithm, which is known as the COA approach, are its definition. Every coati's location within the search area is used to determine the parameter for the decision variables. A candidate's response to the problem is therefore determined by their location on the coati.

Levy operation of flights is taken into consideration to improve this updating process. Using this approach, the residual faults in the audio and video stream process are taken into account when selecting the ideal kernel value.

3.2. *Video Encoding and Secret Sharing Storage H.264/AVC Method*

Encode the protected video once it has been fully protected for added storage; the operation is specified as . Use H.264/AVC codes [25] for the protected foreground and residual error in this case. Only think about encoding and preserving the sampled backdrop frames in the background. The privacy location masks, however, are encoded. It can be anticipated to be more storage effective than H.264/AVC for video V without separation because it helps with relatively stationary backdrops.

The proposed encryption key-related sharing is extremely effective by avoiding large-count video transmission, as opposed to the capacity to recover video data associated managing to a certain count of video streams. Both public users and people with permission can recreate videos in different ways. The clear phase is only made available to authorized users, and the privacy-protected movies are created using regular observers. The precise synchronization issues are not considered because private streams are only controlled for specific instances. The backdrop frames, residual error films, and privacy object-protected videos are first decoded.

4. Results Discussion

The experiments are conduced and evaluated with various indicated performance measures. The proposed approach is developed to empower security in the video of surveillance cameras. In the surveillance video, the sensitive portion is identified and blurred. After that, it is reconstructed in a specific manner. It is mentioned as per the procedure of proposed technique. It has been carried out in MATLAB, and its performances are assessed using the following metrics: decryption time, encryption time, structural similarity index measure (SSIM), peak signal-to-noise ratio (PSNR), and normalisation correlation (NC). Rivest Shamir Adleman (RSA) and elliptical curve cryptography (ECC) are the two conventional methods that the proposed methodology contrasts with.

4.1. *Dataset Description*

The surveillance camera video is taken into consideration in order to validate the proposed method. It is a real-time surveillance film that features a variety of criminal activity, including shoplifting, theft, shooting, robbery, fights, explosions, break-ins, accidents, assaults, arson, arrests, and abuse. These videos have been taken into account, the privacy domain

is located, and the proposed approach is applied in order to protect them. The sample video clips are presented in Fig 2. The input image, blur image, and privacy region are illustrated in fig 3 and fig 4. To validate the proposed approach, it is tested by decryption time and displayed in Fig. 6(a).

It is also contrasted with traditional strategies like RSA and ECC. The proposed approach has attained 4s of decryption time. The conventional techniques of RSA and ECC have attained 6s and 26s of decryption time, respectively. Related to this verification, the proposed approach achieved a low decryption time. Encryption time is used to validate the proposed methodology, which is displayed in Figure 6(b). It is also contrasted with traditional strategies like RSA and ECC. The proposed approach has attained 3s of encryption time.

The conventional techniques of RSA and ECC have attained 7s and 26s of decryption time, respectively. Related to this verification, the proposed approach achieved a low encryption time. To validate the proposed approach, the NC measure is computed and presented in Figure 7. The optimal NC measure is the highest parameter during security enhancement. During the 5th frame, the proposed approach obtained 1 in the NC measure. Similarly, the conventional approaches are obtained at

Figure 2

Demonstrated Videos

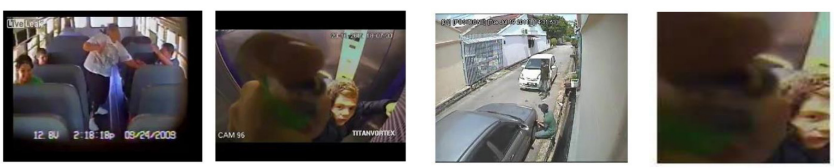


Figure 3

Image with blur

Figure 4

Secure Image

0.98 and 0.85 NC. During the 10th frame, the proposed approach obtained a 0.96 in the NC measure. Similarly, the conventional approaches obtained 0.92 and 0.84 in NC. During the 15th frame, the proposed approach obtained a 0.94 in the NC measure. Similarly, the conventional approaches are obtained at 0.89 and 0.82 in NC. According to the validation, the predicted strategy produced the best results in terms of NC. The PSNR measure is computed it is validating the suggested approach, and it shown in Figure 5.

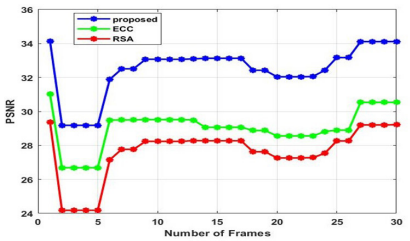
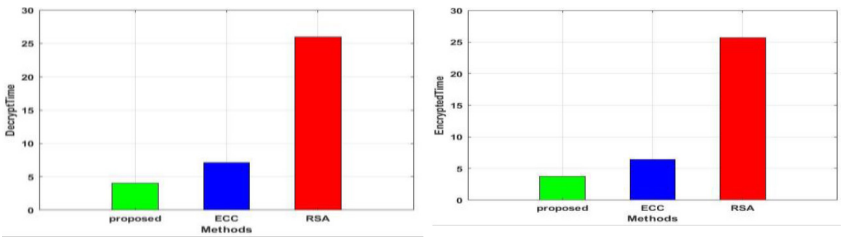


Figure 5

PSNR



a) Decryption Time **b) Encryption Time**

Figure 6

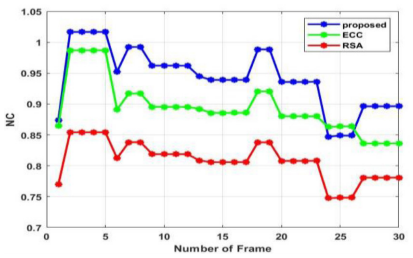


Figure 7

NC

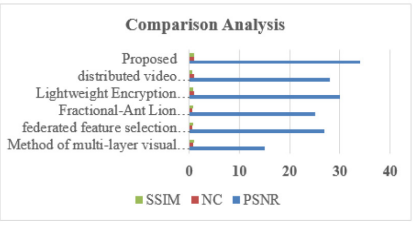


Figure 8

Comparison Analysis

The optimal PSNR measure is the highest parameter during security enhancement. During the 15th frame, the proposed approach obtained a 32.5 PSNR measure. Similarly, the conventional approaches obtained 29.5 and 27.15 in PSNR. According to the validation, the planned strategy produced the best results in terms of PSNR. To validate the projected approach, the SSIM measure is computed. The optimal PSNR measure is the highest parameter during security enhancement. During the 5th frame, the proposed approach obtains 1.0 in the SSIM measure. Similarly, the conventional approaches obtained 0.8 and 0.75 in SSIM. During the 15th frame, the proposed approach obtained a 0.71 in the SSIM measure. Similarly, the conventional approaches obtained 0.5 and 0.4 in SSIM. According to the validation, the predicted strategy produced the best results in terms of SSIM. The comparison analysis is presented in figure 8.

5. Conclusion

An effective privacy protection method for video surveillance data security has been proposed in this paper. This approach integrates several important features—de-identification, characteristic preservation, recoverability, and compressibility—into a single framework. The proposed method has created a public stream and a private residual error by obscuring the secure, sensitive Identifying security-sensitive material, safeguarding anonymity, and combining secret shared storage with video compression were the three main considerations in the development of the proposed method. The proposed approach achieved optimal outcomes for PSNR, NC, and SSIM from the validation. The limitations of the proposed work are does not considered the real time data for validation. In the future, real-time applications will be considered for privacy-preserving schemes.

References

[1] Du, Ling, Wei Zhang, et.al., "An efficient privacy protection scheme for data security in video surveillance." *Journal of Visual Communication and Image Representation* 59 : 347-362 (2019).

[2] Fitwi, Alem, Yu Chen, et.al., "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking." *Electronics* 10, no. 3 : 236 (2021).

[3] 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).

[4] C Krishna Mohan, et.al, "The Impact of Adversarial Attacks on Federated Learning: A Survey", *IEEE Transactions on Pattern Analysis and MachineIntelligence* (2023).

[5] Shifa, Amna, et.al., "Skin detection and lightweight encryption for privacy protection in real-time surveillance applications." *Image and Vision Computing* 94 (2020).

[6] Xu, Xiaolong, et.al. "Trust-aware service offloading for video surveillance in edge computing enabled internet of vehicles." *IEEE Transactions on Intelligent Transportation Systems* 22, no. 3 : 1787-1796 (2020).

[7] Suleman Basha, et.al., Hybrid visual computing models to discover the clusters assessment of high dimensional big data. *Soft Computing*, Springer, 27, (2023).

[8] Aho, Brett, and Roberta Duffield. "Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China." *Economy and Society* 49, no. 2 : 187-212 (2020).

[9] Liu, Changming, et.al., "Privacy-preserving motion detection for HEVC-compressed surveillance video." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 18, no. 1 : 1-27 (2022).

[10] Ardabili, et.al., "Understanding Ethics, Privacy, and Regulations in Smart Video Surveillance for Public Safety." arXiv preprint arXiv:2212.12936 (2022).

[11] Fitwi, Alem, Yu Chen, Sencun Zhu, Erik Blasch, and Genshe Chen. "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking." Electronics 10, no. 3 : 236 (2021).

[12] Xu, Xiaolong, et.al., "Trust-aware service offloading for video surveillance in edge computing enabled internet of vehicles." *IEEE Transactions on Intelligent Transportation Systems* 22, no. 3 : 1787-1796 (2020).

[13] Asghar, Mamoona et.al., "Visual surveillance within the EU general data protection regulation: A technology perspective." IEEE Access 7 : 111709-111726 (2019).

[14] Velliangiri, S. "An enhanced multimedia video surveillance security using wavelet encryption framework." *Journal of Mobile Multimedia* : 239-254 (2019).

[15] Kim, Jinsu, Namje Park, Geonwoo Kim, and Seunghun Jin. "CCTV video processing metadata security scheme using character order preserving-transformation in the emerging multimedia." Electronics 8, no. 4 : 412 (2019).

[16] Hu, Ying, et.al., "A federated feature selection algorithm based on particle swarm optimization under privacy protection." *Knowledge-Based Systems* 260 (2023).

[17] Nagendra Prabhu, et.al., "Fractional-Ant Lion Optimization Algorithm for Privacy Protection in Cloud with MapReduce Framework." Cybernetics and Systems (2023).

[18] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[19] Dave, Mayank, et.al.,"Smart fog-based video surveillance with privacy preservation based on blockchain." *Wireless Personal Communications* : 1-18 (2022).

[20] Kumar, Ankit, et al. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 499-507 (2019).

[21] X. Zhang, S.H. Seo, C. Wang, A lightweight encryption method for privacy protection in surveillance videos, *IEEE Access* 6, 18074–18087 (2018).

[22] Dehghani, Mohammad. "Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems." Knowledge-Based Systems 259 (2023).

[23] Kaidi, Wei, Mohammad Khishe, and Mokhtar Mohammadi. "Dynamic levy flight chimp optimization." Knowledge-Based Systems 235 (2022).

[24] Abomhara, et.al., "Enhancing selective encryption for H. 264/AVC using advanced encryption standard." arXiv preprint arXiv:2201.03391 (2022).

[25] https://www.kaggle.com/datasets/mateohervas/dcsass-dataset

Received April, 2024