Reducing the Ciphertext Expansion in Image Homomorphic Encryption via Linear Interpolation Technique

Yunyu Li[1], Jiantao Zhou[1], Yuanman Li[1], and Oscar C. Au[2]

[1]Faculty of Science and Technology, University of Macau
[2]Department of ECE, Hong Kong University of Science and Technology

December 2, 2015

Outline

Homomorphic encryption (HE):
provides a generic framework of performing basic algebraic operations over the encrypted domain.

It becomes one of the key components in many emerging applications, e.g., cloud computing, to achieve privacy-preserving data processing.

Homomorphic Encryption

Two categories :

- Partially HE: keep the relation of addition or multiplication between plaintexts and ciphertexts; [8-bit vs 2048-bit]
  eg: Paillier(additive).etc.
- Fully HE: allows the computation of any polynomials in the encrypted domain. [4MB vs 73TB]

Problem

However, one of the major drawbacks that precludes the widespread adoption of homomorphic encryption is the huge expansion of the ciphertext.

Previous Methods to Deal with Ciphertext Expansion

- **Packing scheme** [1]: packs several messages as a word and encrypts them together;
  - causes many operations infeasible without interactive protocol.
- **Zheng and Huang's method** [2]: indexs a sequence of ciphertexts produced by the scaled-down histogram of the image;
  - has serious security problems [3].

Outline

Proposed Image Homomorphic Encryption Scheme

Basic Idea

our idea is to encrypt only a subset of the pixels using Paillier, and relate the remaining pixels to these homomorphically encrypted ones.

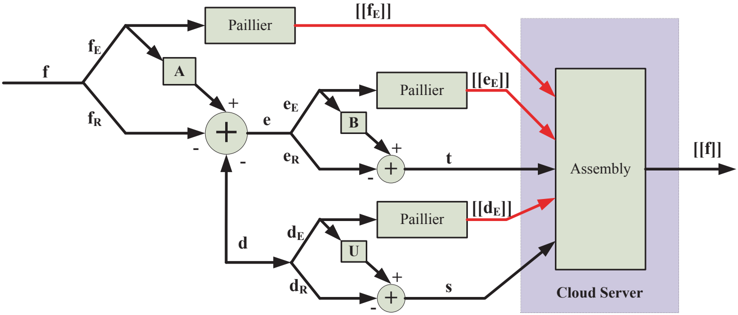

Figure 1: Schematic diagram of the proposed scheme.

Let $\mathbf{f} = [f_1, f_2, \cdots, f_n]^T$ be the image (8-bit) to be encrypted.

Randomly divide $\mathbf{f}$ into two parts:

- $\mathbf{f}_E = [f_{E,1}, f_{E,2}, \cdots, f_{E,m}]^T$;
- $\mathbf{f}_R = [f_{R,1}, f_{R,2}, \cdots, f_{R,n-m}]^T$;

Proposed Image Homomorphic Encryption Scheme

- $\mathbf{f}_E$ part: a sub-image, are encrypted using Paillier,

$$[[\mathbf{f}_E]] = \left[[[f_{E,1}]], [[f_{E,2}]], \cdots, [[f_{E,m}]] \right]^T \tag{1}$$

where semantic security is achieved by employing different r's for different pixels.

- $\mathbf{f}_R$ part: relates the pixels in $\mathbf{f}_R$ with those in $\mathbf{f}_E$ via an interpolation-like form

$$\mathbf{e} = \mathbf{A}\mathbf{f}_E - \mathbf{f}_R - \mathbf{d} \tag{2}$$

where $\mathbf{e}$ represents the residual vector;
$\mathbf{A} \in \{0, 1\}^{(n-m)\times m}$ is the interpolation matrix;
$\mathbf{d}$ is an interference vector designed for security purpose.

Instead of sending **e** and **d** directly without any protection, we further process **e** and **d** in a similar fashion as that to encrypt **f**.

Finilly, the ciphertext of our proposed scheme consists of five components $[[\mathbf{f}_E]]$, $[[\mathbf{e}_E]]$, $[[\mathbf{d}_E]]$, **t** and **s**, which would be sent to the could server.

Cloud Server:

can decompress and obtain the whole encrypted image $[[\mathbf{f}]]$, prior to applying any homomorphic operations over the encrypted data.

Outline

The factor of ciphertext expansion ρ is defined by

$$\rho = \frac{\text{size of the ciphertext}}{\text{size of the plaintext}} \tag{3}$$

The size of plaintext is $8n$ bits, each Paillier ciphertext is of length $2b_N$ bits, we can easily calculate,

$$\rho = \frac{2b_N(m+l+u) + b_t(n-m-l) + b_s(n-m-u)}{8n} \tag{4}$$

where b_t and b_s denote the number of bits needed to represent each element of $\mathbf{t}$ and $\mathbf{s}$.

Outline

To verify the security property, we build up the total variation (TV)-based estimation framework to disclose the original image **f**

$$\min_{\mathbf{f}} \ \frac{\tau}{2}\|\hat{\mathbf{e}} + \hat{\mathbf{d}} - (\mathbf{AC} - \mathbf{D})\,\mathbf{f}\|_2^2 + \|\mathbf{f}\|_{TV} \\ \text{s.t. } 0 \preceq \mathbf{f} \preceq 255 \tag{5}$$

where $\hat{\mathbf{e}}$ and $\hat{\mathbf{d}}$ are optimal estimates in the least-square sense.

Such optimization problem can be efficiently solved using the split Bregman algorithm [4].

Outline

1. Introduction
2. Reducing the Ciphertext Expansion via Linear Interpolation Technique
   - Proposed Image Homomorphic Encryption Scheme
   - Analysis of the Ciphertext Expansion
   - Security Analysis
3. Experiment Results
   - Simulation Experiment
   - Security Experiment

Goal: verify the correctness of the encryption/decryption modules.
Environment: C++ under Ubuntu, NTL and GNU Multi-Precision libraries.

Set $N = 1024$ bits, $l = m = u = 0.005n$.

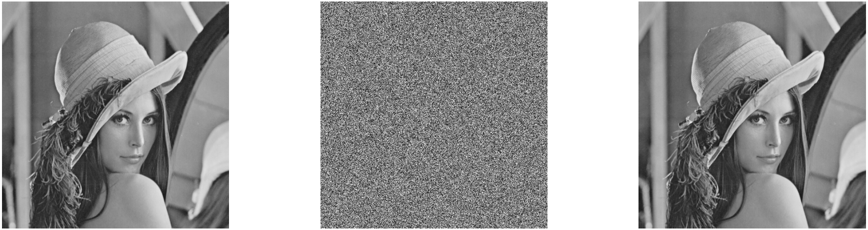

Figure 2: (a) original Lena; (b) encrypted Lena in the Cloud; (c) decrypted Lena

Security Experiments

Goal: demonstrate the ciphertext expansion factor, and the corresponding security level indicated by the reconstruction quality of solving (5).

Set $l = m = u = L$; Perform the TV algorithm for different L's.

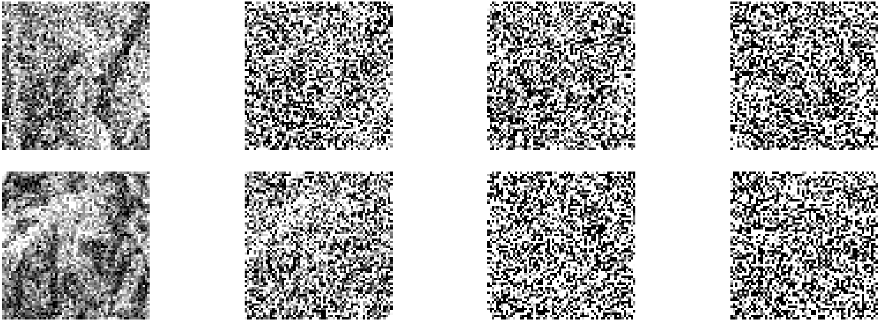

Figure 3: Reconstruction results of Lena and Barbara. (a), (e) $L = 0.001n$; (b), (f) $L = 0.003n$; (c), (g) $L = 0.005n$; (d), (h) $L = 0.007n$

Security Experiments

As L gradually increases, the reconstruction quality becomes worse. The ciphertext expansion factors $\rho = 7.058$ at the critical point $L = 0.005n$.

Compared with the traditional element-wise homomorphic encryption scheme in which $\rho = 256$, our proposed approach achieves the ciphertext expansion reduction of factor around 36, which is significant.

References

[1] J. R. Troncoso-Pastoriza, S. Katzenbeisser, M. Celik, and A. Lemma, "A secure multidimensional point inclusion protocol," in *Proc. 9th ACM Workshop on Multimedia and Security*. ACM, 2007, pp. 109–120.

[2] P. Zheng and J. Huang, "An efficient image homomorphic encryption scheme with small ciphertext expansion," in *Proc. of the 21st ACM Int. Conf. on Multimedia (MM'13)*. ACM, 2013, pp. 803–812.

[3] Y. Li, J. Zhou, and Y. Li, "Ciphertext-only attack on an image homomorphic encryption scheme with small ciphertext expansion," in *Proceedings of the 23rd Annual ACM Conference on Multimedia Conference*. ACM, 2015, pp. 1063–1066.

[4] T. Goldstein and S. Osher, "The split bregman method for l1-regularized problems," *SIAM J. on Applied Mathematics*, vol. 2, no. 2, pp. 323–343, 2009.

If you have any questions, plese do not hesitate to contact the authors.

Email: {mb35468, jtzhou, mb25510}@umac.mo, eeau@ust.hk