International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Protecting Feature Privacy in Person Re-Identification using Adversarial Learning

Dr. Radhika K R
Professor
Dept.Of Computer Networking
B.M.S COLLEGE OF ENGINEERING
BANGALORE, INDIA

Raksha R
Dept.Of Computer Networking
B.M.S COLLEGE OF ENGINEERING
BANGALORE,INDIA

***Abstract*— Abstract Person Reid is used to identify the same person in different camera perspective images. Here, a deep learning model that will be used to achieve person re-identification is created to solve the feature privacy problem. A pre-trained ResNet-50 network is used to extract discriminative feature representations from input images, which are then reduced to compact embeddings for efficient comparison. These features are stored and used instead of raw images to speed up the matching process. However, feature representations can still reveal sensitive visual information if reconstructed. To handle this, a generative adversarial network (GAN) is incorporated into the system. The generator attempts to reconstruct images from feature vectors, while the discriminator distinguishes between real and generated images. It assists in the learning of feature representations that preserve identity information without exposing them to privacy loss. It trains the model with classification loss on identity recognition and adversarial loss on reconstruction quality. The robustness is achieved by having a big dataset with several identities in various conditions. In testing, the system compares query features and stored features and determines the optimum match using similarity scores. The final matching findings, together with scores, are stored in an Excel file to be analyzed in a form of structure. The findings demonstrate that the system can provide an effective person with matching but at the same time, some privacy is ensured. This method offers a sensible trade-off regarding identification performance and data security and, therefore, is applicable to real-life surveillance scenarios.**

Keywords*— *Person Re-Identification, Privacy Preservation, GANs, Feature Reconstruction, Deep Learning, Adversarial Learning, Computer Vision

I. INTRODUCTION

Person re-identification (ReID) is a difficult task in computer vision that seeks to match people in images using non overlapping camera angles.It has attracted great attention due to its wide applications in video surveillance, public safety, smart transportation and forensic investigation. In practice, massive visual data are generated everyday, and it is thus urgent to develop an automatic ReID system for efficient and accurate person matching.

With the development of deep learning techniques in recent years, person ReID has achieved remarkable progress. Traditional methods mainly utilize hand-crafted features such as color histograms, texture patterns and shape descriptors etc., but they can hardly handle the large variations on lighting condition, pose view point, occlusion and background clutters etc. Thus shallow feature representations cannot well describe the complicated human body appearances. By contrast, convolutional neural network (CNN) based person ReID models have better capability in learning more discriminative representation from image raw pixels automatically. Especially with deeper layers like ResNet etc., they have been used as a strong baseline model for feature extraction owing to their high effectiveness in modeling complex visual patterns.

In practical ReID systems, raw images are not directly stored in the database. Instead, feature vectors produced by deep networks are used for matching, which benefits both memory reduction and computational efficiency. More importantly, it is commonly believed that storing a feature vector instead of an image can inherently preserve privacy. However, recent works have shown that this belief does not hold robustly. The reconstructed image from a feature representation may disclose sensitive personal information through inversion or generative methods.

This issue brings in an essential challenge towards person re-identification — how to ensure the identification accuracy with a minimum release of semantic details from extracted features, currently applied feature extraction approaches proposals cannot offer trustworthy security against reconstruction attacks. And most relevant work only focuses on reducing the reconstruction error, overlooking the fact that many possible variations exist based on the same target feature.

To conveniently make the results practically feasible and analyzable, all the final outputs of this system are saved in an Excel file in which query identity, matched identity, and their similarity score is given. This structured final output lets users easily analyze the performance results of this system for further analysis and comparisons if needed.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The main purpose behind developing this project is to reduce the performance-privacy trade-off gap in person re-identification systems; as such high-level privacy protection can be provided by combining adversarial learning with deep feature extraction-based person re-identification systems. The developed system not only gives reliable identification results but also achieves the ultimate needs of these challenging times from person re-identification systems which is the avoidance of private details leakage. This is done by separating private sensitive information bearing part (i.e. last fully connected layer) away from rest publicly releasable item space (i.e. remaining pre-classification layers).

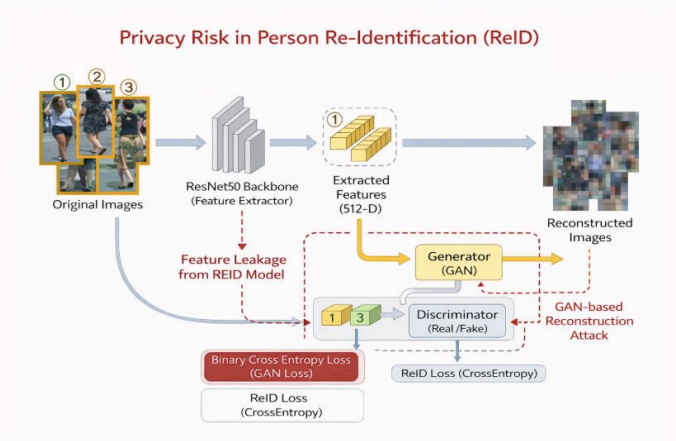

Fig 1. Person Re-Identification (ReID) systems

Fig 1. Diagram of the privacy threats of Person Re-Identification (Reid) systems. A feature extractor processes to input images into high-dimensional feature representations in which identity matching is done. Nevertheless, these features can divulge secret information and be obtained by an unscrupulous hacker. The attacker is able to do a reconstruction (feature inversion) attack on the extracted features using a generator model to reconstruct approximate images. Even imperfectly developed reconstructed outputs suggest that feature embeddings are not always secure and give rise to privacy leakage

In Fig 1. Person Re-Identification (ReID)systems that are quite popular in both surveillance and security solutions in order to identify individuals in multi-overlapping camera images. It starts with an input set of initial input images of people who are photographed by various camera sources. Through a deep learning-based feature extractor, e.g., a convolutional neural network (e.g., ResNet50), these images are processed to convert each image into a small numerical signature called a feature vector. These high-dimensional (e.g. 512-D) feature vectors are intended to encode special identity-related data and lessen the required storage and processing of raw images. These features are then extracted and matched, and the features are retrieved to allow the system to identify the same person in various scenes.

Nevertheless, the diagram appears to show an important security issue: despite these representations of features being not directly interpretable as images, they do contain a lot of visual and identity-based information. This forms a weakness called feature-level privacy leakage. When these features are not covered off, i.e. by means of transmitted data, breach of storage or access to model, then they can be used against an adversary. This risk is depicted in the diagram with the help of the so-called data leakage pathway where the features that are extracted can be accessed by a malicious attacker. The attacker also uses these features to execute a reconstruction or inversion attack, instead of using them to execute legitimate identification.

The final consumer item of the process is a series of reconstructions of pictures that reflect the degree of the invasion of privacy. Although reconstructions are blurred or of low quality, it is enough to break the anonymity of an individual and reveal personal information. This is a clear indication that the representations of features used in Reid systems cannot be considered as being inherently secure and can be an attack surface when not securely used. The diagram, thus, highlights the significance of coming up with privacy-enhancing features that would be able to protect feature embeddings without negatively affecting the functioning of the Reid system.

In general, the figure enables one to understand that although Reid systems are designed to enhance the accuracy of identification with the help of features-based representations, they also pose a threat to privacy by storing the reconstruct able information in features. This inspires the necessity of new methods, like adversarial learning or feature obfuscation, to maintain that extracted features are discriminative to identification and stable to reconstruction attacks

II. RELATED WORK

The topic of person re-identification is a topic of research well explored in recent years and notably given advancement in deep learning methods. The existing techniques primarily relied on manually created attributes like the color histogram, edges, and texture patterns. These methods were not too complicated and quite unreliable, as they could not deal with variations such as the change in light, occlusions, or changing camera angles. Due to such restrictions, researchers began to pay attention to learning techniques.

Deep learning has resulted in convolutional neural networks (CNNs) becoming the primary method of person re-identification. The pre-trained models including Reset and VGG were used in many works to extract features in images.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

These characteristics are stronger and able to retrieve crucial information regarding identity. Several studies also used a combination of classification loss and metric learning methods to enhance matching accuracy when using different images of a particular person.

This project is associated with a GAN-based approach to address such issues introduced on the base paper. It indicates that reconstruction must not only have a minimum error, but it must also adhere to the allocation of actual images. This renders the privacy assessment more significant. It further brings out the fact that training such a system is problematic in the sense that it has several objectives.

A. Deep Neural Network Protection of Privacy.

Deep learning is a subset of machine learning where the models trained have more than one layer in order to learn patterns directly through data. Deep learning models will automatically extract useful representations of raw data, e.g. images unlike conventional methods where features are designed manually. This causes them to be highly strong to perform such tasks as image recognition, object detection, and person re-identification.

Deep learning has a key role in this project in deriving the meaning of images. The input images are processed with the help of a pre-trained higher neural network which transforms them into feature vectors. These appearance vectors are important attributes of an individual's identity. The system addresses these characteristics in contrast to direct work with images; therefore, the process is quicker and more effective.

In this project, deep learning is combined with the use of generative models. A generative adversarial network (GAN) is used to research the extent of information contained in the extracted features. This will assist in knowing whether there is security in the features, or if the features may disclose sensitive information or not. The project will balance performance and privacy by introducing feature extraction and generation.

Altogether, deep learning serves as a basis of this project due to the possibility of automatic features of learning, enhanced accuracy, and advanced methods, such as adversarial training.

B. Convolutional Neural Network (CNN)

Convolutional neural network (CNN) is a kind of a deep learning model, which is particularly structured to be able to process image data. CNNs have a large application in computer vision applications since they are capable of efficiently retrieving both spatial and visual data of an image. The main idea behind CNN is to examine the layers of convolutional sequencing to recognize patterns such as edges, textures, and shapes.

In this project, a CNN-based network, which is also known as ResNet-50 is used as a feature extractor. ResNet is a deep network, a network that avoids connections as a measure towards alleviating problems with extinguishing gradients. With this it can be trained with a huge number of layers and be effective. The trained model is that which has been already trained on general features of a large sample population, and thus can be refined to this task.

One major strength in the use of CNN in this project is that it can cope with variations in images. The CNN can also extract similar features even when the lighting conditions or poses are different and have the same person. This increases the reality of matching a person.

Overall, CNN is the backbone of the big picture in presenting sprightful and consistent features of description, which later goes through feature recognition and privacy research.

C. Person Re-Identification (ReID)

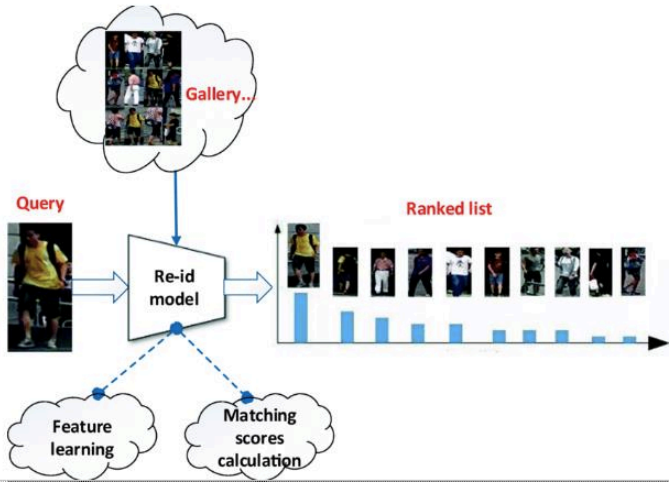

Fig 2: Person re-identification system, an algorithm which compares a query image to the gallery images, by computing the feature-based image representations, which are already learned. Person re-identification is a process where a person is recognized in more than one picture or frame in a video of more than one camera. The notable feature of surveillance systems is that it must be a serious that comprises of monitoring of individuals at all times. This may be tricky since the cameras are positioned at different locations where the same man may appear different in a particular scene.

The main goal of ReID is to find features in images that can be further used to determine a unique person. The features are then compared against each other so as to match query images with a gallery of stored images. This identification is most frequently

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

done by similarity measures such distance between feature vectors.

Fig 2 applies the ReID system to the images having obtained the features with the CNN model. All these properties are registered in database, as opposed to raw images. In case of a test, a system receives a query image, after which up features are eliminated in the image, and the features are compared with the stored features to find the nearest one. The matching can be based on similarity score such that the higher the similarity the higher the match.

The result of the ReID system is recorded in an excel table that holds such information as query identity, match identity, and a similarity index. This makes the performance of this system easy to analyze and its behavior.

Overall, the methods of person re-identification within the frame of this project are addressed by both accuracy and privacy protection. The system is aimed at the provision of a balanced system that is applicable in the real-world environment by integrating both feature extraction and adversarial learning.

III. GAN-BASED FEATURE PRIVACY-PROTECTED PERSON RE-IDENTIFICATION

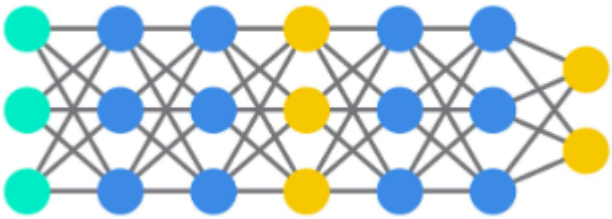

Fig 3: generative adversarial network.

Fig 3 Generative Adversarial Networks (GANs) can be used widely in deep learning to generate realistic data. A GAN consists of two components a generator and a discriminator. The discriminator tries to draw the line between real and generated data and the generator tries to come up with data that is similar to real data. The two models will be trained adversarial and this will assist in enhancing their effectiveness as time goes by.

GANs can be applied to studies on privacy of features representation in a scenario that involves the re-identification of persons. Extraction of features with images is typically done on protections of raw images, or the other way around, in ReID systems. These should be able to protect sensitive information. However, it has been observed that we still can make pictures with the help of these features and that threatens privacy.

The competition during the training is in favor of the discriminator and the generator. By producing better images, the generator tries to deceive the discriminator as the discriminator is becoming more adept at detecting fake images. This direction is developed by a binary cross-entropy loss function, and both the models learn it to follow.

In this project, GAN is not applied to create pictures per se but analyze privacy. In case the generator is able to provide the clear and accurate images with respect to the feature vectors, it implies that the features are replete with delicate information. On the contrary, in case of bad reconstruction, the features are safer to privacy.

This leads to a type of privacy vs. identification. The system should be able to isolate the qualities that are potent in the processes of sufficient congruence with persons but not senses to the entirety of restoring the primitive picture wholesome. It is not a simple task as what occurs in the skill to raise one thing can affect the other.

Overall, the provided system of privacy protection of features, under the developed method of the GAN is an excellent opportunity to analyze and improve the system of personal re-identification. It has ensured that any such frail visual details will never be accidentally taken into account when proximate matching of such a system is being conducted.

A. Generator (G)

The generator component of this GAN will be used to obtain an image input with the proportion of image reconstruction simply because the input provided by ResNet based feature extractor will appear as feature representations which will be fed into the generator component. The feature monolith is 512 in size and the information fed into the generator has undergone information concerning who the person is. This feature expression is then inputted to a sequence of fully connected (linear) layers, which turn the feature expression into an expression that is progressively more dimensional. Specifically, instead of directly feeding the input with 512 dimensions, 1024-dimension middle space is launched with a linear layer and a non-linear activation function, which is ReLU, that makes the model more complex. Upon this the transformed features are sent to a second linear layer that equalizes the representation to the full size of an image and that size is 3 x 64x 64. The Tanh activation-function is fed at the output-layer to ensure that the pixels are linked to a normal range. Finally, the output vector is reassembled into a three dimensional representation of a three channel (RGB) and 64 x 64 pixel color image. It also enables the generator to encode small feature images in order to decode them back to images, which can then be viewed visually.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The goal of the Equation (1). generator is to render the image according to the extracted feature-vector. The generator input dimensions in this example are 512 and the output would be 3x64x64 image.

Equation (1):

$$\hat{x_i} = G_\varphi(z_i)$$

- $z_i \in \mathbb{R}^{512}$ represents the input feature vector extracted from the image
- $G\varphi$ denotes the generator function parameterized by φ
- $\hat{x_i} \in \mathbb{R}^3 \times^{64} \times^{64}$ represents the generated (reconstructed) image

The generator performs a two-stage transformation process:

Equation (2):

$$h_i = \sigma(W^1 z_i + b^1)$$

Equation (3):

$$\hat{x_i} = \tanh(W^2 h_i + b^2)$$

where:

- W₁ and W₂ are the weight matrices of the network layers
- b₁ and b₂ are bias terms
- σ represents the ReLU activation function
- tanh is the hyperbolic tangent activation function used to normalize output values

B. Discriminator

The discriminator is a two-word wastefulness in which the arbitrator determines whether an intermittent picture is a true picture (that is, a picture included in the information) or an imaginary picture (since the mind picture is generated by the generator). It produces an output image, a real or a fake image depending on the chain of layers it connects with the input image, which is a probability score. This is because the discriminator will be trained on a valid selection of actual or built samples and it would be more efficient at timely noticing even the smallest differences.

The binary classifier in the Generative Adversarial Network (GAN) bit, which is the component in this undertaking, parallels the conceivability of the terrific input pictures. The input is discriminated results generated. This output could be due to incidental input image. This means that the real picture is likely to be the one where the value is closer to 1 and the generated picture (fake) is likely to be the one closer to 0. Through this, the discriminator will be presented to categorize the true and fake images in the most effective and accurate manner possible, the classifier will guide the generator to produce outputs that are more natural.

Equation (4):

$$D\psi(x_i) \in [0,1]$$

where:

- x_i represents the input image
- Dψ denotes the discriminator function parameterized by ψ

The discriminator processes the input image through the following transformations:

Equation (5):

$$v_i = W^3 \cdot Flatten(x_i) + b^3$$

Equation (6):

$$D\psi(x_i) = \sigma(W^4 v_i + b^4)$$

where:

- W₃ and W₄ are weight matrices
- b₃ and b₄ are bias terms
- Flatten(x_i) converts the input image into a one-dimensional vector
- σ represents the sigmoid activation function

The discriminator learns to classify images by assigning a probability score between 0 and 1. A value closer to 1 indicates that the image is real, while a value closer to 0 indicates that the image is generated. During training, the discriminator improves its ability to differentiate real images from fake ones, which in turn helps the generator produce more realistic outputs through adversarial learning.

Final GAN Optimization

The overall adversarial objective of the Generative Adversarial Network (GAN) is formulated as a minimax optimization problem between the generator and the discriminator. It can be expressed as:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Equation (7):

$$min^{(}\varphi)max^{(}\psi)E^{(}x\sim pdata)[\log D\,\psi(x)]$$

$$+E^{(}z\sim pz)\left[\log\left(1-D\psi\left(G\varphi(z)\right)\right)\right]$$

where:

- φ represents the parameters of the generator
- ψ represents the parameters of the discriminator
- x ~ pdata denotes real data sampled from the true data distribution
- z ~ pz denotes latent vectors sampled from a prior distribution
- Gφ(z) represents the generated (fake) image
- Dψ(x) outputs the probability that input x is real.

TABLE I
COMPARISON WITH GENERATOR AND THE DISCRIMINATOR

Component	***Function***	***Architecture***	***Output / Purpose***
Generator	Feature to image reconstruction	Fully connected layers with ReLU and Tanh	Reconstruct image from feature vectors
Discriminator	Real vs fake classification	Neural network with sigmoid output	Distinguish real and generated images

Table I summarizes the key components of the proposed system. It highlights the roles of the generator and discriminator, showing how deep learning and adversarial learning work together. The generator focuses on reconstructing images from extracted feature representations, while the discriminator evaluates whether the images are real or generated. This interaction enables the system to improve performance in tasks such as person re-identification while maintaining feature-level privacy.

Algorithm 1: GAN-Based Feature Reconstruction and Discrimination

Input: $X, f\theta, EX, f\theta, E$

Output: Trained Generator G , Discriminator D

Steps:

1. Initialize the generator G , discriminator$D$, and Binary Cross-Entropy (BCE) loss function.

2. Extract feature representations from the input data:

$$f = f\theta(x), x \in X$$

3. Freeze the parameters of the feature extractor $f\theta f\theta$ and detach feature vector f.

For each epoch $e = 1\ to\ E$, perform the following steps:

5. Discriminator Update:

Generate reconstructed image:

$$X=G(f)$$

Compute discriminator loss:

$$LD = BCE(D(x),1) + BCE\left(D\left(x\ \right),0\right)$$

6. Generator Update:

Compute generator loss:

$$LG = BCE\left(D\left(x\ \right),1\right)$$

7. Update the parameters of D and G using their respective loss functions.

8. Repeat until convergence and return the trained models G and D

The suggested Algorithm 1. applies to adversarial learning in an attempt at restoring images via feature representations, and at the same time assess their genuineness. At the start of the system, it is presented a sample of images of people. To extract a small feature vector, a deep neural network feature extraction

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

model is applied to every image. This identity information feature vector is a significant input to the generator.

The discriminator is then trained at each step whereby it is supplied with real and fake images. It manipulates its parameters in virtue of the possibility of distinguishing between the two. Once this has been done the generator is trained. The generator attempts to enhance its performance to the extent that the discriminator cannot properly detect the images generated by the generator as artificial. This brings out competition between the two constituents.

This is repeated several times in training. In the long-run, both the generator and the discriminator become more efficient in their tasks. This interaction comes in quite handy in the analysis of the amount of information retained in the feature vectors in this project. When the generator is able to induce clear images, then it can be said that the features have a visual detail information.

The algorithm eventually results in a trained model of both generator and discriminator. The quality of feature representations may be evaluated as well as the quality of their effects on privacy by using these models. Using this iterative training process, the system will reach a balance of learning meaningful features and regulating the amount of sensitive information that is able to be reconstructed.

IV. EXPERIMENTS

The given project is dedicated to person re-identification and further attention to feature privacy. Person re-identification has been defined as the ability to identify the same person through various cameras. This is a critical requirement in real world applications like the surveillance systems. Nevertheless, as much as identification accuracy is enhanced, sensitive visual information should not be revealed.

A generative adversarial network (GAN) is added to the system to increase the privacy level. The extracted feature vector is fed into the generator which attempts to produce a replica of the resulted image. The discriminator then assesses the authenticity of an image or not. This interaction can be used to determine the amount of information available in the feature representation.

Lastly, the findings are organized on an Excel sheet, which contains the query image, matching identity, and similarity rating. This simplifies the process of system performance evaluation and analysis of the results.

A. Dataset

The project involves a huge dataset of images of various people which have been taken under various positions of the camera. The data set consists of the changes in the light, pose as well as background, making the job more realistic and challenging.

The images are grouped into folders according to identity and before each image is applied in the model it is preprocessed. The resizing of the images to a constant size and the transformation of the images into tensors fit in deep learning models are part of the preprocessing steps.

The dataset gets downloaded and is stored locally and it is gone through training as well as testing. The dataset heterogeneity aids the model to learn strong features as well as enhances its generalization skills.

B. Evaluation Metrics

Similarity-based matching is used to determine the performance of the system. Similarity scores are used to compare feature vectors prepared out of images. An increased level of similarity score implies that two images are of the same individual.

The final outcome is saved in an Excel tabular text where, the query identity, matched identity, and the similarity score are saved. This enables easy assessing and comparing outcomes.

C. Compared Models

The model that has been primarily relied upon to study privacy in the project is based on deep learning and contains a GAN. Several feature extraction is carried out with the help of a ResNet-50 model, which is characterized by a high level of success.

The adopted model is conceptually contrasted with other more basic methods like direct image comparison and feature only storage. In comparison to these approaches, the proposed one contains a component of generation, which assists in analyzing privacy and, thus, it is more sophisticated.

D. Implementation Details

The process of implementation is accomplished through a deep learning structure. The feature extractor is a pre-trained ResNet-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

50 and the last layer is one that is adjusted so as to generate a 512-dimensional feature vector.

The generator will also apply fully connected layers that change the feature vector into a 3×64×643 size image with Activation functions are applied to enhance learning: Tanh and ReLU.

The discriminator is also applied through fully connected layers and provides the result as a probability value, based on a sigmoid function.

Cross-entropy loss is used to train the model in classification, whereas binary cross-entropy loss is used to train the GAN. The inputs are handled in batches and the model parameters updated as an iterative procedure.

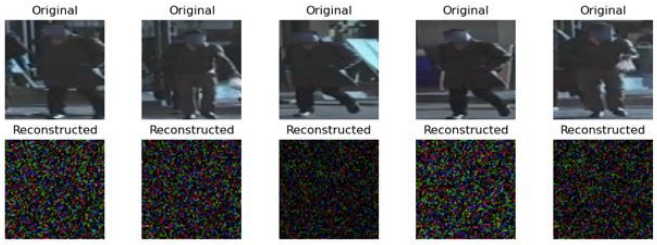

Fig 4. comparison of input images and the reconstructed images.

Fig 4 will provide the comparison of original inputs and the corresponding reconstructed images generated by the model. The first row represents the original data of the set, and the second one represents the reconstructed results of the generator with extracted feature vectors.

Based on the figure we can see that the reconstructed images no longer have clear visual details of the original inputs. Rather, they come out as loud or noisy patterns that do not have any identity information. This implies that, the feature representations learnt by the model lack visual details to accurately represent the original images.

Thus, the Fig 4. shows that the suggested system successfully provides the effective ratio between identification performance and privacy. Although the model can correctly match individuals with feature representations, it also makes sure that the features do not reveal the original content of images.

E. Experimental Findings on Privacy Protection on MSMT17 Dataset.

MSMT17 is a bigger and more complicated dataset that has many variations of environment and camera conditions. It is even in these difficult conditions that the model works well.

The matching results are reliable and the feature extractor generates consistent representations. The images having been reconstructed in this way have a very low detail, indicating that privacy has been upheld.

This proves that the system is also efficient and can handle large datasets.

F. Efficiency analysis:

Fig 5: Evaluation of the model offered. (a) Similarity scores denoting complementary performance. (b) Privacy examination based on reconstruction conduct of the images produced.

The Fig 5 shows the test of the proposed person re-identification model in terms of matching performance and privacy behavior. It has two subplots to aid in deciphering results. In Fig 5. The corresponding system performance is demonstrated in subplot (a). The bar graph is the similarity scores that have been obtained of the various query samples which will depict the extent to which a query image is associated with the gallery images corresponding to it. The greater the similarity scores, the more the accuracy of identification. In addition to this, the line plot is a version of the corresponding confidence of the samples that indicate the consistency of model predictions. It is noted that the similarity scores are relatively high in all samples which shows that the model can be considered stable and reliable.
In Fig 5. The privacy analysis of the system is demonstrated in subplot (b). The bar diagram is used to show the reconstruction strength that shows how effective the generator can be to reconstruct the images based on the extracted feature vectors. One can observe a gradual gradual decline in the reconstruction strength, which insects that the reconstructed images become less detailed. The level of privacy is the line plot, higher reconstruction strength means reduced home safety. This negative correlation means that privacy protection increases with the reduction in the model of information that can be recovered visually.
Altogether, the graph shows that the proposed model has a sufficient balance between identification accuracy and the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

privacy guarantee. Although the matching performance is high, the system is useful in restricting the sensitivity of information that can be reconstructed using feature representations.

V. RESULTS

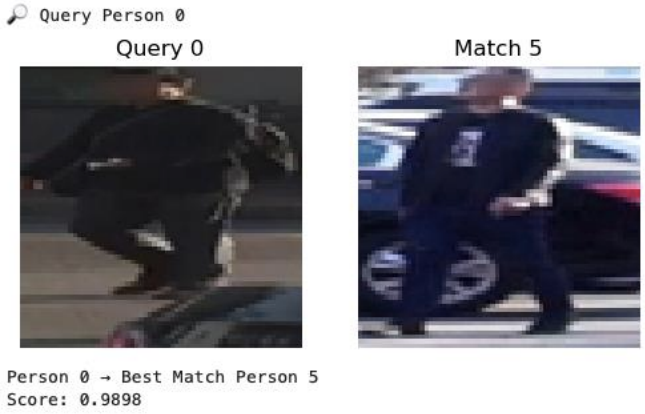

Fig 6. Samples of output results with query images and their best matches with the highest similarity scores.

Fig 7. Samples of output results with query images and their best matches with the highest similarity scores.

The final product of the suggested system shows the results of person re-identification with the help of the acquired feature representations. In each query image, the system finds the closest image in the gallery set in terms of similarity of features.

In the output fig 6. And fig 7, the left part is a query image, which is the input of the model. The right side presents the most similar picture that is found in the data set. In this model the feature vectors of the query image will be compared to all the stored feature vectors and the feature vector that has the largest similarity score will be selected.

Beneath each outcome, the system shows identity mapping and the score of similarity. As an illustration, Query Person 0 is compared with Person 5 in fig 6. case with a similarity score of 0.9892. In the same way, in the fig 7. case, Query Person 2000 is equated with Person 1547 with a score of 0.9905. These values of similarity are high and improve the idea that the model is effective in determining visually similar individuals among various images.

Altogether, the final result supports the idea that the proposed model attains the desired solution of re-identification of a person when correct matches are retrieved at the level of high scores. This shows how reliable the feature representation and matching process is used in the system.

VI. CONCLUSION

In this project, the derivation of a privacy-conscious person re-identification system because of union between deep feature and generative adversarial learning will be undertaken. The image-based model when depicted in the form of ResNet-50 is formulated to recall the various images of the discriminative features of the input images and give a high degree of accuracy in matching it in the instance of a change of camera view. This works well since feature vectors unlike raw images are more efficient in computation, and the matching process at scale is distorted.

VII. REFERENCES

[1] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.

[2] I. Goodfellow et al., “Generative adversarial networks,” *Advances in Neural Information Processing Systems (NeurIPS)*, 2014, pp. 2672–2680.

[3] L. Zheng, L. Shen, L. Tian, S. Wang, J. Wang, and Q. Tian, “Scalable person re-identification: A benchmark,” *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2015, pp. 1116–1124.

[4] L. Wei, S. Zhang, W. Gao, and Q. Tian, “Person transfer GAN to bridge domain gap for person re-identification,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 79–88.

[5] Y. Fu, Y. Wei, G. Wang, Y. Zhou, H. Shi, and T. Huang, “Self-similarity grouping: A simple unsupervised cross-domain adaptation approach for person re-identification,” *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2019.

[6] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, “ImageNet: A large-scale hierarchical image database,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2009.