WCSP 2016

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
GOCPCCC Key Laboratory of Information Security
[2]Xidian University
Corresponding author: {jinxin,lxd}@besti.edu.cn

北京電子科技学院
Beijing Electronic Science and Technology Institute

VICTORY
besti

西安電子科技大學
XIDIAN UNIVERSITY

Outline

1 **Motivation**

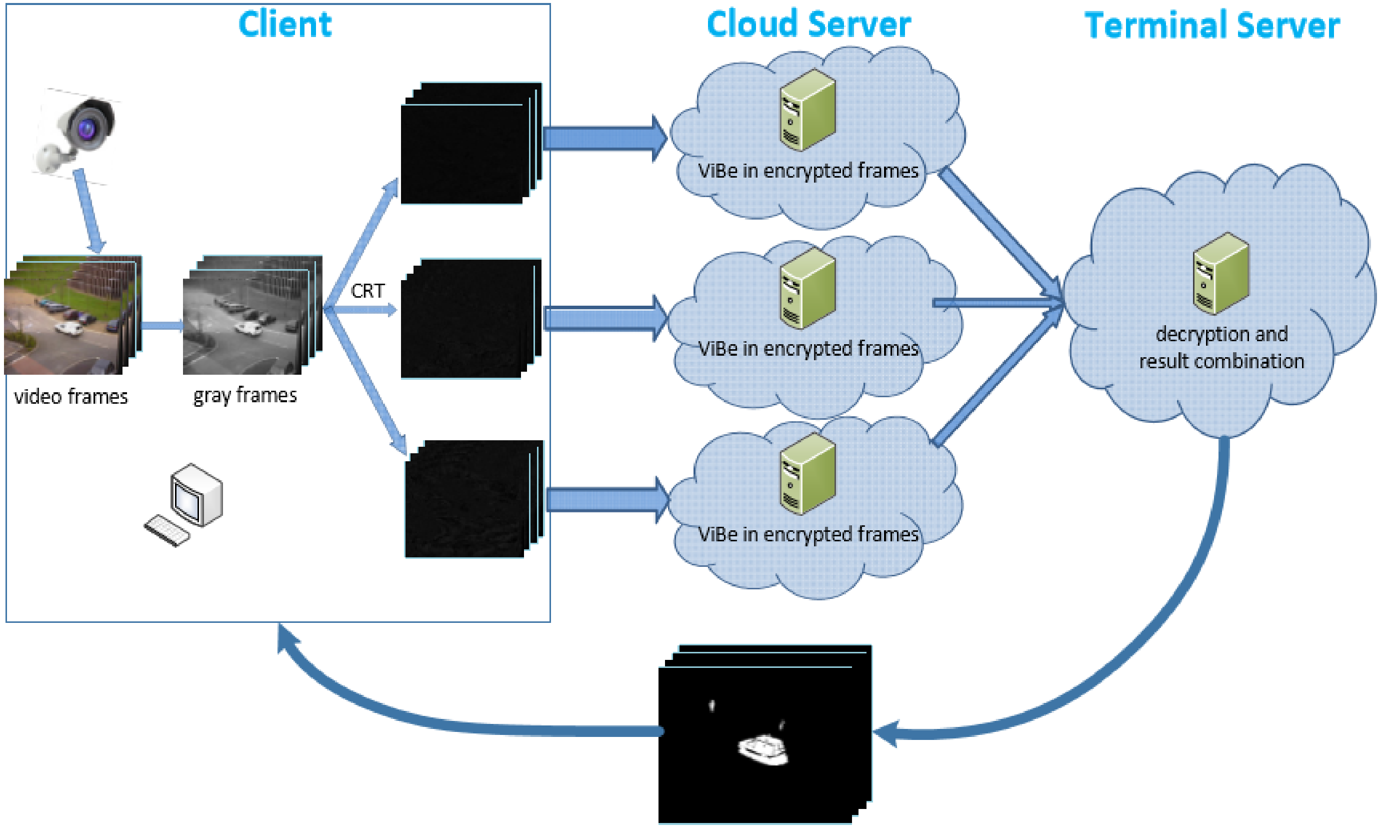
2 **Preliminaries**

3 **Privacy Preserving ViBe**

4 **Results**

5 **Conclusion and Discussion**

Motivation


Client
Cloud Server
Terminal Server
video frames
gray frames
CRT
ViBe in encrypted frames
ViBe in encrypted frames
ViBe in encrypted frames
decryption and
result combination

Outline

1 Motivation

2 Preliminaries

3 Privacy Preserving ViBe

4 Results

5 Conclusion and Discussion

Preliminaries

- **Visual Background Extractor**

Visual Background Extractor (ViBe) is an algorithm of pixel-level background modeling, occupying less memory and having high processing efficiency.

Generally speaking, the values of pixel in background and pixels surrounding it possess the characteristics of having a small change within a certain time.

Making use of the above characteristic, the sample model, which is used to judge whether the background or not, is established for each pixel.

Preliminaries

- **The Chinese Remainder Theorem**

The Chinese Remainder Theorem (CRT) is a result about congruence in number theory and its generalizations in abstract algebra.

According to the CRT, we construct i congruencies for one pixel by i different prime numbers.

Outline

1 Motivation

2 Preliminaries

3 Privacy Preserving ViBe

4 Results

5 Conclusion and Discussion

Privacy Preserving ViBe

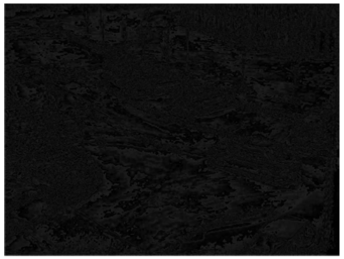
The Client

Every pixel will do the operation by：

$$\alpha_1 = (\alpha * s + \eta) \bmod p_1$$

$$\alpha_2 = (\alpha * s + \eta) \bmod p_2$$

$$\alpha_3 = (\alpha * s + \eta) \bmod p_3$$



Privacy Preserving ViBe

The Cloud Servers

(1) Background modeling

For each pixel, the neighboring pixel values are selected to get its sample model.

$$V(n)=\{x_1,x_2,\ldots,x_i,\ldots x_n\}$$

x_1	$\cdots$	
	x	
		x_i

Privacy Preserving ViBe

The Cloud Servers

(1) Model application

The value of new pixel y in the second frame is made the difference with the pixel values within the sample model. And we will get a set for every pixel.

$$C(y) = \{y - x_1, y - x_2, \ldots, y - x_i, \ldots y - x_n\}$$

$$c_i = (y - x_i) \bmod p_t$$

$$C(y) = \{c_1, c_2, \ldots, c_i, \ldots, c_n\}$$

Privacy Preserving ViBe

The Terminal Server

$$C_{p_1}(y)=\{c_{11},c_{12},\ldots,c_{1i},\ldots,c_{1n}\}$$

$$C_{p_2}(y)=\{c_{21},c_{22},\ldots,c_{2i},\ldots,c_{2n}\}$$

$$C_{p_3}(y)=\{c_{31},c_{32},\ldots,c_{3i},\ldots,c_{3n}\}$$

After received all the difference sets from all the three cloud servers, the terminal server will construct congruence equations as fellows:

$$y_1 \equiv c_{11} \bmod p_1$$

$$y_1 \equiv c_{21} \bmod p_2$$

$$y_1 \equiv c_{31} \bmod p_3$$

Privacy Preserving ViBe

The Terminal Server

Then we can solve the equations by CRT to get decrypted difference set

$$D(y) = \{y_1, y_2, \dots, y_i, \dots, y_n\}$$

for every pixel.

Then:

*(1)*Compares each value in $D(y)$ to the threshold R;

*(2)*If less than R, #++;

*(3)*Count the number of #, if # is more than #min(represents the minimum matching value), the pixel is determined to be the background one.

Outline

1 Motivation

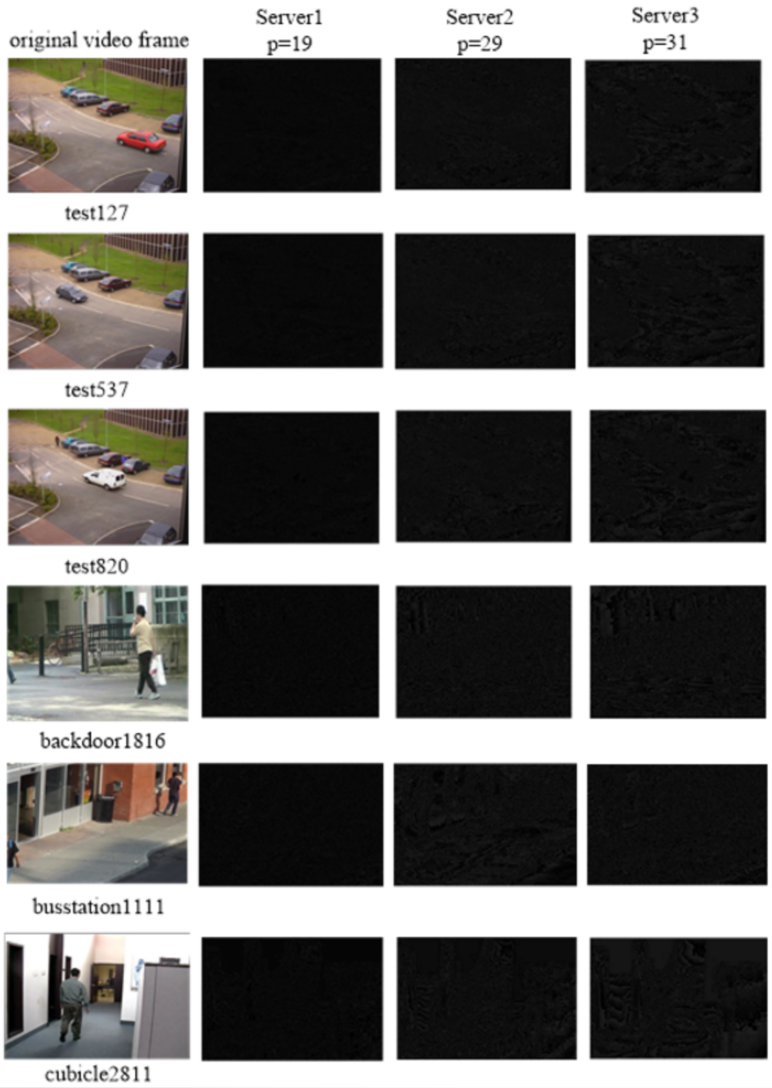
2 Preliminaries

3 Privacy Preserving ViBe

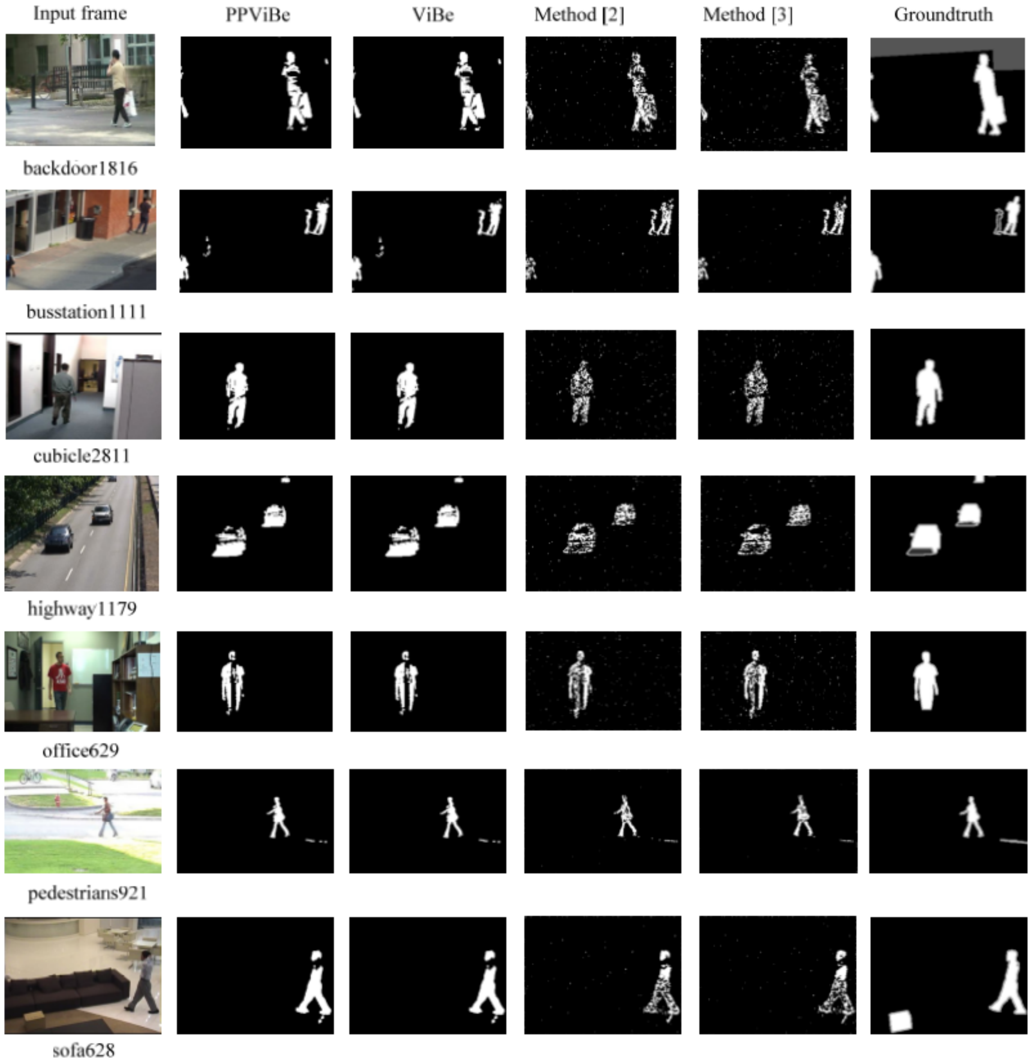
4 Results

5 Conclusion and Discussion

Encryption Results



Background Extraction Results



Outline

1 Motivation

2 Preliminaries

3 Privacy Preserving ViBe

4 Results

5 Conclusion and Discussion

Conclusion and Discussion

- Our method could get precisely background while video frames are safely protected. This is the first time that the ViBe is integrated into the CRT based secret sharing framework.
- In the future work, we will integrate more video surveillance algorithms to Secure Multi-party Computation (SMC) framework and make the computer vision in the cloud more secure.

Thanks！

Scan to visit our
Victory Team
of Besti (WeChat)