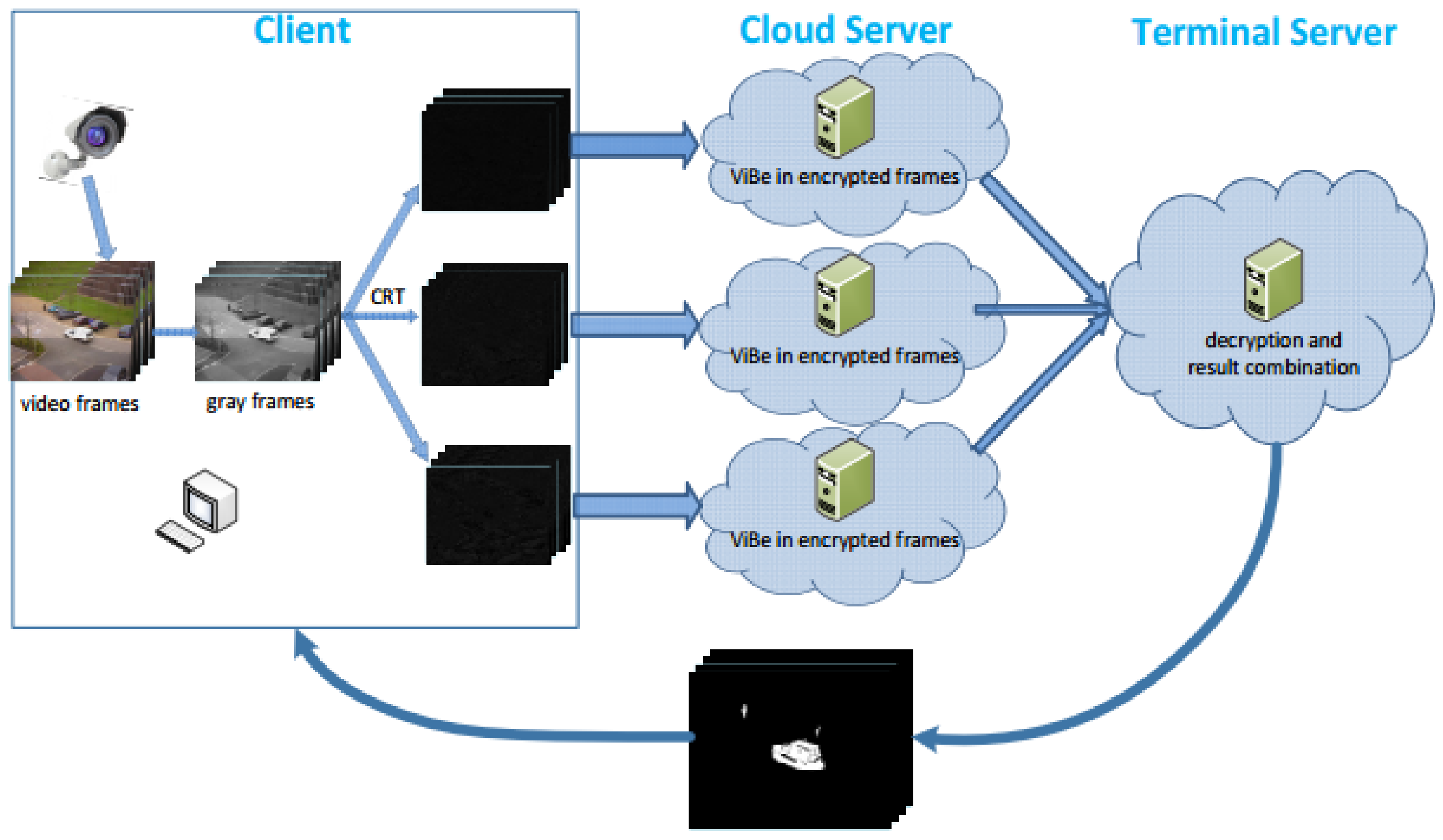
PPViBe: Privacy Preserving Background Extractor via Secret Sharing in Multiple Cloud Servers

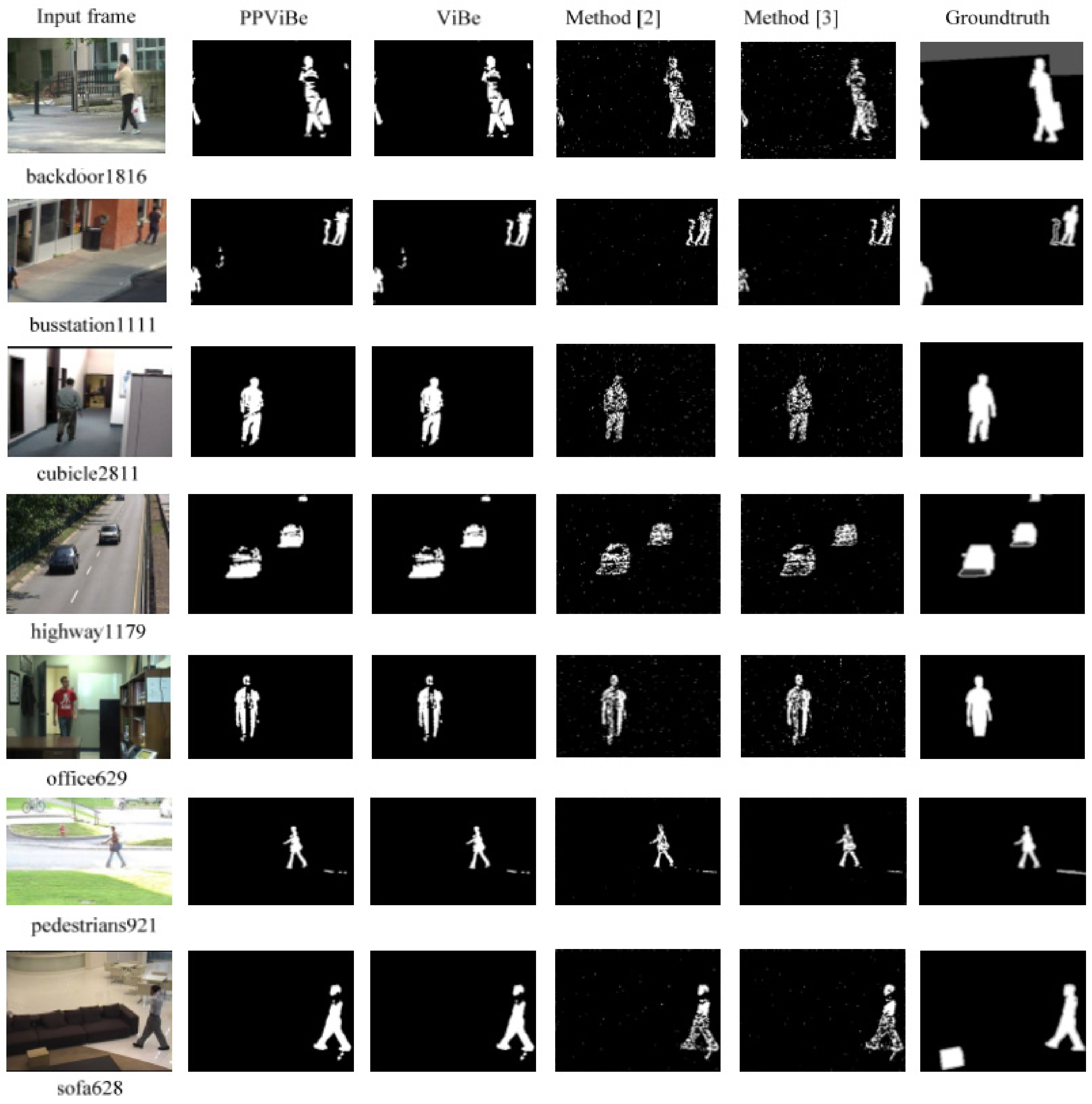
Xin Jin[1], Yaming Wu[2], Xiaodong Li[1], Yuzhen Li[2], Geng Zhao[1], Kui Guo[1]
[1]Beijing Electronic Science and Technology Institute
[2]Xidian University
Corresponding authors: {jinxin,lxd}@besti.edu.cn
http://kislab.besti.edu.cn/victory/

Besti Victory Homepage

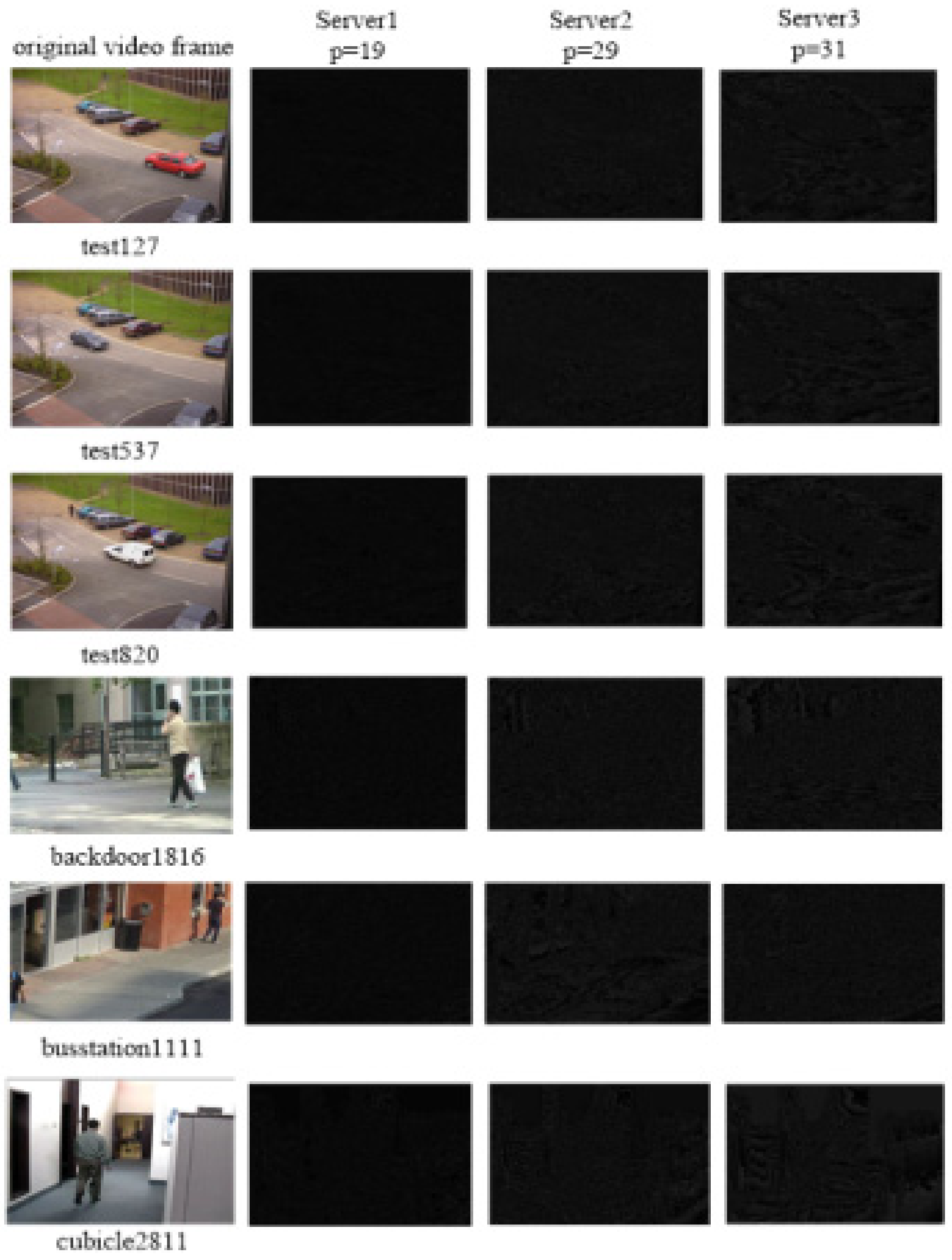
Recently, with the maturity of cloud services and the development of distributed computing, increasing images and video data are stored in the cloud. However, cloud services are generally provided by the third party entities. In addition, the images and video which are stored in the cloud mostly depend on the security of the cloud servers, while the data are not encrypted, which is a great threat to the users’ privacy. In this paper, we propose a method of privacy preserving background extraction of video surveillance in multiple cloud servers based on Chinese Remainder Theorem (CRT).



Method flow char The client does the segmentation process for the video frame .The results are separately sent to different cloud servers. The cloud servers receive the encrypted video frames. In addition, each server learns only a portion of information of the original video frame. The cloud servers use ViBe background detection algorithm [4][5] to process encrypted video frames, following, the processing results in each cloud server are sent to the end server. It is in that place where we judge whether the pixel is in the background or not. Finally, the result is transmitted back to the client. Owing to each server learning only a portion of encrypted information of the video frame, they cannot directly get the information of original video frame. Furthermore, a single server cannot recover the original video frames.



Background Extraction Results We get the same background using ViBe by multiple cloud servers from encrypted frames or unencrypted frames. Thus the results from ViBe background extraction are the same, whether video frames have been encrypted or not. Furthermore, the information of video frames will not directly exposed in cloud servers after be encrypted. This strategy is an efficient way to protect the privacy of user videos.



Encrypted video frames The original frames are split into encrypted shares. The video contents are protected and nearly nothing can be recognized in the cloud servers.

Videos/ Frames	ViBe	PPViBe	Method of [2]	Method of [3]
backdoor/1186	0.822044	0.822044	0.807418	0.795028
bus station/1111	0.943676	0.943676	0.939721	0.946990
cubicle/2811	0.983418	0.983418	0.973237	0.974191
highway/1179	0.951065	0.951065	0.929562	0.936468
office/629	0.905409	0.905409	0.897626	0.901332
pedestrians/921	0.983189	0.983189	0.984055	0.988313
sofa/628	0.946832	0.946832	0.945863	0.944334

The correctness rate of extraction The correctness rate of the background extraction is defined as the number of pixels correctly labelled as foreground or background against the total pixels in the video sequences. Both [2] and [3] use the mixture of Gaussian model to extract the background. The correctness is slightly reduced because of the decryption error. While our PPViBe method has not decryption error and obtain the same correctness rate as that of the ViBe, as shown in Table 1.

Main References

[1] Upmanyu,M., Namboodiri,A.M., Srinathan,K., Jawahar.C.V. Ecient Privacy Preserving Video Surveillance. IEEE 12th International Conference on Computer Vision (ICCV), 1639-1646 (2009).

[2] Chu, K.Y., Kuo Y.H., Hsu W.H. Real-Time Privacy-Preserving Moving Object Detection in the Cloud. ACM Multimedia, 597-600 (2013)

[3] Xin Jin, Kui Guo, Chenggen Song, Xiaodong Li, et al. Private Video Foreground Extraction through Chaotic Mapping based Encryption in the Cloud. The 22nd International Conference On Multimedia Modelling (MMM), 562-573 (2016)

The proposed method has several **advantages:**
1) Based on our encryption method, the original extraction method in the original videos need not be changed;
2) Each cloud server learns only a portion of the video frame information, yet they cannot recover the original video even if the data is leaked;
3) Multiple cloud servers can improve the security of data and enhance the processing efficiency.