A Note on "Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization"

Zhengjun Cao[1] and Lihua Liu[2]

Abstract. Recently, Lu et al. have proposed two image search schemes based on additive homomorphic encryption [IEEE Access, 2 (2014), 125-141]. We remark that both two schemes are flawed because: (1) the first scheme does not make use of the additive homomorphic property at all; (2) the additive homomorphic encryption in the second scheme is unnecessary and can be replaced by a more efficient symmetric key encryption.

Keywords. Cloud computing, confidentiality-preserving image search, additive homomorphic encryption, symmetric key encryption.

1 Introduction

Recently, Lu et al. [1] have discussed how existing additive homomorphic encryption can be potentially used for image search, and proposed two confidentiality-preserving image search schemes based on Paillier's encryption [2]. In the proposed model, a client has many images who wants to store the image data online for convenient data access anywhere anytime. The client has to encrypt each image and its features and upload the encrypted data to a cloud server. In this note, we remark that the Lu et al.'s schemes are flawed.

2 Review of the Lu et al.'s schemes

In the schemes [1], the features of each image are encrypted by any additively homomorphic encryption such as Paillier's cryptosystem [2], which can be described as follows. Pick an RSA modulus $n = pq$. Set $\lambda = \mathrm{lcm}(p-1, q-1)$. Select $g \in \mathbb{Z}^*_{n^2}$ such that $n \mid \mathrm{ord}_{n^2}(g)$. Publish n, g and keep λ in secret. For $m \in \mathbb{Z}_n$, pick $r \in \mathbb{Z}_n$, compute the ciphertext $c = \mathcal{E}(m) = g^m r^n \bmod n^2$. Recover $m = \mathcal{D}(c) = \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right) / \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right) \bmod n$.

Denote the encrypting function and decrypting function of AES by $E(\cdot)$ and $D(\cdot)$, and that of Paillier's cryptosystem by $\mathcal{E}(\cdot)$ and $\mathcal{D}(\cdot)$, respectively. See Table 1 and Table 2 for the details of the two image search schemes.

[1] Department of Mathematics, Shanghai University, Shanghai, China.
[2] Department of Mathematics, Shanghai Maritime University, China. liulh@shmtu.edu.cn

Table 1: The Lu et al.'s scheme 1

Client		Server
Encrypt the image $P^{(i)}$ and its feature vector $\mathbf{f}^{(i)} \in \mathbb{R}^t$ as $\mathcal{E}(\mathbf{f}^{(i)}) = (\mathcal{E}(f_1^{(i)}), \cdots, \mathcal{E}(f_t^{(i)}))$ and $E(P^{(i)})$. Upload them.	$\xrightarrow[i=1,\cdots,N]{\{i,\mathcal{E}(\mathbf{f}^{(i)}),E(P^{(i)})\}}$	Store the encrypted images and features.
Given an image Q and its feature vector $\mathbf{q}$, ask for all the encrypted features.	$\xrightarrow{Request}$	
	$\xleftarrow[i=1,\cdots,N]{\{i,\mathcal{E}(\mathbf{f}^{(i)})\}}$	Return all encrypted features.
Compute $\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)}))$ and the L_2 distance $d_i = \parallel \mathbf{f}^{(i)} - \mathbf{q} \parallel$, $i = 1, \cdots, N$. Send $\mathcal{I} = \{j \mid d_j \leq \lambda\}$, where λ is a fault-tolerant parameter.	$\xrightarrow{\mathcal{I}}$	
Recover all $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$.	$\xleftarrow[k\in\mathcal{I}]{\{E(P^{(k)})\}}$	Return all $E(P^{(k)}), k \in \mathcal{I}$.

Table 2: The Lu et al.'s scheme 2

Client		Server
Encrypt the image $P^{(i)}$ and its feature vector $\mathbf{f}^{(i)} \in \mathbb{R}^t$ as $\mathcal{E}(\mathbf{f}^{(i)}) = (\mathcal{E}(f_1^{(i)}), \cdots, \mathcal{E}(f_t^{(i)}))$ and $E(P^{(i)})$. Compute $\chi_i = \mathcal{E}\left(\Sigma_{\ell=1}^t (f_\ell^{(i)})^2\right)$. Upload them.	$\xrightarrow[i=1,\cdots,N]{\{i,\chi_i,\mathcal{E}(\mathbf{f}^{(i)}),E(P^{(i)})\}}$	Store the encrypted images and features.
Given an image Q and its feature vector $\mathbf{q}$, send $\mathbf{q}$ to the server.	$\xrightarrow{\mathbf{q}}$	Compute $h_i = \left(\prod_{\ell=1}^t (\mathcal{E}(f_\ell^{(i)}))^{q_\ell}\right)^{-2} \cdot \mathcal{E}\left(\Sigma_{\ell=1}^t q_\ell^2\right) \cdot \chi_i$, $i = 1, \cdots, N$.
Compute $d_i = \mathcal{D}(h_i)$, $i = 1, \cdots, N$. Randomly pick a set $\widehat{\mathcal{I}} \subset \{1, \cdots, N\}$ of an appropriate size. Set $\mathcal{I}' = \widehat{\mathcal{I}} \bigcup \mathcal{I}$ where $\mathcal{I} = \{j \mid d_j \leq \lambda, 1 \leq j \leq N\}$, λ is a fault-tolerant parameter.	$\xleftarrow{h_i,i=1,\cdots,N}$ $\xrightarrow{\mathcal{I}'}$	Send them back.
Recover all images $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$.	$\xleftarrow[k\in\mathcal{I}']{\{E(P^{(k)})\}}$	Return all $E(P^{(k)}), k \in \mathcal{I}'$.

Notice that, by the additive homomorphic property of Paillier's encryption, we have

$$\begin{aligned}
\mathcal{E}\left(\|\mathbf{f}^{(i)}-\mathbf{q}\|^2\right) &= \mathcal{E}\left(\Sigma_{\ell=1}^t (f_\ell^{(i)}-q_\ell)^2\right) = \mathcal{E}\left(\Sigma_{\ell=1}^t (f_\ell^{(i)})^2 - 2\Sigma_{\ell=1}^t f_\ell^{(i)} q_\ell + \Sigma_{\ell=1}^t q_\ell^2\right) \\
&= \mathcal{E}\left(\Sigma_{\ell=1}^t (f_\ell^{(i)})^2\right) \cdot \mathcal{E}\left(-2\Sigma_{\ell=1}^t f_\ell^{(i)} q_\ell\right) \cdot \mathcal{E}\left(\Sigma_{\ell=1}^t q_\ell^2\right) \\
&= \chi_i \cdot \left(\prod_{\ell=1}^t (\mathcal{E}(f_\ell^{(i)}))^{q_\ell}\right)^{-2} \cdot \mathcal{E}\left(\Sigma_{\ell=1}^t q_\ell^2\right) = h_i, \\
d_i &= \mathcal{D}(h_i) = \mathcal{D}\left(\mathcal{E}(\|\mathbf{f}^{(i)}-\mathbf{q}\|^2)\right) = \|\mathbf{f}^{(i)}-\mathbf{q}\|^2.
\end{aligned}$$

3 Analysis of the Lu et al.'s schemes

We now show that the Lu et al.'s schemes are flawed.

(1) *The authors [1] have confused the general arithmetic over the field* $\mathbb{R}$ *and the modular arithmetic over the domain* $\mathbb{Z}_n$. In fact, the correctness of the schemes are based on

$$\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)})), \ \ \|\mathbf{f}^{(i)}-\mathbf{q}\|^2 = \mathcal{D}\left(\mathcal{E}(\|\mathbf{f}^{(i)}-\mathbf{q}\|^2)\right).$$

The equations hold on the condition that $\mathbf{f}^{(i)}$ and $\|\mathbf{f}^{(i)}-\mathbf{q}\|^2$ are in the underlying domain $\mathbb{Z}_n$ of Paillier's encryption. That means a visual feature vector $\mathbf{f} \in \mathbb{R}^t$ must be transformed into $\widetilde{\mathbf{f}} \in \mathbb{Z}_n^t$. But the authors [1] have not specified this process.

By the way, there is a typo in the description of the decrypting equation of Paillier's cryptosystem (see Ref.[1], page 128). It should be $m = \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right) / \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right) \bmod n$, not $m = \left(\frac{c^\lambda - 1 \bmod n^2}{n}\right) / \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right) \bmod n^2$.

(2) *In the scheme 1, both the client and the server do not make use of the additive homomorphic property of Paillier's encryption at all.* The related computations for the client are

$$\mathbf{f}^{(i)} = \mathcal{D}(\mathcal{E}(\mathbf{f}^{(i)})), \ i = 1, \cdots, N.$$

Actually, the process has no relation to the additive homomorphic property. Thus, in the scheme the Paillier's public key encryption can be reasonably replaced by the more efficient symmetric key encryption AES.

It seems that the authors [1] have not realized that the computational performance of public-key encryption is inferior to that of symmetric-key encryption. For example, the authors wrote [1] "image encryption can be done using state-of-the-art ciphers such as AES or RSA by treating images as ordinary data". We here would like to stress that images should be encrypted by a symmetric key encryption, instead of any public key encryption. In practice, RSA is usually used for encrypting session keys, not for images. Compared with AES, RSA is fairly inefficient.

(3) In the scheme 2, the server has to make use of the additive homomorphic property for computing the encrypted distance $h_i = \mathcal{E}\left(\|\mathbf{f}^{(i)} - \mathbf{q}\|^2\right)$. But in such case, the client has still to compute $d_i = \mathcal{D}(h_i), i = 1, \cdots, N$, which dominate the client's computational cost. Compared with the revised scheme, we find, *the scheme 2 has not truly mitigated the client's computational cost*. See the Table 3 for the comparisons of the dominated computations for the client in the three schemes.) Apparently, the revised scheme is more efficient because it only needs to perform symmetric key decryption $N + |\mathcal{I}|$ times.

Table 3: The dominated computations for the client in the three schemes

	Dominated computations	Computational cost
Scheme 1	$\mathbf{f}^{(i)} = \left(\mathcal{D}(\mathcal{E}(f_1^{(i)})), \cdots, \mathcal{D}(\mathcal{E}(f_t^{(i)}))\right)$, $i = 1, \cdots, N$. $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$.	public key decryption: tN (times) symmetric key decryption: $\vert\mathcal{I}\vert$
Scheme 2	$d_i = \mathcal{D}(h_i)$, $i = 1, \cdots, N$. $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$.	public key decryption: N symmetric key decryption: $\vert\mathcal{I}\vert$
The revised	$\mathbf{f}^{(i)} = D(E(\mathbf{f}^{(i)}))$, $i = 1, \cdots, N$. $P^{(k)} = D(E(P^{(k)})), k \in \mathcal{I}$.	symmetric key decryption: $N + \vert\mathcal{I}\vert$

4 Conclusion

We show that the Lu et al.'s schemes for image search are flawed and somewhat misleading. We here want to stress that the computational performance of public-key encryption is inferior to that of symmetric-key encryption. A homomorphic encryption allows anyone to perform some computations on encrypted data, despite not having the secret decryption key. But any computations performed on encrypted data are constrained to the underlying domain (finite domains). The real goal of using modular arithmetic in cryptography is to obscure and dissipate the redundancies in a plaintext message, not to perform any numerical calculations.

References

[1] W.J. Lu, A. L. Varna and M. Wu, "Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization", IEEE Access, 2 (2014), 125-141.

[2] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", In: Stern, J. (ed.), Proc. of EUROCRYPT 1999, LNCS, vol. 1592, pp. 223-238, 1999.