Masking Identification Information On Visual Surveillance Systems By Granting Access Permission

Telugu Maddileti , Y. Rasagna

Abstract: Video surveillance systems (VSS), are used to gather the information about a crime, to check, prevent the crimes or investigate the crime that have already taken place. Surveillance is defined as performing observations of a group or an individual The most common techniques for surveillance is to store the concerned information. The stored visual footage is then recovered to its normal state by the authorized users. This paper proposes a mechanism of masking where infiltration of privacy on videos is minimized. This paper aims for the security or ensuring the privacy of a particular moving person or an object and provides the access to a limited extent only.

Index Terms:Surveillance, investigate, observations, techniques, Video system, masking, infiltration

1. INTRODUCTION

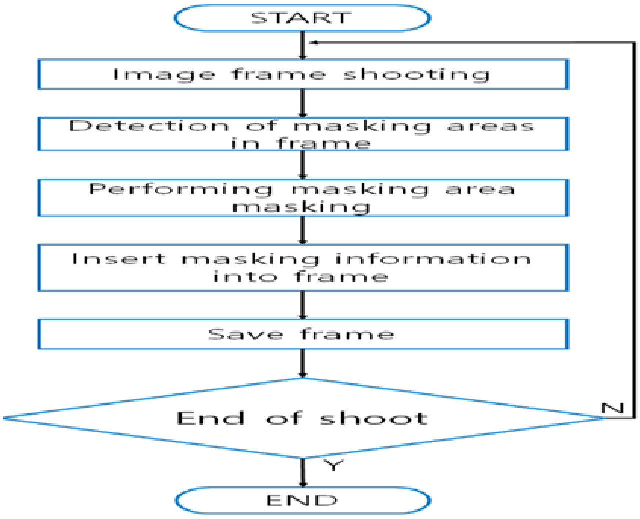
It is very important to have a secured, safe and a protected city with no compromise. Surveillance through video analytics is unavoidable in crowded areas and sensitive areas which are considered to be public the public places. It might be a shopping complex, an airport or schools and colleges you always need a monitoring system. So, the main challenge is to ensure the privacy while monitoring the places. The collected or recorded data is sent to the CCTV control department which is supposed to supervise the appropriate device with certain access rights. Video surveillance systems (VSS) are installed in crowded areas (private buildings/organizations) to monitor and acquire any secret information to increase the public protection thereby preventing any violent crimes such as kidnapping, robbery etc. The recorded visuals can be accessed by the administrators only where there is a chance of leakage of the personal identification information. Privacy masking of videos and images are decrypted and are not differential. The recorded visuals can be accessed by the administrators only where there is a chance of leakage of the personal identification information. Privacy masking of videos and images are decrypted and are not differentialTo ensure the privacy only some amount or only limited amount of the recorded visuals should be left for the users to access. In this study this is the proposed mechanism of masking.

2 MASKING TECHNIQUES

CCTVs are greatly in use these days. It has become the most important element in any organization, industry etc. But the major disadvantage is lack of privacy. It usually records everything by default. So there should be some specific device which captures or records certain unusual happenings eliminating the normal ones thus increasing the efficiency, privacy and reliability.

2.1 PRIVACY MASKING DEVICE

Here the visual images are captured as frames. Now masking of the one of the visual information is taken place in each frame, now after masking the information which is masked is stored in the frame as cluster.


START
Image frame shooting
Detection of masking areas in frame
Performing masking area masking
Insert masking information into frame
Save frame
End of shoot
N
Y
END

Masking device has
1. Filming module
2. Storage module

2.1. *Flow Chart of Privacy Masking Device*

In Filming module, masking of each frame is done and Storage module stores the masked information or images.

2.2 IMPLEMENTATION RESULTS

- *Telugu Maddileti, Assistant Professor, ECM Department, Sreenidhi Institute of Science and Technology, Ghatekesar, Telangana-501301.*
  E-mail:madhu14283@gmail.com.
- *.Yarlagadda Rasagna, ECM Department, Sreenidhi Institute of Science and Technology, Ghatekesar, Telangana-501301. E-mail:Rasagna.y@gmail.com*

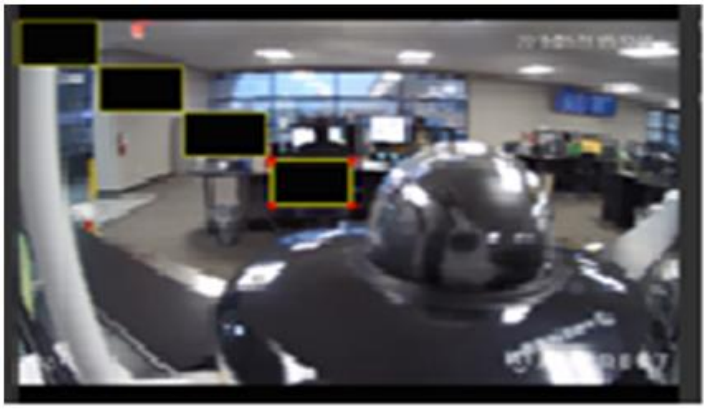


Fig 2.2 *Privacy Masking Device*

2.3FACEDETECTIONENABLEDPRIVACYPROTECTION TECHNIQUES

Here the main aim is to mask the faces of moving human for privacy protection. This equipment consists of
Server: It stores series of the video images.
Extraction of the frames in a sequence

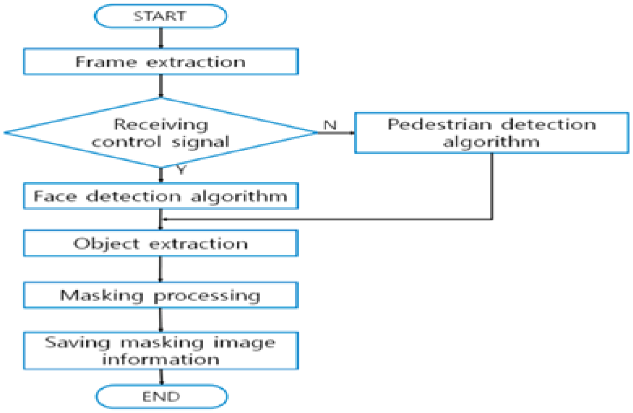


Fig: 2.3 *Privacy Protection Technique-Face Detection*

Extraction of the Object: Here it masks the faces that are in the frame. These techniques automatically detect pedestrians in a certain distance and also face in shorter distance.
Masking module: Provides authentication keys for accessing the masked visual information

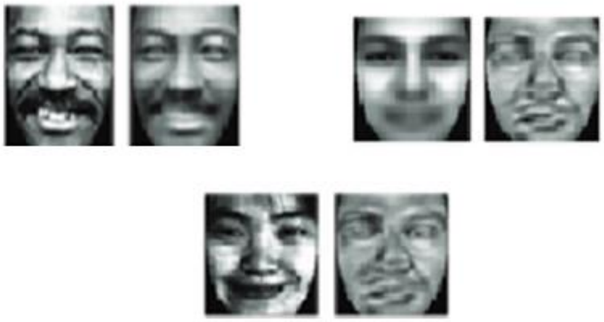


Fig. 2.3 *Comparison of original and reconstructed images*

IMPLEMENTATION RESULTS OF THE PRIVACY PROTECTION TECHNIQUE-FACE DETECTION

2.3 VIDEO MANIPULATION METHOD DEVICES

VSS is the device that helps in privacy protection usually prevents infiltration. In case of law enforcement agencies the process of masking is done through a receiver of control signals. The operational status is compared with the regulatory data of the cameras and check if they match or not.

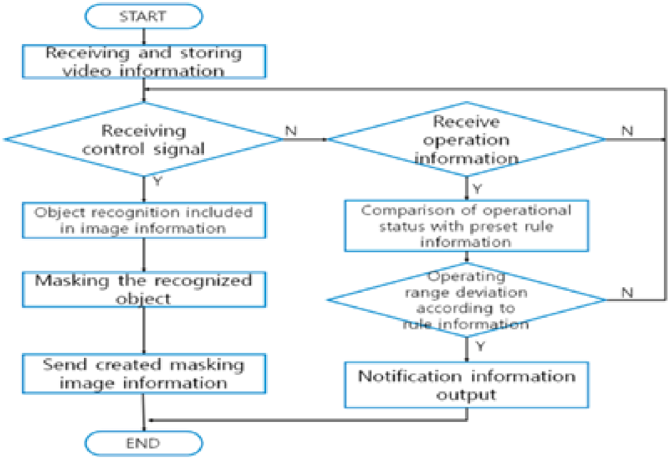

START
Receiving and storing video information
Receiving control signal
N
Receive operation information
N
Y
Y
Object recognition included in image information
Comparison of operational status with preset rule information
Masking the recognized object
Operating range deviation according to rule information
N
Y
Send created masking image information
Notification information output
END

Fig 2.5 *Flow Chart of Video Manipulation Techniques*

If the matching is not done, the output will be a match failure. It comprises of 3 modules
Storage module: The video images are stored here.
Interface module: It takes the input from the user as a signal.
Image processing module: Highly susceptible portions of the video are masked.
The masked images are sent outside through a control unit.

Implementation results of the Video Manipulation Techniques

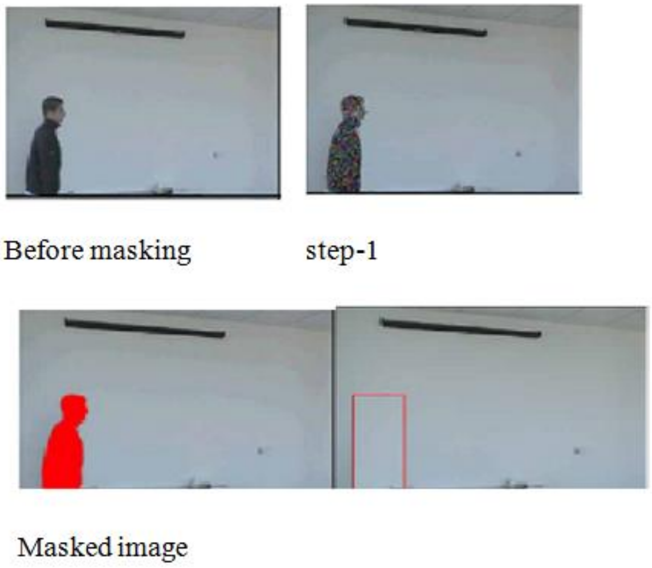


Fig 2.6 *Video Manipulation results*

3. PROPOSED MECHANISM OF MASKING THAT MINIMIZES ACCESSIBLE INFORMATION

This proposed system can be used in various applications like New and media, security monitoring and evidence management.

3.1 MOTION DETECTION

Here new entering frame is taken and passed to the background modeling for the purpose of differentiating the pixels. Once these pixels are recognized, they are passed through a 4 way and it clusters these pixels into blobs. If these are small then they are considered as noise and ignored. They pass through blob merging filter. Sometimes it is often that an object breaking into multiple blobs for various reasons likes noise, frame rate jitter. A filter merges these broken blobs have been implemented which lie along the Y-axis and on the X-axis projection of blob is examined overlapped projections of blobs are merged into single blob.

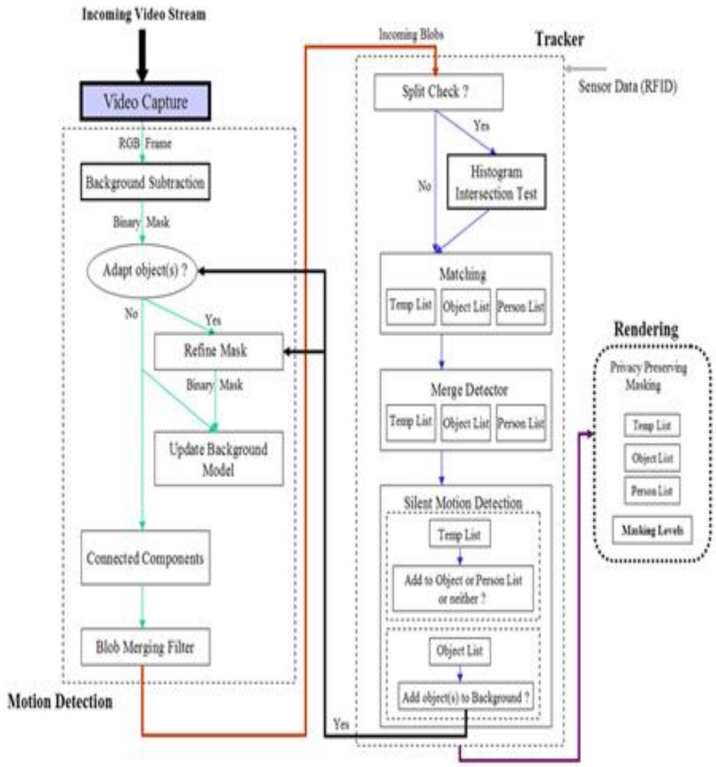


Fig 3.1 *Proposed Architecture*

TRACKING

The tracker has 3 lists:

1. The Temporary list
2. The person and object list
3. Updating list

The recently entered subjects are holded by the temporary list. The deposited objects are stored by the object list. The persons entered are stored by the persons list.
These are the parameters in each entry list
1) Pixel range of X and Y in order to know the bounding around a certain blob.
2) The occupancy of a blob
3) The COG (Center of Gravity) of the blob
4) Blob's RGB pixel values
5) The past information of the blob.
6) Previous blob information.

To check the Center of Gravity of the incoming blobs:

```
bool Tracker :: doesInBlobMatchPerson(CBlobinBlob,
Person inPerson)
{
if(((inPerson.info.cog.y<=inBlob.ymax)&&
(inPerson.info.cog.y>=inBlob.ymin))
&&((inPerson.info.cog.x<=inBlob.xmax)&&
(inPerson.info.cog.x>=inBlob.xmin)))  return true;
else return false;
```

The tracker matches the newly entering blobs and entries in the list for each frame. This match is made by testing the bounding box of the blob wraps the COG of candidate blob. In case of matching, the information is stored and the updated by the incoming blob. If it doesn't match it is just left from the list. The blob is thus placed to the list that is temporary. Based on merge detector the entries are flagged as merged.

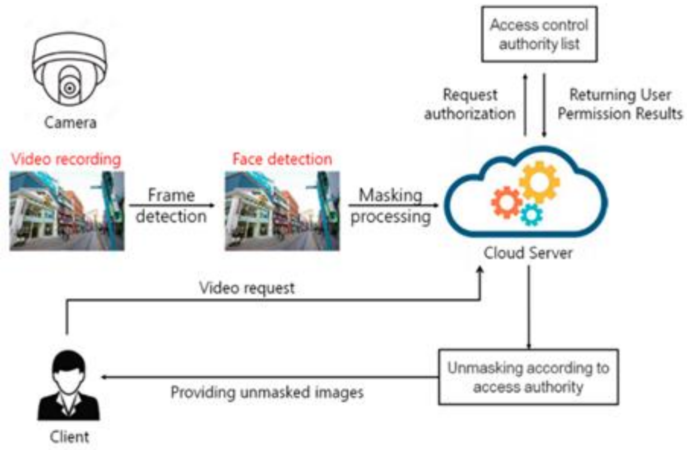
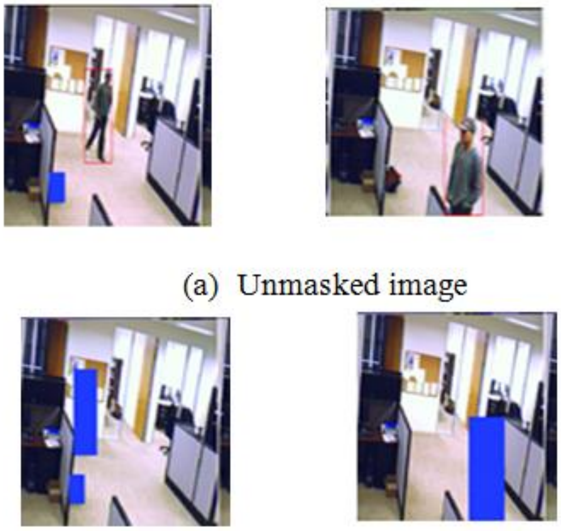

Camera
Access control authority list
Request authorization
Returning User Permission Results
Video recording
Frame detection
Face detection
Masking processing
Cloud Server
Video request
Client
Providing unmasked images
Unmasking according to access authority

Fig 3.2 *Tracking objects and persons*

MERGING

After the matching of the entries with incoming blobs is perfomed

```
for (int i=1; i<numOfPerson; i++)
{
for (int j= i+1; j <numOfPerson; j++)
{
if(personList[i].info.matchedIncomingBlobId
==personList[j].info.matchIncomingBlobId )
{
        personList[i].info.merge = true;
        personList[j].info.merge = true;}
```



(a) Unmasked image

(b) Masked image

}

Fig4.1 *Flow Chart of Video Manipulation Method.*

}

To check if there is a merger between merge detectors and entries. It checks whether the blobs and entries match or not. If they match, entries are named as merged entries.

4. SILENT MOTION DETECTION

The recent appearance of the entries is specified in the temporary list hence it is important to examine them frame by frame. This is done by a special silent motion detector which verifies if they are moving or newly entered objects. So, in temporary list it contains the motion of the new entries.

If an object moves to a certain pixel (say J) it can be recognized that it is a person and is kept in the person list and if an object moves to some other rate of pixels (say < J/4) it can be recognized as an object and is placed in the object list. So, if it is a static entry then object is considered as candidate and the background model adopts the object in the next frame. In the figure3.3, the image that is captured generates an object. This object is detected and is stored. If any request for this masked image is received, only authorized access object is performed and image which is restored is given to the user.

5. FUTURE ENHANCEMENT

Even though the proposed system is fully functional, this system is to be taken to the next step of the camera. Here we combined the power of the PCs to the power of the camera. It is performed without archival of image or video information. The power of processing is remained within the level of camera so as to ensure the privacy. Here the key component is the optimization for the object tracking and also masking by the assurance of privacy.

6. CONCLUSION

The proposed system basically masks the images which are recorded and provides access to the user upon request. The user can get access to the recorded information to a certain level that he is allowed to and access exceeding this level is almost impossible for the user. Hence it can be highlighted that this mechanism is secure, efficient, and reliable, ensures privacy and provides a strong restricted access to the user who is not authorized. It can be applied to health care systems, industries, organizations and many other areas which are supposed to be maintained in a confidential way.

7. REFERENCES

[1] https://ieeexplore.ieee.org/document/6128013

[2] 2.https://www.semanticscholar.org/paper/A-Study-on-the-Human-Identification-Technique-for-Kim-Moon/bcaa3c8062058c0265a87d607d971cec45577aeb

[3] 3.https://www.researchgate.net/publication/221109333_A_Study_on_the_Human_Identification_Technique_for_Privacy_Protection_in_Intelligent_Video_Surveillance_System

[4] https://core.ac.uk/download/pdf/29471695.pdf

[5] https://link.springer.com/chapter/10.1007/978-1-84882-301-3_7

[6] https://ijmttjournal.org/Volume-1/Issue-1/ijmttjournal-v1i1p8.pdf

[7] Whatson, S. Faster Higher Stronger Secure. ITNOW 2012, 54, 12–15.

[8] Hagmann, J. Security in the Society of Control: The Politics and Practices of Securing Urban Spaces. Int.

[9] Polit. Sociol. 2017, 11, 418–438.

[10] Park, N.; Lee, D. Electronic identity information hiding methods using a secret sharing scheme in

[11] multimedia-centric internet of things environment. Pers. Ubiquitous Comput. 2018, 22, 3–10.

[12] Yan, J.; Zhang, X.; Lei, Z.; Li, S.Z. Face detection by structural models. Image Vis. Comput. 2014, 32, 790–799.

[13] Chen, W.-G.; Ling, Y. Noise variance adaptive successive elimination algorithm for block motion

[14] estimation: Application for video surveillance. IET Signal Process. 2007, 1, 150–155.

[15] Park, N.; Kang, N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors 2016, 16, 20.

[16] Ziani, A.; Motamed, C.; Noyer, J.-C. Temporal reasoning for scenario recognition in video-

[17] surveillanceusing Bayesian networks. IET Comput. Vis. 2008, 2, 99–107.

[18] Lee, K.; Yeuk, H.; Kim, J.; Park, H.; Yim, K. An efficient key management solution for privacy masking,

[19] restoring and user authentication for video surveillance servers. Comput. Stand. Interfaces 2016, 44, 137–143.

[20] Vijayakumar, P.; Chang, V.; Deborah, L.J.; Balusamy, B.; Shynu, P.G. Computationally efficient privacy

[21] preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. Future

[22] Gener. Comput. Syst. 2018, 78, 943–955.

[23] Diaz, J.; Arroyo, D.; Rodriguez, F.B. A formal methodology for integral security design and verification of

[24] networkprotocols. J. Syst. Softw. 2014, 89, 87–98.

[25] Lee, K.; Yim, K.; Mikki, M.A. A secure framework of the surveillance video network integrating
[26] heterogeneous video formats and protocols. Comput. Math. Appl. 2012, 63, 525–535.
[27] Gope, P. LAAP: Lightweight Anonymous Authentication Protocol for D2D-Aided Fog Computing
[28] Paradigm. Comput. Secur. 2019, 86, 223–237.
[29] Choi, L.K.; Bovik, A.C. Video quality assessment accounting for temporal visual masking of local flicker.
[30] Signal Process. Image Commun. 2018, 67, 182–198.
[31] Koscinski, I.; El Alaoui-Lasmaili, K.; Di Patrizio, P.; Kohler, C. Videos for embryology teaching. power and
[32] weakness of an innovative tool. Morphologie 2019, 103, 72–79.

.