Security and Privacy of Visual Data

Anoop M. Namboodiri, Kannan Srinathan, C.V. Jawahar

Center for Visual Information Technology

CSTAR

Video Encryption

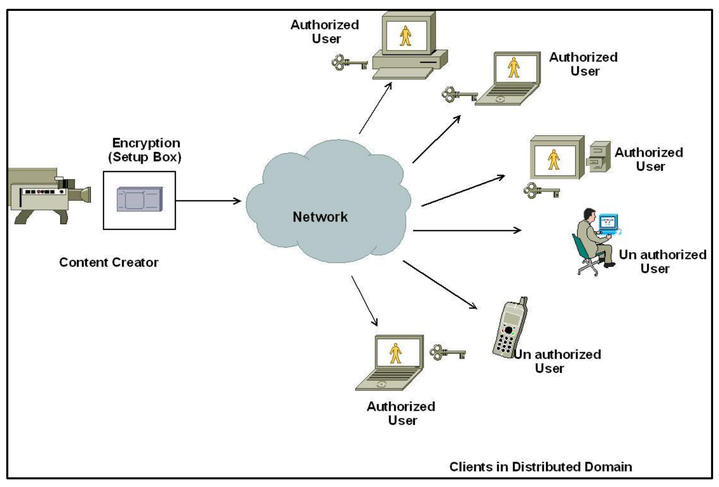
--C. Narsimha Raju

Video protection using encryption is an extremely useful method for the stopping unwanted interception and viewing of any transmitted video or other information.

Based on the importance of the DC component to the visual content, It is shared among the ACs based on Shamir Secret Sharing. [ICIP 2008]

Statistical behavior of the DCT coefficients are analyzed and based on the variation of the coefficients, a scrambling followed by permutation scheme is proposed. [TENCON 2008]

Apart from their statistical behavior, in this work, we exploit the properties of the coefficients and their influence on the visual content for designing the encryption scheme. [ICVGIP 2008]



A Network model of the distributed multimedia systems

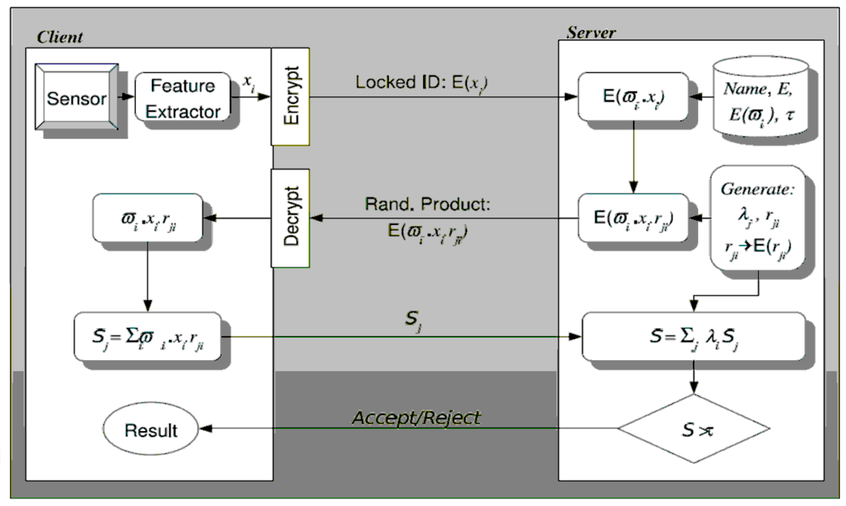
Blind Authentication

--Maneesh Upmanyu

Problem setting: Alice wants to create an account in Bob-mail, that requires biometrics based authentication. However, she neither trusts Bob to handle her biometric data securely, nor trusts the network to send her plain biometric. [ICB 2009]

We carry out the authentication in the encrypted domain. This is accomplished by using additive and multiplicative homomorphic encryption schemes .

The proposed scheme does not make any assumption on the nature of the data and is hence applicable to any biometric. Such a protocol has significant advantages over existing biometric cryptosystems, which use a biometric to secure a secret key, which in turn is used for authentication.



Blind Authentication Process

Broad Objective

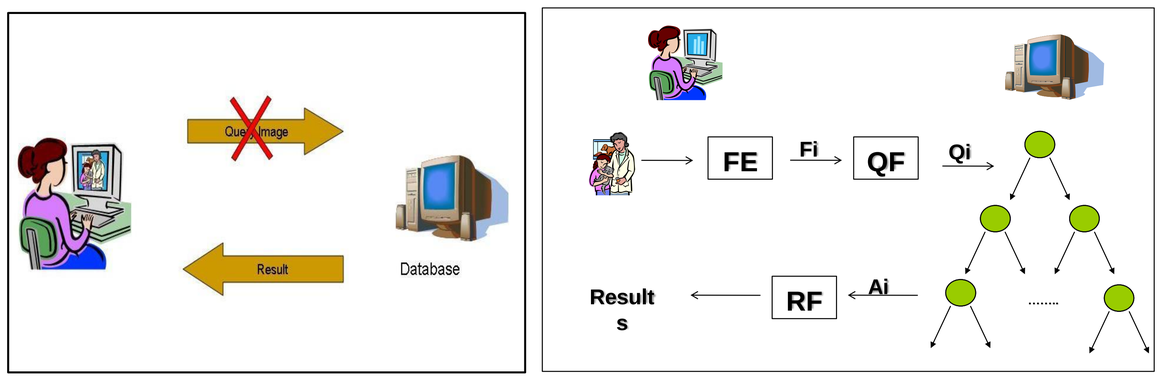
Develop secure computational algorithms in computer vision and related areas.

To Develop

- Provably secure solutions
- Computationally efficient solutions
- Solutions to problems with immediate impact

Private Content Based Image Retrieval (PCBIR)

--Shashank , Kowshik



Private Content Based Image Retrieval Scheme

Problem setting: Alice has query image (I), Bob maintains a image-database server. However, the image may contain personal information and hence Alice wants to retrieve similar images without revealing (I) to Bob. [CVPR 2008]

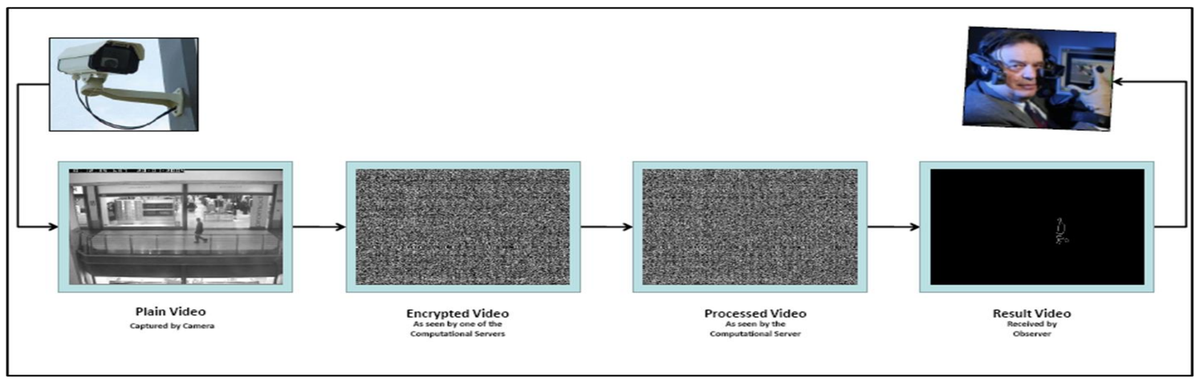
Secure algorithms designed to address it. Exploits the clustered nature of image databases to reduce the amount of communication required in SMC

We achieve this using the private information retrieval (PIR) scheme, proposed for linear databases. We suitably adapt their proposed solution to BST. Extensions are also proposed to other tree structures such as hierarchical , hash-tree based retrieval.

Proposed algorithms are completely private and feasible for extremely large datasets. Possible applications include Medical Image Databases, Surveillance Systems, Logo Patent Search, Defense Systems etc.

Efficient Privacy Preserving Video Surveillance

--Maneesh Upmanyu



Proposed Surveillance Process

Problem Setting: Alice wants to have her office environment under surveillance by Bob. To preserve privacy of the employees, Alice wants to encrypt the surveillance videos before giving it to Bob, and wants Bob to carry out surveillance directly on them. [ICCV 2009]

We achieve this using the paradigm of Secret Sharing, suitably adapted to image data.

The privacy of our surveillance system is based on splitting the information present in an image into multiple shares., such that no share by itself conveys anything about the original image. Each share is then sent to an independent server for processing.

Circumvent the theoretical communication bounds by exploiting characteristic properties of the image data. Proposed solution is 1 million times faster than that based on SMC.

Center for Visual Information Technology
International Institute of Information Technology Hyderabad
http://cvit.iiit.ac.in