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

***Abstract*—Homomorphic encryption becomes one of the key components in many emerging applications, e.g., cloud computing, to achieve privacy-preserving data processing. However, one of the major drawbacks that precludes the widespread adoption of homomorphic encryption is the huge expansion of the ciphertext. This problem becomes even more severe when multimedia data (images/videos) are handled, as these files are essentially of large sizes. This work addresses this challenging issue and proposes a strategy of reducing the ciphertext expansion in image homomorphic encryption. To this end, a randomly selected subset of the pixels are encrypted using homomorphic cryptosystem to form one part of the ciphertext. The remaining pixels are encrypted by relating them with this random subset through a linear interpolation technique. The whole homomorphically encrypted image can be obtained, upon receiving all the ciphertexts, by exploiting the homomorphic property and the linearity. It is demonstrated that the proposed scheme is secure, and is capable of achieving significant reduction of the ciphertext expansion, while perfectly preserving the homomorphic property.**

***Index Terms*—homomorphic encryption, ciphertext expansion, linear interpolation**

## I. Introduction

Signal processing over encrypted domain (SPED) has been receiving increasing attention in recent years, primarily driven by the various privacy-preserving applications and the wide adoption of cloud computing platforms [1], [2], [3]. Among the encryption solutions enabling SPED, homomorphic encryption is arguably the most popular one, as it provides a generic framework of performing basic algebraic operations over the encrypted domain [4], [5], [6], [7]. The existing homomorphic cryptosystems can be roughly classified into two categories: partially homomorphic schemes [5], [6] and fully homomorphic ones [7]. The partially homomorphic schemes support encrypted domain operations that correspond to the addition *or* multiplication in the plaintext domain, while the latter type allows both the addition *and* multiplication. Well-known partially homomorphic schemes include Paillier cryptosystem [5], ElGamal cryptosystem [6], etc. The development of the fully homomorphic cryptosystems is in the infancy stage, and may still be far away from practical deployment [7]. A variety of applications utilizing partially homomorphic cryptosystems (particularly Paillier) have been proposed such as privacy-preserving face recognition [8], fingerprint recognition [9], and zero-knowledge watermarking [10].

However, one of the major obstacles that precludes the widespread adoption of homomorphic encryption in practice is the huge expansion of the ciphertext. For instance, when the Paillier cryptosystem, with modulus $N$ being 1024 bits, is used to encrypt 8-bit image, the resulting encrypted file is 256 times larger than the original image [5]. For fully homomorphic cryptosystem, the ciphertext expansion is even prohibitive: 73 TB of encrypted file are generated for 4 MB of the original data [7]. If not otherwise specified, we focus on the Paillier scheme in this paper. To deal with the ciphertext expansion problem, Trobcoso-Pastoriza proposed a packing scheme, in which several messages are packed as a word and encrypted together [11]. This scheme was later extended in [12] with generalized packing basis. However, such packing makes it impossible to process each message differently, and causes many operations, e.g., encrypted-domain DFT [13] and DWT [14], infeasible without interactive protocol. Zheng and Huang recently suggested a more promising approach for reducing the ciphertext expansion by indexing a sequence of ciphertexts produced by the scaled-down histogram of the image [15]. Nevertheless, as mentioned in [16], this scheme suffers from serious security problems, especially for images with large portion of homogeneous regions.

In this paper, we propose a strategy of reducing the ciphertext expansion in image homomorphic encryption. To this end, a randomly selected subset of the pixels are encrypted using homomorphic cryptosystem to form one part of the ciphertext. The remaining pixels are encrypted by relating them with this random subset through a linear interpolation framework. The whole homomorphically encrypted image can be obtained, upon receiving all the ciphertexts, by exploiting the homomorphic property and the linearity. It is demonstrated that the proposed scheme is secure, and is capable of achieving significant reduction of the ciphertext expansion, while perfectly preserving the homomorphic property.

The rest of this paper is organized as follows. Section 2 briefly overviews the Paillier cryptosystem. Section 3-5 present our method to reduce the ciphertext expansion and the performance analysis. Security analysis as well as experimental results are given in Section 6 and Section 7, respectively. We finally conclude in Section 8.

978-1-4799-7591-4/15/$31.00 ©2015 IEEE

## II. Paillier Cryptosystem

One of the best known homomorphic encryption schemes is due to Paillier [5], belonging to the category of additively (partially) homomorphic cryptosystem. The operations of the Paillier cryptosystem are briefly described as follows.

Let $p$ and $q$ be two large primes, and $N = pq$. Define $\mathcal{Z}_{N^2} = \{0, 1, \cdots, N^2 - 1\}$, and let $\mathcal{Z}^*_{N^2} \subset \mathcal{Z}_{N^2}$ denote the set of non-negative integers that have multiplicative inverse modulo $N^2$. We choose $g \in \mathcal{Z}^*_{N^2}$ satisfying $\gcd(L(g^\lambda \mod N^2), N) = 1$, where $\lambda = \mathrm{lcm}(p-1, q-1)$ and $L(u) = \frac{u-1}{N}$. The public key is composed of the pair $(g, N)$, and $\lambda$ is defined as the private key. For security reasons, the length of $N$, i.e. $b_N \geq 1024$ bits. A message $m \in \mathcal{Z}_N$ is encrypted by

$$c = E(m, r) = g^m r^N \mod N^2 \tag{1}$$

where $c \in \mathcal{Z}_{N^2}$ denotes the ciphertext and $r \in \mathcal{Z}^*_N$ is the uniformly chosen key. Since $r$ is changeable, different ciphertexts could be generated even for the same plaintext $m$. Hence, the Paillier cryptosystem satisfies the so-called "*semantic security*". For notation convenience, we also write

$$c = E(m, r) \triangleq [[m]] \tag{2}$$

At the decryption phase, $m$ can be retained by

$$m = D(c, \lambda) = \frac{L(c^\lambda \mod N^2)}{L(g^\lambda \mod N^2)} \mod N \tag{3}$$

where $r$ is not needed.

The Paillier cryptosystem is said to be homomorphically additive because

$$D((E(m_1, r_1) \cdot E(m_2, r_2))) = m_1 + m_2 \tag{4}$$

## III. Proposed Image Homomorphic Encryption Scheme with Reduced Ciphertext Expansion

To achieve reduction of the ciphertext expansion, our idea is to encrypt only a subset of the pixels using Paillier, and relate the remaining pixels to these homomorphically encrypted ones. More specifically, let $\mathbf{f} = [f_1, f_2, \cdots, f_n]^T$ be the image to be encrypted. Without loss of generality, we assume that the image is 8-bit. We *randomly* divide the image into two parts: $\mathbf{f}_E = [f_{E,1}, f_{E,2}, \cdots, f_{E,m}]^T$ and $\mathbf{f}_R = [f_{R,1}, f_{R,2}, \cdots, f_{R,n-m}]^T$. Letting $\mathbf{C}$ and $\mathbf{D}$ be the associated extraction matrices, we have

$$\begin{aligned} \mathbf{f}_E &= \mathbf{Cf} \\ \mathbf{f}_R &= \mathbf{Df} \end{aligned} \tag{5}$$

where $\mathbf{C} \in \{0,1\}^{m \times n}$ and $\mathbf{D} \in \{0,1\}^{(n-m) \times n}$ are randomly generated according to a *public* key.

The first part $\mathbf{f}_E$ is treated as a sub-image, and each of its pixel is encrypted using Paillier. The encrypted $[[\mathbf{f}_E]]$ can be written as,

$$[[\mathbf{f}_E]] = \Big[ [[f_{E,1}]], [[f_{E,2}]], \cdots, [[f_{E,m}]] \Big]^T \tag{6}$$

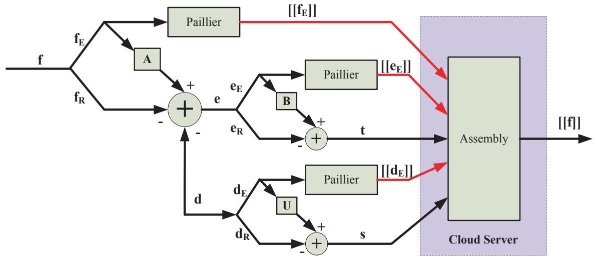

Fig. 1. Schematic diagram of the proposed scheme.

where semantic security is achieved by employing different $r$'s for different pixels. $[[\mathbf{f}_E]]$ forms one part of the ciphertext, as illustrated in Fig. 1.

For $\mathbf{f}_R$, we adopt a different strategy to encrypt. Motivated by the image interpolation in which one pixel is related to the others through linear estimation, we propose to relate the pixels in $\mathbf{f}_R$ with those in $\mathbf{f}_E$ via an interpolation-like form

$$\mathbf{e} = \mathbf{A}\mathbf{f}_E - \mathbf{f}_R - \mathbf{d} \tag{7}$$

where $\mathbf{e}$ represents the residual vector, $\mathbf{A} \in \{0,1\}^{(n-m) \times m}$ is the interpolation matrix, and $\mathbf{d}$ is an interference vector designed for security purpose. Each element of $\mathbf{d}$ is uniform randomly generated in $[0, 255]$. Plugging in (5) into (7) yields

$$\mathbf{e} = (\mathbf{AC} - \mathbf{D})\mathbf{f} - \mathbf{d} \tag{8}$$

Instead of sending $\mathbf{e}$ and $\mathbf{d}$ directly without any protection, we further process them in a similar fashion as that to encrypt $\mathbf{f}$. We first *randomly* partition $\mathbf{e}$ into two parts: $\mathbf{e}_E = [e_{E,1}, e_{E,2}, \cdots, e_{E,l}]^T$ and $\mathbf{e}_R = [e_{R,1}, e_{R,2}, \cdots, e_{R,n-m-l}]^T$, using a pair of extraction matrices $\mathbf{G}$ and $\mathbf{H}$. Namely,

$$\begin{aligned} \mathbf{e}_E &= \mathbf{Ge} \\ \mathbf{e}_R &= \mathbf{He} \end{aligned} \tag{9}$$

where $\mathbf{G} \in \{0,1\}^{l \times (n-m)}$ and $\mathbf{H} \in \{0,1\}^{(n-m-l) \times (n-m)}$.

Similarly, we can divide the interference vector $\mathbf{d}$ into two segments $\mathbf{d}_E$ and $\mathbf{d}_R$ with extraction matrices $\mathbf{J}$ and $\mathbf{K}$,

$$\begin{aligned} \mathbf{d}_E &= \mathbf{Jd} \\ \mathbf{d}_R &= \mathbf{Kd} \end{aligned} \tag{10}$$

where $\mathbf{J} \in \{0,1\}^{u \times (n-m)}$ and $\mathbf{K} \in \{0,1\}^{(n-m-u) \times (n-m)}$.

$\mathbf{e}_E$ and $\mathbf{d}_E$ are encrypted element-wise using Paillier to form the second part of the ciphertext, and their encrypted versions are denoted as $[[\mathbf{e}_E]]$ and $[[\mathbf{d}_E]]$, respectively. Similar to $\mathbf{f}_R$, the vectors $\mathbf{e}_R$ and $\mathbf{d}_R$ are related to $\mathbf{e}_E$ and $\mathbf{d}_E$ in the following interpolation-like form

$$\mathbf{t} = \mathbf{B}\mathbf{e}_E - \mathbf{e}_R \tag{11}$$

$$\mathbf{s} = \mathbf{U}\mathbf{d}_E - \mathbf{d}_R \tag{12}$$

where $\mathbf{B} \in \{0,1\}^{(n-m-l) \times l}$, $\mathbf{U} \in \{0,1\}^{(n-m-u) \times u}$, and no interference term is included. Plugging (9) and (10) respectively into (11) and (12) yields

$$\mathbf{t} = (\mathbf{BG} - \mathbf{H})\mathbf{e} \tag{13}$$

$$\mathbf{s} = (\mathbf{UJ} - \mathbf{K})\mathbf{d} \tag{14}$$

The residual vectors $\mathbf{t}$ and $\mathbf{s}$ form the third part of the ciphertext.

Note that the extraction matrices $\mathbf{C}$, $\mathbf{D}$, $\mathbf{G}$, $\mathbf{H}$, $\mathbf{J}$, $\mathbf{K}$, and the interpolation matrices $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{U}$, though randomly generated, are based on a public seed and hence, they are publicly accessible for the cloud server as well as the attacker. This implies that they do not need to be transmitted.

## IV. Analysis of the ciphertext expansion

The factor of ciphertext expansion $\rho$ is defined by

$$\rho = \frac{\text{size of the ciphertext}}{\text{size of the plaintext}} \tag{15}$$

Clearly, the size of the plaintext is $8n$ bits, where $n$ is the image size.

The ciphertext of our proposed scheme consists of five components: $[[\mathbf{f}_E]]$, $[[\mathbf{e}_E]]$, $[[\mathbf{d}_E]]$, $\mathbf{t}$ and $\mathbf{s}$. Noticing that each Paillier ciphertext is of length $2b_N$ bits, we can calculate $\rho$ by

$$\rho = \frac{2(l+m+u)b_N + b_t(n-m-l) + b_s(n-m-u)}{8n} \tag{16}$$

where $b_t$ and $b_s$ denote the number of bits needed to represent each element of $\mathbf{t}$ and $\mathbf{s}$, respectively, and they can be obtained on-the-fly upon getting the whole $\mathbf{t}$ and $\mathbf{s}$. Both $b_t$ and $b_s$ need to be sent to the cloud server. As their sizes are negligible, they are not included into the calculation of $\rho$.

## V. Obtaining the whole homomorphically encrypted image in the cloud

Upon receiving $[[\mathbf{f}_E]]$, $[[\mathbf{e}_E]]$, $[[\mathbf{d}_E]]$, $\mathbf{t}$ and $\mathbf{s}$, the cloud server attempts to obtain the whole encrypted image $[[\mathbf{f}]]$, prior to applying any homomorphic operations over the encrypted data.

With $[[\mathbf{e}_E]]$ and $\mathbf{t}$ in hand, the cloud server can calculate $[[\mathbf{e}_R]]$ element-wise according to (11) by

$$[[\mathbf{e}_R(i)]] = \prod_{j=1}^{l} ([[\mathbf{e}_E(j)]])^{\mathbf{B}_{ij}} ([[\mathbf{t}(i)]])^{-1} \mod N^2 \tag{17}$$

where $\mathbf{x}(i)$ denotes the $i$th element of a vector $\mathbf{x}$. By combining $[[\mathbf{e}_E]]$ and the generated $[[\mathbf{e}_R]]$, we can form the whole $[[\mathbf{e}]]$.

Similarly, we can derive

$$[[\mathbf{d}_R(i)]] = \prod_{j=1}^{u} ([[\mathbf{d}_E(j)]])^{\mathbf{U}_{ij}} ([[\mathbf{s}(i)]])^{-1} \mod N^2 \tag{18}$$

which can be combined with $[[\mathbf{d}_E]]$ to form the whole $[[\mathbf{d}]]$. Furthermore, the cloud server can reconstruct $[[\mathbf{f}_R]]$ element-wise through

$$[[\mathbf{f}_R(i)]] = \prod_{j=1}^{m} ([[\mathbf{f}_E(j)]])^{\mathbf{A}_{ij}} ([[\mathbf{e}(i)]])^{-1} ([[\mathbf{d}(i)]])^{-1} \mod N^2 \tag{19}$$

As the extraction matrices $\mathbf{C}$ and $\mathbf{D}$ are public, it is straightforward to form the whole encrypted image $[[\mathbf{f}]]$ by combining $[[\mathbf{f}_E]]$ and $[[\mathbf{f}_R]]$.

## VI. Security analysis

In this section, we present the security analysis of the proposed encryption scheme with reduced ciphertext expansion. In our threat model, the cloud sever is considered as the adversary, who attempts to disclose the original image $\mathbf{f}$ based on all the available information.

When applying Paillier, the parameter $r$ is different for each element encrypted. This implies that the only applicable attack model is the ciphertext-only attack. Noticing the linear relationship in (13) and (14), a feasible strategy of estimating the vectors $\mathbf{e}$ and $\mathbf{d}$ from the available $\mathbf{t}$ and $\mathbf{s}$ is

$$\hat{\mathbf{e}} = (\mathbf{BG} - \mathbf{H})^{\dagger}\mathbf{t} \tag{20}$$

$$\hat{\mathbf{d}} = (\mathbf{UJ} - \mathbf{K})^{\dagger}\mathbf{s} \tag{21}$$

where $(\cdot)^{\dagger}$ denotes the matrix pseudoinverse, and $\hat{\mathbf{e}}$ and $\hat{\mathbf{d}}$ are optimal estimates in the least-square sense.

The estimated $\hat{\mathbf{e}}$ and $\hat{\mathbf{d}}$ can be further utilized to estimate the original signal $\mathbf{f}$ according to the linear relationship presented in (8), namely,

$$\hat{\mathbf{f}} = (\mathbf{AC} - \mathbf{D})^{\dagger}(\hat{\mathbf{e}} + \hat{\mathbf{d}}) \tag{22}$$

However, when applying the above simple attack strategy, we neglect some important information inherent to the image signal. For instance, image signal satisfies the smoothness prior, and each pixel value is bounded by $[0, 255]$, which cannot be guaranteed by (22). To more thoroughly evaluate the strength of our proposed encryption scheme, we go beyond the naive estimation in (22), and build up the more powerful total variation (TV)-based estimation framework, integrating all the prior information available

$$\begin{aligned} &\min_{\mathbf{f}} \ \frac{\tau}{2}\|\hat{\mathbf{e}} + \hat{\mathbf{d}} - (\mathbf{AC} - \mathbf{D})\,\mathbf{f}\|_2^2 + \|\mathbf{f}\|_{TV} \\ &\text{s.t. } 0 \preceq \mathbf{f} \preceq 255 \end{aligned} \tag{23}$$

The cost function integrates the linear relationship in (8), (13), and (14), and the smoothness prior. The constraint guarantees that each estimated pixel value must be within $[0, 255]$, where $\preceq$ denotes element-wise inequality. Such TV-based optimization problem has been extensively studied in image restoration scenarios, and can be efficiently solved using the split Bregman algorithm [17].

## VII. Experimental Results

The proposed system is implemented using C++ under the Ubuntu platform. NTL and GNU Multi-Precision libraries are used to process integers with arbitrary length. The modulo $N$ in the Paillier cryptosystem is set to be 1024 bits.

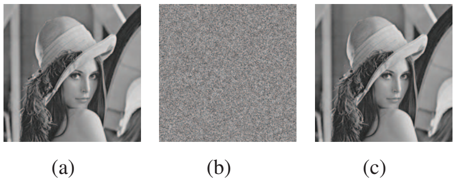

Fig. 2. (a) original; (b) encrypted in the Cloud; (c) decrypted

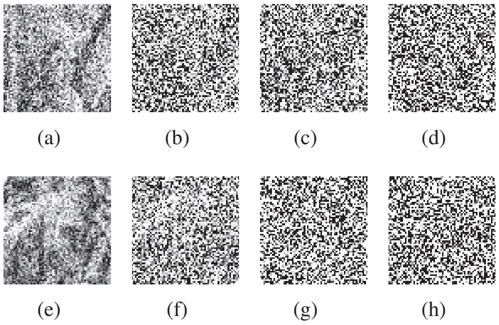

Fig. 3. Reconstruction results of Lena and Barbara. (a), (e) $L = 0.001n$; (b), (f) $L = 0.003n$; (c), (g) $L = 0.005n$; (d), (h) $L = 0.007n$

We first verify the correctness of the encryption/decryption modules. The Lena image is encrypted using our scheme presented in Section 3. The whole homomorphically encrypted image is obtained by applying the method described in Section 4, and then a standard Paillier decryption engine with the private key is employed to decrypt the generated $[[\mathbf{f}]]$. As can be seen from Fig. 2, an error-free image can be successfully decrypted from $[[\mathbf{f}]]$, demonstrating the correctness of the encryption-decryption loop. We also have tried many other test images, and similar observations can be retained.

We then conduct the experiments to demonstrate the ciphertext expansion factor, and the corresponding security level indicated by the reconstruction quality of solving (23). We set $l = m = u = L$, and perform the TV reconstruction algorithm for different $L$'s. Due to the page limit, we in Fig. 3 show the results of only two test images Lena and Barbara. It can be seen that when $L$ is very small, e.g., $L = 0.001n$, where $n$ is the image size, the TV-based attack can reconstruct a roughly recognizable image, demonstrating the effectiveness of this attack approach. As $L$ gradually increases, the reconstruction quality becomes worse. When $L \geq 0.005n$, the resulting images from the TV-based attack can hardly convey any useful visual information. For both Lena and Barbara, 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. We have tried other 8 test images, and similar conclusion could be made. In our forthcoming work, we plan to test all the 1338 images in the UCID data base to draw more convincing conclusions.

## VIII. Conclusions

We have investigated the strategy of reducing the ciphertext expansion in image homomorphic encryption. To this end, we have proposed to randomly select a subset of pixels to be encrypted by using the traditional homomorphic cryptosystem. The remaining pixels are encrypted by relating them with this random subset via a linear interpolation technique. Experimental results have shown that our proposed scheme is secure, and can achieve reduction of ciphertext expansion of factor around 36, while perfectly preserving the homomorphic property.

## IX. Acknowledgments

This work was supported in part by the Macau Science and Technology Development Fund under grants FDCT/009/2013/A1 and FDCT/046/2014/A1, in part by the Research Committee at University of Macau under grants MRG007/ZJT/2015/FST, MRG021/ZJT/2013/FST, MYRG2014-00031-FST and MYRG2015-00056-FST, and in part by the National Science Foundation of China under grant 61402547.

## References

[1] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, “Image feature extraction in encrypted domain with privacy-preserving sift,” *IEEE Trans. on Image Proc.*, vol. 21, no. 11, pp. 4593–4607, 2012.

[2] C. Aguilar Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, “Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain,” *IEEE Sig. Proc. Mag.*, vol. 30, no. 2, pp. 108–117, 2013.

[3] R. L. Lagendijk, Z. Erkin, and M. Barni, “Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation,” *IEEE Sig. Proc. Mag.*, vol. 30, no. 1, pp. 82–105, 2013.

[4] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169–180, 1978.

[5] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Advances in Cryptology (EUROCRYPT'99)*. Springer, 1999, pp. 223–238.

[6] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Trans. on Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[7] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “(leveled) fully homomorphic encryption without bootstrapping,” in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. ACM, 2012, pp. 309–325.

[8] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, “Privacy-preserving face recognition,” in *Proc. of the 9th Int. Symp. on Privacy Enchancing Technologies*. Springer, 2009, pp. 235–253.

[9] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva *et al.*, “A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates,” in *Proc. the 4th IEEE Int. Conf. on Biometrics Compendium*. IEEE, 2010, pp. 1–7.

[10] J. R. Troncoso-Pastoriza and F. Pérez-González, “Efficient zero-knowledge watermark detection with improved robustness to sensitivity attacks,” *EURASIP J. on Inf. Security*, vol. 2007, pp. 1–14, 2007.

[11] 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.

[12] T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage-efficient processing of encrypted signals,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 180–187, 2010.

[13] ——, “On the implementation of the discrete fourier transform in the encrypted domain,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 86–97, 2009.

[14] P. Zheng and J. Huang, “Discrete wavelet transform and data expansion reduction in homomorphic entrypted domain,” *IEEE Trans. Image Proc*, vol. 22, no. 6, pp. 2455–2468, 2013.

[15] ——, “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.

[16] Y. Li, J. Zhou, and Y. Li, “Ciphertext-only attack on an image homomorphic encryption scheme with small ciphertext expansion,” in *Proc. of the 21st ACM Int. Conf. on Multimedia (MM’15)*. ACM, 2015, in press.

[17] 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.