Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1195–1204
DOI : 10.47974/JDMSC-1974

Human skin encryption based efficient feedback mode for privacy protection method in surveillance video

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

This paper develops an optimal privacy protection technique aimed at image security in video surveillance. Its technique is combined with various key problems such as de-identification, characteristics compressibility, recoverability, and preservation in one united architecture. Proposed technique developed a public stream and a secluded enduring error by distorting the secure sensitive portion. This study work takes into account both research

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**

areas and suggests a hybrid system for detecting and protecting human skin by using colour information under constantly changing lighting and environmental circumstances. With this motivation, proposed method is developed by considering two phases such as human skin detection and encryption which empowers the privacy of the surveillance video. The input image moved to the pre-processing stage of the Gaussian filter to remove noises present in the image. This process is obtained by using Enhanced Cipher Feedback Module Encryption (ECFME). In this process, the optimal key parameters are selected by the Modified Golf Optimization Algorithm (MGOA). Finally, the skin region is encrypted. The proposed methodology is assessed and evaluated by using performance measures to demonstrate the efficiency of the work compared to the conventional techniques.

Subject Classification: *94AC0.*

Keywords: *Skin detection, Discriminative skin detection approach, Enhanced cipher feedback module encryption, Modified golf optimization algorithm.*

1. Introduction

Because human skin is not uniform, identifying individuals in movies is an ever-evolving challenge that is frequently associated with significant computing complexity [1]. The look of human skin can differ depending on the colour of the skin in different parts of the body as well as external and internal environmental factors like contrast in lighting. The major aim of the research presented in this paper remains to distinguish pixels with human skin tones from those without. In numerous significant image-processing applications [2], including human-computer interaction, Content-Based Image Retrieval (CBIR) systems, face tracking, face detection, and human skin detection is essential [3]. Consequently, the capacity to identify human skin is an essential prerequisite in various fields, such as robotics, medical systems, and military systems [4]. Skin tone pixel identification is supplied as an extra piece of data to develop effective face identification, in addition to the shape-based detection of significant features [5].

Most video privacy security techniques rely on encryption, which can safeguard personal data [6]. This can lead to time-consuming computing effort during the picture processing stage that follows [7]. To overcome these shortcomings, multi-layer CS (MCS) ciphering is performed on surveillance video that is susceptible to privacy leaks using compressed sensing (CS) technology in this work, resulting in visual privacy protection (VPP) [8]. Furthermore, consideration needs to be given to the data loss caused through the compression coding of video pictures aimed at the entire system procedure [9] (together with partial transmission of visual

information, processing or imaging, processing etc.). Any of these could result in privacy breaches in later intelligent video applications [10].

Wickramasuriya was the first to suggest privacy protection for surveillance videos. Three major categories can be used to categorize current video privacy protection strategies [11]: (1) identifying and determining the privacy area and replacing it directly; (2) using encryption and image scrambling approach to obtain scramble dispensation [12], like blurring sensitive data; and (3) beating or erasing private data by consuming a watermark that is embedded in the background after the video has been repaired [13]. There is still no one assessment standard, and the variety of video privacy protection strategies consumes given rise towards several different assessment techniques [14], each with its drawbacks. The evaluation method's major body is separated into two approaches: (i) examine the technique from a coding security standpoint. The evaluation method's major body is separated into two categories: (ii) analyses the technique from the standpoint of coding security in addition assesses how well it protects privacy by assessing the algorithm's security [15].

The paper is organized as follows. In section 2, we present the survey work. Section 3 discusses the proposed architecture. Section 4 provides results and discussion. Finally, in section 5 we draw conclusions and future work.

2. Survey Work

A few common strategies for protecting privacy in surveillance videos are examined and discussed in this section. A multi-layer visual privacy-protected (VPP) coding technique has been presented by Jixin Liu et al., [16] towards distortion private information in videos at the graphic stage while minimizing the loss of significant graphic elements. Additionally, this ensures the caliber of the keyframe extraction process that comes next. Next, an algorithm for visual evaluation is suggested to determine the level of privacy protection provided by VPP-encoded video. Furthermore, the experiment demonstrates that the outcomes agree with the results of subjective assessment. A technique for assessing the level of privacy protection for multilayer compressed sensing video has been presented by Jixin Liu et al., [17]. The similar approach was utilized to map video sensibleness ratings by classifiers, and it was combined with a CNN and an RNN convolutional network to excerpt visual privacy protection scores with video spatial temporal feature mapping. The suggested strategy

outperformed earlier techniques in terms of identification result and generalization validation for videos. According to Kajal Kansal et al.,[18] deep learning-based re-identification (Re-ID) models encode personally identifiable information (PII) in the learnt features, which raises severe privacy problems, even though the models are solely trained with a Re-ID aim (i.e., if two samples belong to the same identity). It is a novel dual-stage person Re-ID system that, in consideration of current privacy legislation protecting personally identifiable information. An adversarial-identity (Adv-ID) module and a self-supervised de-identification (De-ID) decoder are used to accomplish the former, while a Gaussian noise generator and a controlled privacy budget are used in the latter mechanism to create a privacy-protected gallery. A novel 3D-Aware Adversarial Makeup Generation GAN (3DAM-GAN) has been presented by Yueming Lyu et al., [19]. which attempts to raise the standard and transferability of cosmetics that were synthetic for hiding identity information. A unique Makeup Transfer Module (MTM) and Makeup Adjustment Module (MAM) were utilized towards create a UV-based generator that uses the symmetric features of human faces to produce makeup that is resilient and realistic. To increase the transferability of black-box designs, a makeup attack approach along with an ensemble training technique was also suggested. To identify privacy parameters like windows, perpetrators, and, faces Alem Fitwi et al., [20] presented a Privacy-preserving Surveillance as an Edge service (PriSE) technique with a hybrid design that consists of a video protection scheme and lightweight foreground object scanner that functions on fog/cloud-based models and edge cameras. End-to-end privacy was guaranteed by the Reversible Chaotic Masking (ReCAM) apporach, and resource usage was minimized by the simplified foreground-object detector, which eliminates frames that solely contain background objects.

3. Proposed Architecture

Most of the current research focuses on ROI-based partial encryption with modest complication approaches like pixilation or blurring to empower privacy protection to reduce privacy and security issues in video surveillance systems. Hence, the optimal privacy protection technique aimed at image security in video surveillance. This technique is combined with various key problems such as compressibility, recoverability, characteristics preservation and de-identification in one unified architecture. This proposed technique developed a private residual error

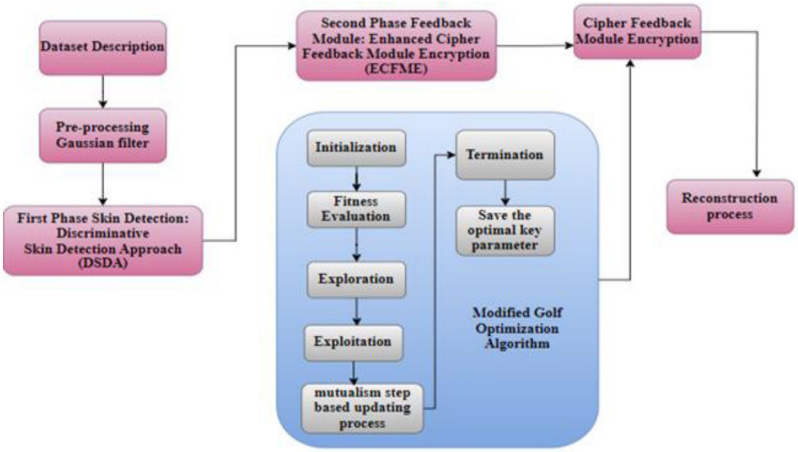


Figure 1

Block Diagram of Proposed Architecture

and a public stream through distorting the secure sensitive portion. The flow of the proposed process is illustrated in Figure 1. The proposed technique is developed by considering two phases such as human skin detection and encryption which empowers the privacy of the surveillance video. Initially, the databases are gathered. After that, it is sent to the pre-processing stage of the Gaussian filter to remove noises present in the image. The pre-processed image is sent to the human skin detection phase.

First Phase Skin Detection: This process is obtained by using DSDA. Based on this approach, the human skin portion is detected. Textural and spatial variables are frequently used in skin modeling to improve the skin classification schemes' ability to discriminate between different skin types. Second Phase Feedback Module: This process is obtained by using ECFME. In this process, the optimal key parameters are selected by the MGOA. Finally, the skin region is encrypted.

4. Results and Discussion

Performance analysis and comparison analysis are used to justify the projected approach's performance. The suggested method is designed to strengthen security by using video surveillance data. The identification and encryption of human skin are seen in the security footage. After that, it is rebuilt in a particular way. The suggested methodology is used to obtain this process. Efficiency of implemented proposed method is evaluated by performance measures such as encryption time, decryption

time, peak signal-to-noise ratio (PSNR), and normalization correlation (NC) are used to assess performances. The suggested methodology is contrasted with H.264/AVC, Rivest Shamir Adleman (RSA), Elliptical Curve Cryptography (ECC), NDLM, and other conventional techniques. The measures that were developed are enumerated below.

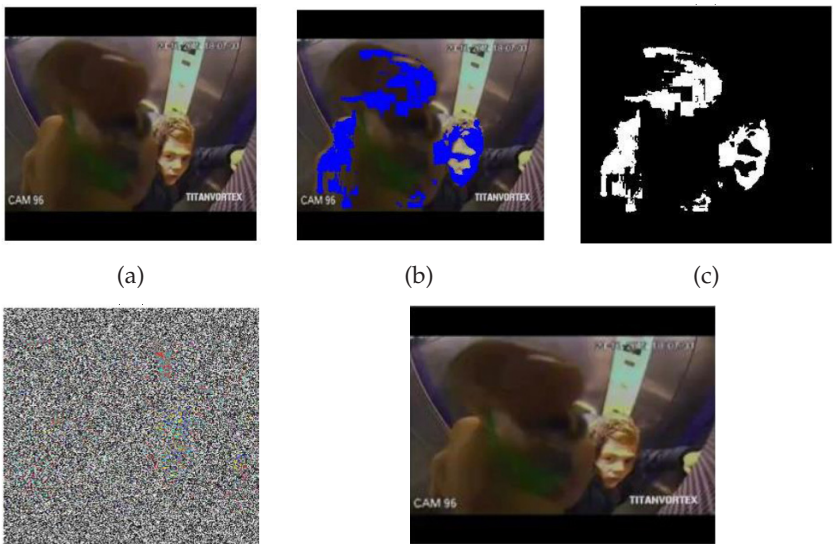
$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{\sqrt{MSE}} \tag{1}$$

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

$$NC\ (input\,imge, reconstruct\,image) = \frac{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{ini,j} w_{rci,j}}{\sqrt{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{ini,j}{}^2}\sqrt{\Sigma_{i=1}^{m}\Sigma_{j=1}^{n} w_{rci,j}{}^2}} \tag{3}$$

Performance Analysis

The input video is then transformed into various frames based on that. Figure 2 displays the photos that this database uses as input, skin detection, encryption, and output. Subsequently, the areas of human skin are identified. The identified areas of skin are sent to the encryption procedure to protect the private area (human skin). Ultimately, the encoding procedure is used to reconstruct the original image as well as it can be. The SSIM measure is calculated and shown in Table 1 to validate the suggested methodology. When enhancing security, the highest parameter is the ideal PSNR measure. The suggested method produced a 1.3SSIM measure in the fifth frame. Comparably, the traditional methods produced SSIM values of 1.1, 1.0, 0.8, and 0.75. The suggested method produced an SSIM measure of 1.2 in the tenth frame. Comparably, the traditional methods produced SSIM values of 0.88, 0.78, 0.56, and 0.48. In the fifteenth frame, the suggested method achieved a 0.9 SSIM measure. Comparably, the traditional methods produced SSIM values of 0.76, 0.71, 0.5, and 0.4. According to the validation, the anticipated strategy produced the best results in terms of the SSIM measure. Comparably, the traditional methods yield results at 35, 33, 28.5, and 28 PSNR. In the fifteenth frame, the suggested method achieved a 38 PSNR measurement. In a similar vein, 34, 32.5, 29.5, and 27.15 PSNR were obtained by the traditional methods. According to the validation, the planned strategy produced the optimal outcomes in terms of the PSNR metric.



(a) (b) (c)

(d) (e)

Figure 2

Proposed Process ((a) Input Image, (b) Skin Detection Phase 1, (c) Skin Detection Phase 2, (d) Encrypted Image and (e) Output Image

The proposed methodology is compared with the published articles and it is presented in Table 1.

Table 1

Comparison Analysis

S. No	Method	PSNR	NC	SSIM
1	Jixin Liu et al., [16] Multi-Layer Visual Privacy-Protected (VPP)	18	0.88	0.91
2	Jixin Liu et al., [17] CNN	28	0.68	0.75
3	Kajal Kansal et al., [18] Deep Learning-based Re-Identification (Re-ID)	20	0.71	0.83
4	Yueming Lyu et al., [19] 3D-Aware Adversarial Makeup Generation GAN (3DAM-GAN)	32	0.74	0.75
5	Alem Fitwi et al., [20] Reversible Chaotic Masking (ReCAM)	14	0.80	0.78
6	Proposed	56	1.5	1.3

The suggested method produced a 56 PSNR measure in the fifth frame. In the same way, the traditional methods are 38, 34, 31, and 28 PSNR. The suggested method produced a 48 PSNR measure in the tenth frame.

5. Conclusion and Future Scope

This paper has been developed an efficient privacy protection technique for image security in video surveillance. The proposed method has been developed by considering two phases such as human skin detection and encryption which empowers the privacy of the surveillance video. The input image has been sent to the pre-processing stage of the Gaussian filter to remove noises present in the image. The pre-processed image is sent to the human skin detection phase. In this phase, DSDA is utilized in human skin detection. Based on this approach, the human skin portion is detected. In this phase, ECFME is utilized for encrypting the image. In this process, the optimal key parameters are selected by the MGOA. Finally, the privacy protection is obtained by using the proposed method. Proposed method is to be extended in future with linear subspace learning techniques for handling the curse of dimensionality problems.

References

[1] Du, Haohua, Linlin Chen, Jianwei Qian, Jiahui Hou, Taeho Jung, and Xiang-Yang Li. "Patronus: A system for privacy-preserving cloud video surveillance." *IEEE Journal on Selected Areas in Communications* 38, no. 6 : 1252-1261 (2020).

[2] 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).

[3] Kim, Jinsu, and Namje Park. "A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems." Symmetry 12, no. 6 : 891 (2020).

[4] Elhadad, Ahmed, Safwat Hamad, Amal Khalifa, and Hussein Abulkasim. "A steganography approach for hiding privacy in video surveillance systems." In Digital Media Steganography, pp. 165-187. Academic Press (2020).

[5] Li, Hao, Tianhao Xiezhang, Cheng Yang, Lianbing Deng, and Peng Yi. "Secure video surveillance framework in smart city." Sensors 21, no. 13 : 4419 (2021).

[6] Yang, Jiachen, Yong Zhu, Shuai Xiao, Guipeng Lan, and Yang Li. "A controllable face forgery framework to enrich face-privacy-protection datasets." *Image and Vision Computing* 127 : 104566 (2022).

[7] Wen, Heping, Zhiyu Xie, Zhuxi Wu, Yiting Lin, and Wei Feng. "Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography." *Journal of King Saud University-Computer and Information Sciences* : 101871 (2023).

[8] Feng, Wenzhen, Guopeng Liang, Tiantian Wang, Guangshun Li, and Yuanwang Zheng. "A privacy protection scheme for facial recognition and resolution based on edge computing." Security and Communication Networks 2022 (2022).

[9] Mishra, Pratik K., Andrea Iaboni, Bing Ye, Kristine Newman, Alex Mihailidis, and Shehroz S. Khan. "Privacy-protecting behaviours of risk detection in people with dementia using videos." BioMedical Engineering OnLine 22, no. 1 : 1-17 (2023).

[10] Yang, Russell. "Privacy and surveillance concerns in machine learning fall prediction models: implications for geriatric care and the internet of medical things." AI & SOCIETY : 1-5 (2023).

[11] Du, Ling, Wei Zhang, Huazhu Fu, Wenqi Ren, and Xinpeng Zhang. "An efficient privacy protection scheme for data security in video surveillance." *Jnl. of visual communication and image representation* 59 : 347-362 (2019).

[12] Tu, Nguyen Anh, Thien Huynh-The, Kok-Seng Wong, M. Fatih Demirci, and Young-Koo Lee. "Toward efficient and intelligent video analytics with visual privacy protection for large-scale surveillance." *The Journal of Supercomputing* 77, no. 12 : 14374-14404 (2021).

[13] 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).

[14] Hosny, Khalid M., Mohamed A. Zaki, Hanaa M. Hamza, Mostafa M. Fouda, and Nabil A. Lashin. "Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection." IEEE Access 10 : 106750-106769 (2022).

[15] Tian, Xianhao, Peijia Zheng, and Jiwu Huang. "Robust privacy-preserving motion detection and object tracking in encrypted streaming video." *IEEE Transactions on Information Forensics and Security* 16 : 5381-5396 (2021).

[16] Liu, Jixin, Yicong Li, Guang Han, and Ning Sun. "Visual video evaluation association modeling based on chaotic pseudo-random multilayer compressed sensing for visual privacy-protected keyframe extraction." *Jnl. of Visual Communication and Image Representation* 90 : 103691 (2023).

[17] Liu, Jixin, Pengcheng Dai, Guang Han, and Ning Sun. "Combined CNN/RNN video privacy protection evaluation method for monitoring home scene violence." *Computers and Electrical Engineering* 106 : 108614 (2023).

[18] Küsmüş, Ömer & Hanoymak, Turgut. A novel public-key encryption scheme based on Bass cyclic units in integral group rings, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:2, 579-589 (2022), DOI: 10.1080/09720529.2020.1756042.

[19] Talapula, Dharani Kumar, Kumar, Adarsh, Ravulakollu, Kiran Kumar & Kumar, Manoj. A novel intrusion detection system in cloud infrastructure using deep learning technique, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1277–1303 (2023), DOI: 10.47974/JDMSC-1739.

[20] D'Alconzo, Giuseppe , Meneghetti, Alessio & Piasenti, Paolo. Security issues of CFS-like digital signature algorithms, *Journal of Discrete Mathematical Sciences and Cryptography*, 27:1, 175–187 (2024), DOI: 10.47974/JDMSC-1643.