Engineered Science
DOI: https://dx.doi.org/10.30919/es1429

Privacy Protection in Surveillance Videos Using Human Skin Encryption with Efficient Feedback Mechanism

Dattatray G Takale,[1,*] Gargi Joshi,[2,*] Tushar Jadhav,[3] Deepali S. Jadhav,[4] Sonali M. Antad,[5] Chitrakant O. Banchhor,[6] Omkaresh Kulkarni,[7] Parikshit N. Mahalle,[8,*] Gopal B. Deshmukh[9] and Bipin Sule[10]

Abstract

This paper presents an optimized privacy protection framework designed to enhance image security in video surveillance, addressing key challenges such as de-identification, compressibility, recoverability, and preservation within a unified architecture. The proposed approach introduces a hybrid system combining advanced human skin detection and encryption techniques to safeguard sensitive information under varying lighting and environmental conditions. The methodology operates in two key phases: skin detection and encryption. In the first phase, a discriminative skin detection approach (DSDA) is employed to identify human skin regions accurately. This approach leverages textural and spatial variables to enhance the classification of skin types, ensuring precise detection. An enhanced cipher feedback module encryption (ECFME) encrypts the detected skin regions in the second phase. The modified golf optimization algorithm (MGOA) optimizes the encryption process, ensuring optimal vital parameters are selected for robust encryption. The input image undergoes preprocessing using a Gaussian filter to eliminate noise before proceeding to the detection and encryption stages. The methodology is implemented in MATLAB, and its performance is evaluated using comprehensive metrics. Comparative analysis demonstrates that the proposed approach outperforms conventional accuracy, efficiency, and privacy preservation techniques. This study contributes significantly to the field of privacy protection in video surveillance, offering a reliable and efficient solution for safeguarding sensitive visual data.

Keywords: Skin detection; Discriminative skin detection approach; Enhanced cipher feedback module encryption; Modified golf optimization algorithm.
Received: 12 December 2024; Revised: 07 February 2025; Accepted: 15 February 2025.
Article type: Research article.

1. Introduction

Because human skin is not uniform, identifying individuals in movies is an ever-evolving challenge 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 the contrast in lighting. The primary 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 and 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 more arduous and time-consuming computing effort during the following picture processing stage.[7] To overcome these shortcomings, multilayer CS ciphering is performed on

[1] *Department of Computer Engineering, BRACT's Vishwakarma Institute of Information Technology, Pune, 411048, India*
[2] *Symbiosis Institute of Technology, Symbiosis International Deemed University, Pune, 412115, India*
[3] *Department of Electronics and Telecommunications, BRACT's Vishwakarma Institute of Information Technology, Pune, 411048, India*
[4] *Department of Computer Engineering, BRACT's Vishwakarma Institute of Technology, Pune, 411037, India*
[5] *Department of Information Technology BRACT's Vishwakarma Institute of Technology, Pune, 411037, India*

surveillance video that is susceptible to privacy leaks using compressed sensing (CS) technology in this work, resulting in visual privacy protection (VPP).[8] Additionally, we must carefully evaluate how to protect personal data during the VPP process. Furthermore, consideration must be given to the data loss caused by the compression coding of video pictures aimed at the entire system procedure, together with partial transmission of visual information, processing or imaging, processing, *etc*.[9] 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 has given rise to several different assessment techniques,[14] each with its drawbacks. The evaluation method's central body is separated into two approaches: (i) examine the technique from a coding security standpoint. The evaluation method's central body is separated into two categories: (ii) it analyses the technique from the standpoint of coding security and assesses how well it protects privacy by assessing the algorithm's security.[15]

1.1 The main contribution of the research

Initially, the databases are gathered. After that, it is sent to the preprocessing stage of the Gaussian filter to remove noises present in the image. The preprocessed image is sent to the human skin detection phase.

- First Phase Skin Detection: This process is obtained by using the discriminative skin detection approach (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 enhanced cipher feedback module encryption (ECFME). The modified golf optimization algorithm (MGOA) selects the optimal vital parameters in this process. Finally, the skin region is encrypted.

This discusses a few common strategies for protecting privacy in surveillance videos. A multilayer VPP coding technique has been presented by Liu *et al*.[16] for the distortion of private information in videos at the graphic stage while minimizing the loss of significant graphic elements. Additionally, this ensures the calibre 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 subjective assessment results. Furthermore, we present an unsupervised two-layer clustering keyframe extraction technique with a matching presentation assessment index for VPP-encoded video. Ultimately, an association model is developed to strike a compromise between the effectiveness of keyframe extraction and the quality of privacy protection.

Liu *et al*.[17] have presented a technique for assessing the level of privacy protection for multilayer compressed sensing video. A similar approach was utilized to map video sensibleness ratings by classifiers, and it was combined with a convolutional neural network (CNN) and an recurrent neural network (RNN) to excerpt visual privacy protection scores with video spatial-temporal feature mapping. The suggested strategy outperforms earlier techniques regarding identification results and video generalization validation. Ultimately, a design of the relationship between the practicability score and the visual privacy protection score is constructed.

According to Kansal *et al*.,[18] deep learning-based re-identification (Re-ID) models encode personally identifiable information (PII) in the learned 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). We suggest a novel dual-stage person Re-ID system that, considering current privacy legislation protecting personally identifiable information, (1) suppresses PII from discriminative features and (2) uses differential privacy to create a configurable privacy mechanism. An adversarial identity (Adv-ID) module and a self-supervised de-

[6] *Department of CSE (Artificial Intelligence), BRACT's Vishwakarma Institute of Information Technology, Pune, 411048, India*

[7] *Department of Artificial Intelligence and Machine Learning, BRACT's Vishwakarma Institute of Information Technology, Pune, 411048, India*

[8] *Research and Development, Vishwakarma Institute of Technology, Pune, 411037, India*

[9] *Department of Computer Engineering, BRACT's Vishwakarma Institute of Information Technology, Pune, 411048, India*

[10] *BRACT's Vishwakarma Institute of Technology, Pune, 411037, India*

**Email:* dattatray.takale@viit.ac.in (D. G. Takale); gargi.bhide@sitpune.edu.in (G. Joshi); parikshit.mahalle@vit.edu (P. N. Mahalle)

identification (De-ID) decoder are used to accomplish the former. In contrast, a Gaussian noise generator and a controlled privacy budget are used in the latter mechanism to create a privacy-protected gallery.

Lyu *et al*.[19] have presented a novel 3D-aware adversarial makeup generation generative adversarial networks (3DAM-GAN). This attempt raises the standard and transferability of synthetic cosmetics for hiding identity information. A unique makeup transfer module (MTM) and makeup adjustment module (MAM) were utilized to create a universal vertex (UV) based generator that uses the symmetric features of human faces to produce resilient and realistic makeup. A makeup attack approach and an ensemble training technique were also suggested to increase the transferability of black-box designs. To identify privacy parameters like windows, perpetrators, and faces, 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) approach, and resource usage was minimized by the simplified foreground-object detector, which eliminates frames that solely contain background objects. A reliable window-object detector was created to stop people from looking in through windows. A multi-tasked cascaded convolutional neural network (MTCNN) was used to detect faces to achieve de-identification.

2. Materials and methods

A brief overview of the models and techniques used in the field of privacy protection in surveillance video is provided in this section. We also briefly explain the suggested technique for encrypting surveillance video while protecting privacy and detecting skin. This section includes a description of the datasets and an explanation of the suggested background studies. To validate the projected approach, consider the surveillance camera video. In Fig. 1, Videos from 13 classes are included in this dataset: assault, robbery, explosion, fighting, theft, shoplifting, vandalism, arrest, arson, assault,

Fig. 1: Sample input frames from five surveillance videos representing different types of security incidents.[13]

and accident. Based on the content of each video, a classification of normal (0) or abnormal (1) is assigned to it. Every label is located in Ref. [21].

2.1 Preprocessing model

Image denoising aims to reduce noise without sacrificing the necessary image qualities. Gaussian filters are applied in this study to eliminate noise from the converted frame (input image).[22] It is a standard linear filter that is mainly employed for denoising images. The following Equation (1) describes how the pixel weight in this filter reductions with distance from the filter center:

$$g_{\sigma(x,y)} = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}} \quad (1)$$

The Gaussian filter reduces noise while maintaining picture features by averaging pixel parameters over a local area. This method assumes that images have smooth spatial changes and that pixels in a region have close parameters. The noise removal image is sent to the skin detection phase to protect private information by detecting the skin portions from the surveillance image.

2.2 First phase skin detection: DSDA

The most distinguishing skin feature, defined as chrominance combined with luminance, is identified in this phase, and the skin colour is correctly constructed in various colour spaces, supporting the virtual reality of traditional skin detection approaches. Furthermore, the significant variance of the colour inside the skin class and the high likeness of various backdrop substances to the skin limits the color's ability to discriminate. Consequently, this establishes a particular upper constraint on the effectiveness of skin models based on colour. A skin design is generally assumed to be more ubiquitous, with more excellent false-positive rates. This architecture must leverage the remaining features and the pixel-wise colour-related categorization to minimize false positives.[23] This research contribution is related to the observation that, in various conditions, the false positive presents a comparatively smooth design in the luminance and colour areas.

The image is converted to grayscale throughout this procedure. A skin probability map is then considered, and a Bayesian classifier is employed. The higher chance is indicated on the map by the darker shade. The smooth design with little differences in the combined grayscale and colour areas characterizes the magnified non-skin area. Furthermore, differences in the skin probability are seen according to the texture pattern, which is invisible in the actual skin areas. Furthermore, after applying the acceptance reference, there would be false positives because the parameters in the probability map are typically high inside the area and not the same as the probability of the actual skin regions. Similar observations are made for several photos, which generally leads to the conclusion that the textural characteristics taken from the probability map could be helpful in skin identification.[24]

We modified a design that can be created for the image colorization requirements to compute textural information and provide the optimal possible discernment among the non-skin and skin areas. First, compute basic picture statistics for different dimensions and kernels. The general image features are produced and then connected to LDA to create the discriminative textural feature space. An input skin probability map is converted into a discriminative textural feature space skin map by taking discriminative textural feature space into account. Lower identification mistakes follow from the ideal division between non-skin and skin pixels.

2.2.1 Discriminative skin presence features (DSPF)

Using kernels of various sizes, the first simple analysis is calculated from every pixel neighborhood in the probability map to compute the discriminative skin attendance features. Four characteristics, the standard deviation, the minimal parameters, the median, and the difference between the maximum and minimum are calculated experimentally. The feature vector also has the raw skin probability parameter applied to it. The skin probability parameter and its variation in the vicinity of the processed pixel are specified using these features.

The feature vector also has the raw skin probability parameter applied to it. This characteristic is explicitly applied to the skin probability parameter and its variance in the vicinity of the processed pixel. Subsequently, skin and non-skin pixels are altered into dual feature vector classes connected to latent dirichlet allocation (LDA) to enhance their ability to discriminate. This is a research procedure to obtain features. It then produces a discriminative feature space, which is used to create the skin maps aimed at the DSPF.[25] First, Bayesian skin modeling obtains the probability lookup table for a specified training pair of images and related skin masks. Finally, the LDA projection matrix is calculated using the generic feature vectors that are categorized with ground truth skin masks.

It is necessary to remember that the fundamental picture features projected onto the DSPF space of a pixel do not clearly state whether the pixel defines skin. Some reference points in the DSPF space must be provided for classification. Generally speaking, the DSPF aims to maximize the distances between the

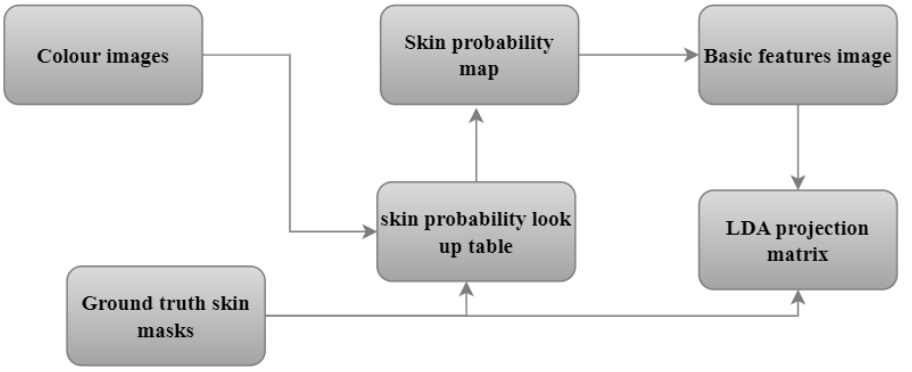

Fig. 2: Block diagram of the training of detection process.

skin and non-skin classes while decreasing the distances inside them.

2.2.2 Based on DSPF skin detection

The three standard stages of skin detection processing are skin probability map calculation considering the Bayesian classifier, skin map generation utilizing DSPF space, and spatial validation associated with the DSPF skin map. First, the lookup table obtained from learning the Bayesian model converts the input image into the skin probability map. Additionally, utilizing the LDA projection matrix,[26] each pixel from the probability map is in the DSPF region. This skin map is produced in the DSPF space of each pixel S from the threshold pixel R and is based on the distance function using Equation (2):

$$d(S) = \left[\sum_{I=1}^{M}\left(T_I^{(S)} - T_I^{(R)}\right)^2\right]^{1/2} \quad (2)$$

where $T_I^{(S)}$ is defined as the dimension of the DSPF vector achieved aimed at the pixel S.

Using the high kernel function, the reference pixel is calculated using the highest probability parameter associated with erosion in the skin probability map. Because the nearby non-skin pixels can obscure the textural features, the threshold pixel should not be an inaccessible skin location, so erosion is necessary.[27] The procedure ensures that the reference pixel is calculated to maximize the extraction of its DSPFs from pixels with a high skin probability parameter. Because of this, the dimension of the erosion kernel is larger than the highest kernel utilized for BIF extraction. Afterward, to handle the input images, which do not contain human skin altogether as best as possible, the probability parameter of the threshold pixel needs to be overhead of the point reference. Finally, the distances of DSPF space are calculated from the reference pixel sorted from 1 for the threshold pixel to 0 for the highest distance, which is used to create the DSPF skin map Equation (3):

$$d_n(S) = \frac{(d_{max} - d(S))}{d_{max}} \quad (3)$$

The scaling function assumes that there are a few non-skin pixels in the image. It encounters full-life visuals at random in this scenario. When the acceptance reference is used, the DSPF skin map proposes a more excellent parting between non-skin and skin pixels, lowering the identification errors. Furthermore, carrying out spatial validation can reduce identification errors. In this instance, the normalized distance map's calculation of the probability cost is done as follows Equation (4):

$$\rho_P(S \to U) = \begin{cases} 1 - d_n(U), & for\ d_n(U) > P_\beta \\ \infty, & for\ d_n(U) \le P_\beta \end{cases} \quad (4)$$

Comparing the DSPF skin map to the conventional skin probability map, it can be an ideal propagation domain since it is based on features that effectively distinguish between non-skin pixels and the skin. Furthermore, validating the DSPF maps implies that determining the optimal seed threshold parameter is straightforward. In this approach, the pixels that have the highest degree of resemblance to the reference pixel in the DSPF domain design the skin. Skinless is achieved by scaling the distance on the map from 1 for the skins to 0 for the most significant distance, and the distance transform is confirmed from the skins.

2.3 Second phase feedback module: ECFME

Following skin identification (Table 1), x the pixel parameters in the positions designated by a bitmap were encrypted utilizing the CFME in the suggested approach. This paradigm is used because it makes it possible to encrypt real-time streaming surveillance data using a stream cipher called AES, which complements a block cipher. Additionally, CFME mode holds the characteristics of chaining dependency and self-synchronization.[28] Additionally, in this phase, any variation in the plain bitstream or the setup vector is reproduced in the preceding encrypted output bitstream. Hence, there is no

requirement to manage the secret key. The skin pixels are also encrypted individualistically and do not create necessary encryption bitrate overhead. This encryption procedure is formulated as follows in Equations (5) and (6):

$$V_I = V_E(E_I - 1) \quad (5)$$

$$E_I = M_I \oplus V_I \quad (6)$$

where E_I is defined as the skin-encrypted output bitstream, M_I as the skin-encrypted output bitstream, the XOR operator and V_I are defined as the generated keys stream. E_I are encrypted output skin regions. This encryption starts with creating the current encrypted bitstream as output by XORing the previous encrypted bitstream with the current plain bitstream.

Table 1: The algorithm of seudocode of proposed encryption approach.

Input: Skin-detected frames
Skin encryption ()
Int Dh key () //* secret key exchange Diffie Hellam*// MGOA (key generation)
Private key1, public key 2, public key1 and private key 2
long int x=PK 1
long int y=PK 2
long int z= private key 1
long int a= private key 2
S= y's mod x
T=y's mod x
Temp=S
S=T
T=Temp
kz=Y's mod M;
Ka=x's mod M;
N=kz=ka;
Return (N);
Output: secret key (N)
//* secret key optimally selected by using MGOA*//
}
Proposed encryption
Input: skin detection pixels, initialization vector, key size=128, and secret key
defined (CIPHER_MODE)
Encryption (ENCRYPT_AES)
Encrypt
Output: Skin-encrypted video bitstream
}
Reconstruct (); // skin encrypted bitstream and non-skin bitstream reconstruction //
Output: Bitstream with skin encrypted.

The Diffie-Hellman essential exchange technique generates and distributes the 128-bit encryption key. Subsequently, the non-skin pixels and skin-encrypted output bitstream are rebuilt to provide a private output bitstream. This suggested encryption creates a private area by independently encrypting the skin pixels without interfering with the video frame's design. After that, the suggested technique leaves the protected sensitive region's design intact, allowing for the observation of human traits without disclosing the identity of the subjects. For this reason, the suggested approach is suitable for real-time applications. Subsequently, it becomes imperative to interpret video and analyze behavior while protecting individuals' privacy.

In the second stage, every video frame deprived of skin identification was selectively encrypted using the research's proprietary system as a default, lightweight encryption method for surveillance footage. This selective encryption enhances the H.264/AVC codex operating in a single-layer phase, considering the compression procedures with scalable video coding (SVC). It is described as encryption occurring during a portion of the H.264/SVC compression process in a phase connected to H.264/AVC. The locations inside each frame are established by a bitmap following the first encryption phase, which encrypts detected skin detection. In this case, the suggested encryption encrypts only the skin pixels by acting as a stream cipher. The chosen areas of the image are encrypted using this recommended technique. Lastly, it serves as the default method of protecting surveillance video; in the proposed technique, skin pixels are encrypted, and similar compression is applied for the detected skin portion. The selection is based on coding parameters rather than skin pixels in the selectively encrypted bitstreams. Therefore, skin encryption offers adequate privacy protection; the remaining pixels remain unencrypted, and the protected surveillance movies retain the necessary data that is subsequently used for real-time analysis. If an authorized individual has to access an encrypted image using a comparable 128-bit secret key, MGOA is the best method for selecting this secret key.

2.4 Modified golf optimization algorithm

Golf is an outdoor team sport or solitary game played with specially designed clubs that must be skillfully manipulated. The generational foundations of this game mandate that it requires deft handling of the ball's propulsion from its starting position to a far-off hole. This activity, played with deliberate strokes and subject to a set of rules, is golf's ultimate form. Even with the apparent simplicity, the game's rules introduce complexity, enabling a higher degree of difficulty.[29] The algorithm draws inspiration from this tactical dance, an example of intellectual strength. This technique is the algorithm's blueprint, smoothly integrating its contours into a design architecture. This technique is used in the GOA to

compute embodiment, define its phases, and crystallize its conceptual foundations through rigorous mathematical modeling.

2.4.1 Step 1: Setup

A population-related method uses a haphazard search of its associates in the issue-solving space to supply the necessary solutions to optimization problems. The problem's parameters are computed based on the GOA members' positions inside the problem search space. Equation (7) provides a matrix used to define GOA members' population numerically. Compared to the different techniques, population members are uniformly distributed and randomly dispersed over the issue space. Equation (8) randomly initializes the GOA associates' locations in the search space at the start of the algorithm's execution.

$$S = \begin{bmatrix} S_1 \\ \dots \\ S_I \\ \dots \\ S_N \end{bmatrix}_{N\times M} = \begin{bmatrix} S_{1,1} & \dots & S_{1,D} & \dots & S_{1,M} \\ \dots & \dots & \dots & \dots & \dots \\ S_{I,1} & \dots & S_{I,D} & \dots & S_{I,M} \\ \dots & \dots & \dots & \dots & \dots \\ S_{N,1} & \dots & S_{N,D} & \dots & S_{N,M} \end{bmatrix}_{N\times M} \quad (7)$$

$$S_I: S_{I,D} = LB_D + R \times (UB_D - LB_D) \quad (8)$$

where UB_D is defined as the upper bound of the variable, LB_D is defined as the lower bound of the variable, R is defined as the random variable in the range [0-1], M is defined as the number of parameters, N is the number of GOA members, $S_{I,D}$ is the parameter of the GOA member variable, S_I is defined as the GOA member, and S is defined as the population matrix of GOA with $N \times M$.

2.4.2 Step 2: Calculating fitness

This approach computes the problem parameters associated with each GOA member and treats each one as a potential solution to the problem. The objective function's parameter is calculated. A vector connected to Equation (9) is used to determine the computed parameters for the fitness function.

$$FF = Min\,(Encryption\ Time) \quad (9)$$

$$FV = \begin{bmatrix} f_1 \\ \dots \\ f_I \\ \dots \\ f_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} f(S_1) \\ \dots \\ f(S_I) \\ \dots \\ f(S_N) \end{bmatrix}_{N\times 1} \quad (10)$$

where FF is defined as the achieved parameter of the fitness function related to their GOA member, and FV is defined as the vector of objective function parameters. The parameter provided as the fitness function's optimal parameter is identified as the optimal member by comparing the parameters achieved for the objective function. Every iteration upgrades the fitness function's parameters and the location of the GOA members; therefore, it stands to reason that every iteration also upgrades the population's optimal member.

2.4.3 Step 3: Exploration

After the algorithm's setup phase, GOA begins upgrading the population's members. There are two phases to population upgrading in GOA: exploitation and exploration. The exploration hole is the location of the ideal member.[30] This method defines the GOA's exploration capacity in a global search by scanning different parts of the search space.

In this procedure, a novel position is initially determined and aimed at each GOA member using Equation (11), based on the simulation of the player's most vital shot at the ball. The relevant member's prior location is then replaced based on Equation (11) if the value of the fitness function increases in this afresh computed position. Players can make shots in golf where the ball goes through or gets close to the hole. Equations (10) and (11) describe the GOA members' upgrading procedure during the exploring stage.[31]

$$S_I^{U1}: S_{I,D}^{U1} = S_{I,D} + R \times \left(b_D - I \times S_{I,D}\right) \quad (11)$$

$$S_I = \begin{cases} S_I^{U1}, & f_I^{U1} < f_I \\ S_I, & Else \end{cases} \quad (12)$$

where I is defined as the arbitrary number that is chosen randomly from the pair of $\{1,2\}$, R is defined as the random number in the interval [0-1], b_D is defined as the dimension, b is defined as the optimal member of GOA, f_I^{U1} is defined as an objective function parameter, $S_{I,D}^{U1}$ is defined as its dimension, and S_I^{U1} is defined as the new computed phase of GOA members related to the exploration stage.[32]

2.4.4 Step 4: Exploitation

The playground area, known as the "green," is where the hole is located. Players attempt to place the golf ball hooked on the hole here using thrills classified as putts. Low-power kicks best prevent the golf ball from changing direction between the green and the hole. This technique defines the exploitation potential of the GOA in a local search by enabling the optimal scanning of the location where each GOA member is presented. Equations (13) and (14) outline the process for upgrading GOA members to the exploitation stage.

During this phase of the GOA upgrade, each GOA member's new position is calculated using Equation (13), which deals with the exact construction of low-power strokes made by the player to the ball. The last location of the associated member related to Equation (14) is altered by the novel location if it increases the parameter of the fitness function.

$$S_I^{U2}: S_{I,D}^{U2} = S_{I,D} + (1-2R) \times \frac{LB_D + R \times (UB_D - LB_D)}{T} \quad (13)$$

$$S_I = \begin{cases} S_I^{U2}, f_I^{U2} < f_I \\ S_I, Else \end{cases} \quad (14)$$

where f_I^{U2} is defined as the fitness function parameter, $S_{I,D}^{U2}$ is its dimension, $and\ S_I^{U2}$ is defined as the novel computed position of the GOA member related to the exploitation stage. After every stage of upgrading the location of the population variables, it must be validated if the novel solutions are related to the pair of possible solutions or not. The initial group of restraints correlates to the satisfactory period for choice parameters. If the parameter of the decision parameters slightly surpasses the lower or upper band, its parameter is usually on the marginal parameters.

2.4.5 Step 5: Mutualism step-based updating process

After finishing the setup step, the global optimal solution is determined by computing each fitness. Following that, the mutualism step is handled at each iteration. At this point, two people are selected randomly from each individual's population. To list the new parameters for both the current individual and the remaining random individual, the individual with the lowest fitness score amongst these two arbitrarily chosen individuals is selected. The update procedure is designed so that the first random individuals who get the minimum fitness between the two can do so Equations (15) and (16) or (17) and (18):

$$S_I^{k+1} = S_I^k + RND(0,1) \times (S_M - mv \times bf^1) \quad (15)$$

$$S_N^{k+1} = S_N^k + RND(0,1) \times (S_M - mv \times bf^2) \quad (16)$$

$$S_I^{k+1} = S_I^k + RND(0,1) \times (S_N - mv \times bf^1) \quad (17)$$

$$S_N^{k+1} = S_N^k + RND(0,1) \times (S_N - mv \times bf^2) \quad (18)$$

where RND is defined as the random number in the range [0,1], bf^1, bf^2 are defined as the benefit factor having a randomly created parameter of either one or two, $mean(S_I, S_M)$ is a second occasion, $mean(S_I, S_N)$ is the first occasion, and mv is defined as the enumerated mean. Based on this process, the optimal updating process of GOA is obtained, which empowers the solution of privacy protection in surveillance.

2.5 Proposed architecture

Most current research focuses on region of interest (ROI) based partial encryption with modest complication approaches like pixelation or blurring to empower privacy protection and reduce privacy and security issues in video surveillance systems. Though such a method cannot withstand privacy attacks, it is nonetheless likely beneficial for protecting privacy in public real-time. Hence, the optimal privacy protection technique aimed at image security in video surveillance. This technique combines vital problems such as compressibility, recoverability, characteristics preservation, and de-identification in one unified architecture. This proposed technique developed a private residual error and a public stream by distorting the secure sensitive portion. This study takes into account both research areas. It suggests a hybrid system for detecting and protecting human skin using color information under constantly changing lighting and environmental circumstances. The flow of the proposed process is illustrated in Fig. 3.

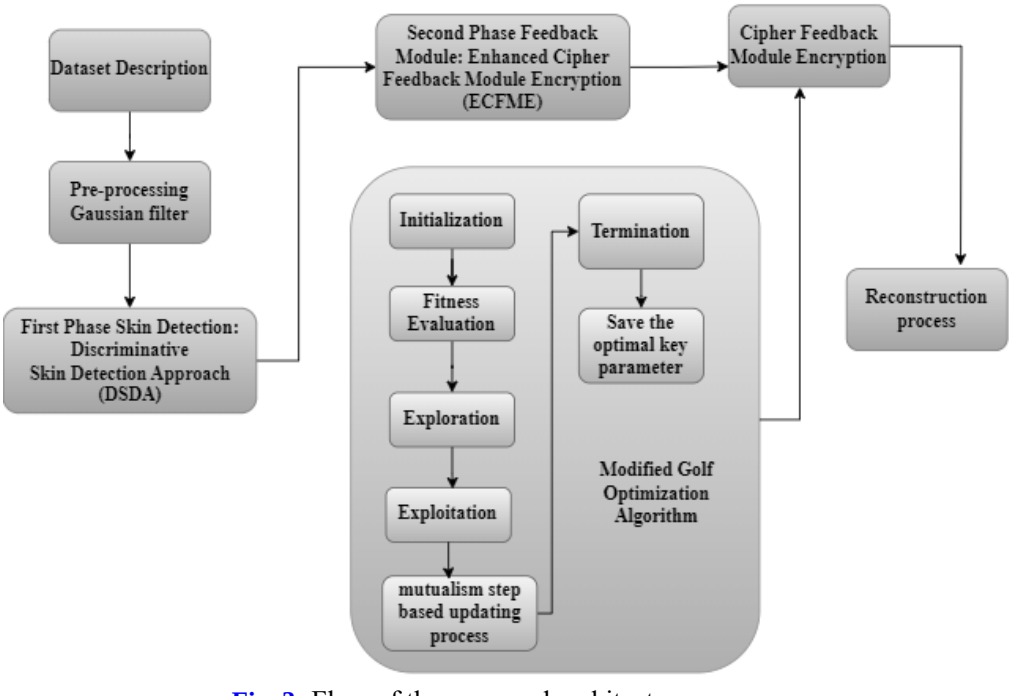

Fig. 3: Flow of the proposed architecture process.

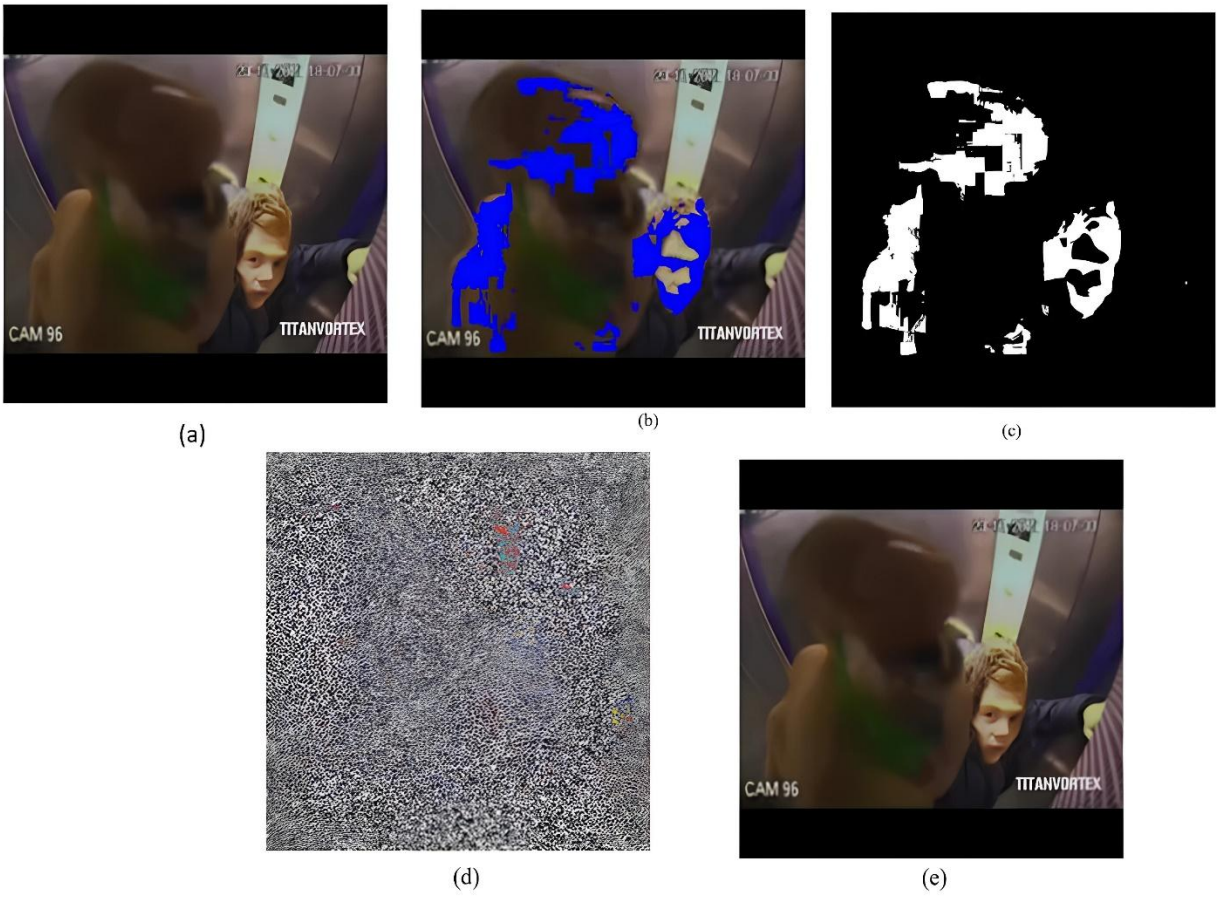

Fig. 4: Proposed process (a) input image, (b) skin detection phase 1, (c) skin detection phase 2, (d) encrypted image and (e) output image.

The proposed technique is developed by considering two phases, skin detection and encryption, which empower the privacy of the surveillance video. Initially, the databases are gathered. After that, it is sent to the preprocessing stage of the Gaussian filter to remove noises present in the image. The preprocessed image is sent to the human skin detection phase. One is the 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 modelling to improve the skin classification schemes' ability to discriminate between different skin types. The other is the Second Phase Feedback Module: This process is obtained by using ECFME. In this process, the MGOA selects the optimal vital parameters. Finally, the skin region is encrypted.[33]

3. 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.[34] After that, it is rebuilt in a particular way. The suggested methodology is used to obtain this process. The suggested method is implemented in MATLAB, and metrics such as encryption time, decryption time, peak signal-to-noise ratio (PSNR), and normalization correlation (NC) are used to assess performances. The proposed methodology is contrasted with H.264/AVC, rivest shamir adleman (RSA), elliptical curve cryptography (ECC), nonlinear dynamic logistic mapping (NDLM), and other conventional techniques. Table 2 contains a list of the implementation parameters.

Table 2: Implementation parameters.

S. No	Measures	Values
1	Radius	50
2	Dimension	30
3	Upper bound	10
4	Lower bound	-10
5	Number of populations	100
6	Number of iterations	100

The measures that were developed are enumerated in Equations (19)-(21).

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{\sqrt{MSE}} \quad (19)$$

$$SSIM = \frac{(2\times\overline{x}\times\overline{y}+c1)(2\times\sigma_{xy}+c2)}{(\sigma_x^2+\sigma_y^2+c2)\times((\overline{x})^2+(\overline{y})^2+c2)} \quad (20)$$

$$NC(input\ image, reconstruct\ image) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w_{ini,j}w_{rci,j}}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w_{ini,j}{}^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w_{rci,j}{}^2}} \quad (21)$$

3.1. Performance analysis

The online data is considered to validate the suggested strategy; the specifics are given in Section 3. The input video is then transformed into various frames based on that. Fig. 4 displays this database's photos 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 NC metric is calculated and shown in Fig. 5 to validate the suggested technique. When enhancing security, the highest parameter is the ideal NC measure. The suggested method produced a 1.5 NC measure in the fifth frame. The traditional methods yield results at 1.1, 1, 0.98, and 0.85 NC in a similar manner. The suggested method produced a 1.2 NC measure in the tenth frame. The traditional methods produced similar results of 0.98, 0.96, 0.92, and 0.84 NC. In the fifteenth frame, the suggested method achieved a 1.2 NC measure. The traditional methods yield results at 0.96, 0.94, 0.89, and 0.82 NC in a similar manner. According to the validation, the projected strategy produced the best results in terms of the NC measure.

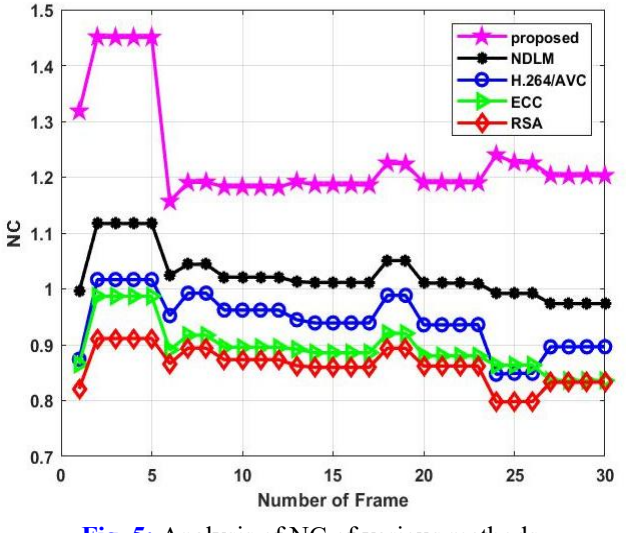

Fig. 5: Analysis of NC of various methods.

As shown in Fig. 6, the suggested methodology is validated by decryption time analysis. It contrasts traditional methods like RSA, ECC, H.264/AVC, and NDLM. The proposed method has achieved a decryption time of two seconds. The decryption times for the traditional methods, NDLM, H.264/AVC, RSA, and ECC, are 3, 4, 6, and 26s. The anticipated method attained a minimal decryption duration in connection with this validation. As shown in Fig. 7, the suggested methodology is validated by analyzing it according to encryption time. It contrasts traditional methods like RSA, ECC, H.264/AVC, and NDLM. The anticipated method has achieved an encryption time of 1.7 seconds. The decryption times for the traditional methods NDLM, H.264/AVC, RSA, and ECC are 2, 3, 7, and 26s. In connection with this confirmation, the anticipated method attained brief encryption durations.

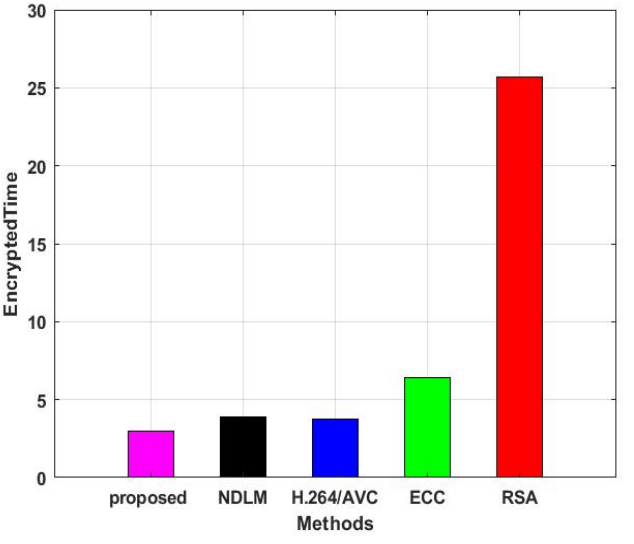

Fig. 6: Analysis of encryption time under various methods.

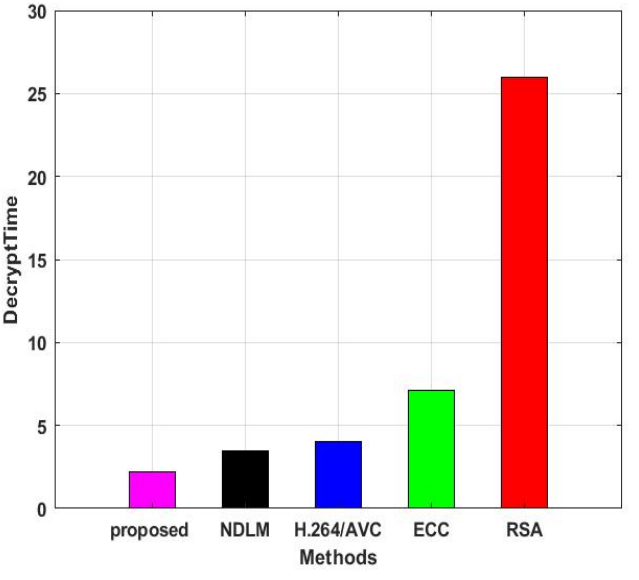

Fig. 7: Analysis of decryption time under various methods.

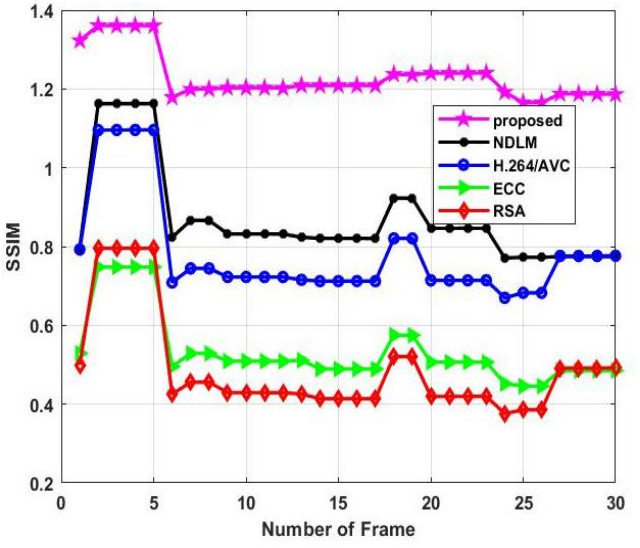

Fig. 8: Structural similarity index measure (SSIM) of various methods.

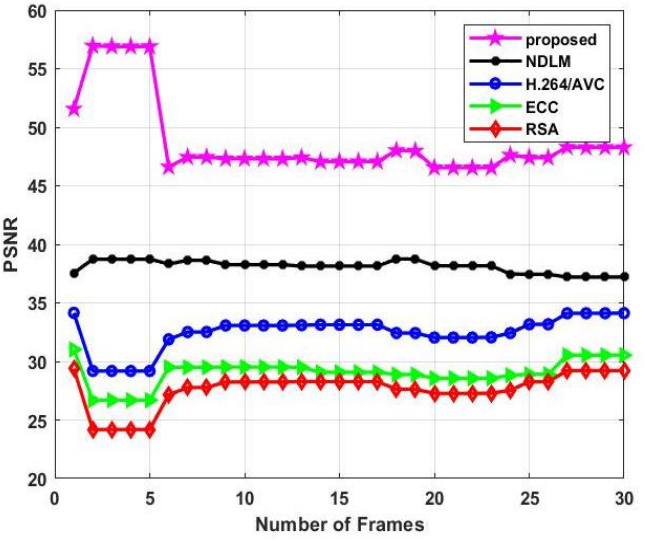

Fig. 9: The PSNR value of various methods.

The SSIM measure is calculated and shown in Fig. 8 to validate the suggested methodology. In Fig. 9, 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 regarding the SSIM measure. The proposed methodology is compared with the previous researches and presented in Table 3.

Table 3: Comparison analysis.

S. No	Method	PSNR	NC	SSIM
1	Liu *et al.*[16] multilayer VPP	18	0.88	0.91
2	Liu *et al.*[17] CNN	28	0.68	0.75
3	Kansal *et al.*[18] deep learning-based Re-ID	20	0.71	0.83
4	Lyu *et al.*[19] 3DAM-GAN	32	0.74	0.75
5	Alem *et al.*[20] ReCAM	14	0.80	0.78
6	Proposed method	56	1.5	1.3

The PSNR measure is calculated and displayed in Fig. 9 to validate the suggested methodology. When enhancing security, the highest parameter is the ideal PSNR measure. 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. 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. Similarly, traditional methods obtained 34, 32.5, 29.5, and 27.15 PSNR. According to the validation, the planned strategy produced the optimal outcomes regarding the PSNR metric.

4. Conclusion

This paper has developed an efficient privacy protection technique for image security in video surveillance. The proposed method has been developed by considering two phases, skin detection and encryption, which empower the privacy of the surveillance video. The input image has been sent to the preprocessing stage of the Gaussian filter to remove noises present in the image. The preprocessed 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 to encrypt the image. In this process, the MGOA selects the optimal vital parameters. Finally, privacy protection is obtained using the proposed method. The proposed methodology is applied in MATLAB, and the presentation is computed using performance measures. The proposed method is contrasted with the conventional techniques. In future, the real-time data will be considered for the analysis.

Conflict of Interest

There is no conflict of interest.

Supporting Information

Not applicable.

References

[1] H. Du, L. Chen, J. Qian, J. Hou, T. Jung, X. Li, PatronuS: A system for privacy-preserving cloud video surveillance, *IEEE Journal on Selected Areas in Communications*, 2020, **38**, 1252-1261, doi: 10.1109/JSAC.2020.2986665.

[2] Y. Qiu, Z. Niu, B. Song, T. Ma, A. Al-Dhelaan, M. Al-Dhelaan, A novel generative model for face privacy protection in video surveillance with utility maintenance, *Applied Sciences*, 2022, **12**, 6962, doi: 10.3390/app12146962.

[3] J. Kim, N. Park, A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems, *Symmetry*, 2020, **12**, 891, doi: 10.3390/sym12060891.

[4] A. Elhadad, S. Hamad, A. Khalifa, H. Abulkasim, A steganography approach for hiding privacy in video surveillance systems, Digital Media Steganography, Academic Press, 2020, 165-187, ISBN: 978-0-12-819438-6.

[5] H. Li, T. Xiezhang, C. Yang, L. Deng, P. Yi, Secure video surveillance framework in smart city, *Sensors*, 2021, **21**, 4419, doi: 10.3390/s21134419.

[6] J. Yang, Y. Zhu, S. Xiao, G. Lan, Y. Li, A controllable face forgery framework to enrich face-privacy-protection datasets, *Image and Vision Computing*, 2022, **127**, 104566, doi: 10.1016/j.imavis.2022.104566.

[7] H. Wen, Z. Xie, Z. Wu, Y. Lin, W. 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*, 2024, **36**, 101871, doi: 10.1016/j.jksuci.2023.101871.

[8] J. wu, W. Feng, G. Liang, T. Wang, G. Li, Y. Zheng, A privacy protection scheme for facial recognition and resolution based on edge computing, *Security and Communication Networks*, 2022, **2022**, 4095427, doi: 10.1155/2022/4095427.

[9] P. K. Mishra, A. Iaboni, B. Ye, K. Newman, A. Mihailidis, S. S. Khan, Privacy-protecting behaviours of risk detection in people with dementia using videos, *Biomedical Engineering Online*, 2023, **22**, 4, doi: 10.1186/s12938-023-01065-3.

[10] R. Yang, Privacy and surveillance concerns in machine learning fall prediction models: implications for geriatric care and the Internet of medical things, *AI & Society*, 2024, **39**, 1969-1973, doi: 10.1007/s00146-023-01655-8.

[11] L. Du, W. Zhang, H. Fu, W. Ren, X. Zhang, An efficient privacy protection scheme for data security in video surveillance, *Journal of Visual Communication and Image Representation*, 2019, **59**, 347-362, doi: 10.1016/j.jvcir.2019.01.027.

[12] N. A. Tu, T. Huynh-The, K. Wong, M. F. Demirci, Y. K. Lee, Toward efficient and intelligent video analytics with visual privacy protection for large-scale surveillance, *The Journal of Supercomputing*, 2021, **77**, 14374-14404, doi: 10.1007/s11227-021-03865-7.

[13] E. Guo, P. Li, S. Yu, H. Wang, Efficient video privacy protection against malicious face recognition models, *IEEE Open Journal of the Computer Society*, 2022, **3**, 271-280, doi: 10.1109/OJCS.2022.3218559.

[14] K. M. Hosny, M. A. Zaki, H. M. Hamza, M. M. Fouda, N. A. Lashin, Privacy protection in surveillance videos using block scrambling-based encryption and DCNN-based face detection, *IEEE Access*, 2022, **10**, 106750-106769, doi: 10.1109/ACCESS.2022.3211657.

[15] X. Tian, P. Zheng, J. Huang, Robust privacy-preserving motion detection and object tracking in encrypted streaming video, *IEEE Transactions on Information Forensics and Security*, 2021, **16**, 5381-5396, doi: 10.1109/TIFS.2021.3128817.

[16] J. Liu, Y. Li, G. Han, N. Sun, Visual video evaluation association modeling based on chaotic pseudo-random multi-layer compressed sensing for visual privacy-protected keyframe extraction, *Journal of Visual Communication and Image Representation*, 2023, **90**, 103691, doi: 10.1016/j.jvcir.2022.103691.

[17] J. Liu, P. Dai, G. Han, N. Sun, Combined CNN/RNN video privacy protection evaluation method for monitoring home scene violence, *Computers and Electrical Engineering*, 2023, **106**, 108614, doi: 10.1016/j.compeleceng.2023.108614.

[18] K. Kansal, Y. Wong, M. Kankanhalli, Privacy-enhancing person re-identification framework - A dual-stage approach, 2024 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), January 3-8, Waikoloa, HI, USA, IEEE, 2024, 8543-8552, doi: 10.1109/wacv57701.2024.00835.

[19] Y. Lyu, Y. Jiang, Z. He, B. Peng, Y. Liu, J. Dong, 3D-Aware adversarial makeup generation for facial privacy protection, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023, **45**, 13438-13453, doi: 10.1109/tpami.2023.3290175.

[20] A. Fitwi, Y. Chen, S. Zhu, E. Blasch, G. Chen, Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking, *Electronics*, 2021, **10**, 236, doi: 10.3390/electronics10030236.

[21] Z. Xu, C. Hu, L. Mei, Video structured description technology based intelligence analysis of surveillance videos for public security applications, *Multimedia Tools and Applications*, 2016, **75**, 12155-12172, doi: 10.1007/s11042-015-3112-5.

[22] M. Feng, Retraction Note: Human motion image detection and tracking method based on Gaussian mixture model combined with light sensor, *Optical and Quantum Electronics*, 2024, **56**, 1583, doi: 10.1007/s11082-024-07564-4.

[23] S. Ge, B. Liu, P. Wang, Y. Li, D. Zeng, Learning privacy-preserving student networks *via* discriminative-generative distillation, *IEEE Transactions on Image Processing*, 2022, **32**, 116-127, doi: 10.1109/TIP.2022.3226416.

[24] T. Murakami, Y. Sei, Automatic tuning of privacy budgets in input-discriminative local differential privacy, *IEEE Internet of Things Journal*, 2023, **10**, 15990-16005, doi: 10.1109/JIOT.2023.3267082.

[25] Q. U. Ain, H. Al-Sahaf, B. Xue, M. Zhang, Generating knowledge-guided discriminative features using genetic programming for melanoma detection, *IEEE Transactions on*

Emerging Topics in Computational Intelligence, 2021, **5**, 554-569, doi: 10.1109/TETCI.2020.2983426.
[26] Y. Lei, W. Yuan, H. Wang, W. You, W. Bo, A skin segmentation algorithm based on stacked autoencoders, *IEEE Transactions on Multimedia*, 2017, **19**, 740-749, doi: 10.1109/TMM.2016.2638204.
[27] A. Lumini, L. Nanni, Fair comparison of skin detection approaches on publicly available datasets, *Expert Systems with Applications*, 2020, **160**, 113677, doi: 10.1016/j.eswa.2020.113677.
[28] M. Furka, M. Kalúz, M. Fikar, M. Klaučo, Guidelines for secure process control: harnessing the power of homomorphic encryption and state feedback control, *IEEE Access*, 2023, **11**, 110328-110341, doi: 10.1109/ACCESS.2023.3322035.
[29] Z. Montazeri, T. Niknam, J. Aghaei, O. P. Malik, M. Dehghani, G. Dhiman, Golf optimization algorithm: a new game-based metaheuristic algorithm and its application to energy commitment problem considering resilience, *Biomimetics*, 2023, **8**, 386, doi: 10.3390/biomimetics8050386.
[30] S. Chakraborty, A. Kumar Saha, S. Sharma, S. Mirjalili, R. Chakraborty, A novel enhanced whale optimization algorithm for global optimization, *Computers & Industrial Engineering*, 2021, **153**, 107086, doi: 10.1016/j.cie.2020.107086.
[31] T. Chabuanoi, N. Pannucharoenwong, P. Wongsangnoi, P. Rattanadecho, J. Saemathong, S. Hemathulin, Simulation effect of laser moving speed and spot size on maximum temperature in laser welding human skin tissue, *Engineered Science*, 2024, **31**, 1193, doi: 10.30919/es1193.
[32] C. Mulambia, S. Varshney, A. Suman, Privacy preserving blockchain based authentication scheme for vanet, *Engineered Science*, 2024, **28**, 1073 doi: 10.30919/es1073
[33] N. Goswami, S. Raj, D. Thakral, J. L. Arias-Gonzáles, J. Flores-Albornoz, E. Asnate-Salazar, D. Kapila, S. Yadav, S. Kumar, Intrusion detection system for IoT-based healthcare intrusions with lion-salp-swarm-optimization algorithm: metaheuristic-enabled hybrid intelligent approach, *Engineered Science*, 2024, **31**, 1193 doi: 10.30919/es933
[34] R. K. Enneti, Synthesis of nanocrystalline tungsten and tungsten carbide powders in a single step *via* thermal plasma technique, *International Journal of Refractory Metals and Hard Materials*, 2015, **53**, 111-116, doi: 10.1016/j.ijrmhm.2015.06.011.