A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DFT Encrypted Domain

Jiangtao Dong and Jingbing Li

Abstract In order to protect personal information, numerous works has been done in watermarking field. However, there still leaves some problems to be solved: (1) most of the watermarking methods were processed in the plaintext domains, which leave latent risk of exposing host image information, thus it is needed to encrypt the host image and process the watermarking scheme in the encrypted domain; (2) numerous image encryption methods had been searched, while not all of them can meet the robustness requirements when applied in the encrypted domain; (3) for some special fields of watermarking applications, medical images, for example, image integrity is an important criterion that should be strictly taken into account. Thus, that kind of watermarking methods which applies by modifying the pixel values are not suitable in this situation. In order to achieve information hiding in such kind of images, special techniques which do not change image integrity is needed. (4) By utilizing homomorphic encryption scheme, one can process watermark extraction without decrypting the encrypted watermarked image first, while it cost too much time in image encryption and decryption, the computational speed need to be improved. Based on the points mentioned above, we proposed a robust zero-watermarking scheme in the DWT-DFT encrypted domain, which embeds and extracts watermark without modifying the pixel values. Firstly, we encrypted both original medical image and watermark image. Then, we extract the DWT-DFT low frequency coefficients as encrypted medical images' feature vector. In watermark embedding and extraction phases, we adopt zero-watermarking technique to ensure integrity of medical images. Taking "db2" wavelet transform for example, we conduct the experiments on the visual quality and robustness of our watermarking scheme. Experimental results demonstrate that our algorithm achieves not only good watermarking robustness, but also ideal computation speed in the homomorphic encrypted domain.

J. Dong · J. Li (✉)
College of Information Science and Technology, Hainan University, Haikou, China
e-mail: jingbingli2008@hotmail.com

J. Dong
e-mail: jiangtao.dong@hotmail.com

Y.-W. Chen et al. (eds.), *Innovation in Medicine and Healthcare 2016*,
Smart Innovation, Systems and Technologies 60,
DOI 10.1007/978-3-319-39687-3_19

Keywords Robustness · Zero-watermarking · Feature vector · Homomorphic cryptosystem · DWT-DFT encrypted domain

1 Introduction

Medical image is a special kind of image which contains lots of patients' information, whose security should be seriously taken into account. Digital watermarking has been proposed as a possible brick of information protection systems, providing a means to embed a unique code into each copy of the distributed content. However, application of watermarking for multimedia content protection in realistic scenarios poses several security issues [1]. In most previously proposed image watermarking schemes, the embedding and extraction of a watermark often processed in the plaintext domain, which only protect the watermark information while ignoring the security of host image. When watermarking is processed by a third party, for example, an cloud sever, there leaves a latent risk of exposing the raw data.

Cryptosystems play an important role for the afore mentioned problem, i.e., to process the watermark in the encrypted domain. However, not all cryptosystems are appropriate for signal processing in the encrypted domain. Most cryptosystems, such as data encryption standard (DES) and advanced encryption standard (AES), do not retain the algebraic relations among the plaintexts after encryption [2, 3]. A special kind of cryptosystems, the homomorphic cryptosystems, are able to keep the algebraic structure of the plaintext, and thus are particularly suitable for this purpose.

Current solutions based on homomorphic encryption offer provable security at the price of a very high complexity [4]. Here, the bottleneck is the secure embedding module, since all watermarked features have to be encrypted using a costly homomorphic cryptosystem. As an example, in [5] it is reported that on a 1,024 × 1,024 image secure embedding takes about 2 min using a standard personal computer. Hanaa et al. [6] proposed a homomorphic block-based KLT image watermarking which works by segmenting the reflectance component of the host image into blocks by using spiral scan and adding the watermark to every block during the application of the KLT to each block, separately. Li et al. [7] proposed a novel CDWM scheme based on homomorphic encryption and dirty paper precoding. They introduced a decryption module before watermark detection to create some nonlinearity and thereby inhibit conventional watermark attacks based on linear operations. Zheng et al. [8] proposed a new signal processing procedure, where the multiplicative inverse method is employed as the last step to limit the data expansion. Bianchi et al. [9] conducted an investigation on the implementation of the discrete Fourier transform (DFT) as well as the fast Fourier transform (FFT) on encrypted signals. A Walsh-Hadamard transform-based image watermarking scheme was proposed in [10], which possesses the character of blind watermark extraction, in both the decrypted domain and the encrypted domain.

In this paper, we propose a robust zero-watermarking algorithm for medical images in the DWT-DFT encrypted domain. In Sect. 2, we introduce the fundamental theory. In Sect. 3, we discuss the zero-watermarking scheme in the DWT-DFT encrypted domain. In Sect. 4, we discuss the robustness of our algorithm under various kinds of attacks based on experimental results, and compared the watermarking methods between plaintext domain and encrypted domain. Finally, we conclude our paper in Sect. 5.

2 The Fundamental Theory

In this section, we will give an introduction to the homomorphic cryptosystem and the implementation of DWT and DFT in the encrypted domain. Since DWT cannot resist the geometric attacks, such as scaling and rotation [11], we combine the DWT-DFT hybrid approach to improve the robustness of our watermarking algorithm.

2.1 Paillier Homomorphic Encryption

In 1978, Rivest et al. first introduced an idea of homomorphic encryption which permits encrypted data to be manipulated without preliminary decryption [12]. It provides a suitable way for secure signal processing, since it retains the algebraic relations among the plaintext after encryption, so that an algebraic operation on the ciphertexts is corresponding to another operation on the plaintexts. The Paillier cryptosystem [13] is a public key cryptosystem with both the homomorphic property and probabilistic property [14]. It is a partial homomorphic cryptosystem, in which only addition or multiplication homomorphism can be achieved.

The reason why we can use the Paillier cryptosystem to encrypt an image is that the Paillier cryptosystem is a homomorphic cryptosystem. Most of the implementations of secure signal processing are based on the homomorphic properties. And the security of Paillier cryptosystem has been proved. There are also a few kinds of secure signal processing techniques based on the Paillier cryptosystem, such as DWT and DCT in the encrypted domain [15]. Our watermarking scheme is based on such transformations in the encrypted domain.

2.2 Non-parametric Probabilistic Models

DWT is a wavelet transform for which the wavelets are sampled at discrete intervals. It provides a simultaneous spatial and frequency domain information of the image. In DWT operation, an image can be analyzed by the combination of analysis

filter bank and decimation operation. The analysis filter bank consists of a pair of low and high pass filters corresponding to each decomposition level. The low pass filter extracts the approximate information of the image whereas the high pass filter extracts the details such as edges. The application of 2D DWT decomposes the input image into four separate sub-bands: low frequency components in horizontal and vertical direction directions (cA), low frequency component in the horizontal and high frequency component in the vertical direction (cV), high frequency component in the horizontal and low frequency component in the vertical direction (cH) and high frequency component in horizontal and vertical directions (cD). cA, cV, cH and cD can also be represented as LL, LH, HL and HH respectively.

The decomposing equation of the Mallat algorithm can be defined as follows:

$$W_{\varphi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \varphi_{j_0, m, n}(x, y) \tag{1}$$

$$W_{\Psi}(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \varphi^{i}_{j, m, n}(x, y), i = \{H, V, D\} \tag{2}$$

In this paper, we adopt the 'db2' wavelet, and process the original medical image within just one layer decomposition in order to maintain sufficient computational speed.

2.3 Implementation of DFT in the Encrypted Domain

The Discrete Fourier Transform is a signal analysis theory. The M × N medical images' DFT is done by using:

$$\begin{aligned} &F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cdot e^{-j2\pi xu/M} e^{-j2\pi yv/N} \\ &u = 0, 1, \ldots, M-1 \; ; \; v = 0, 1, \ldots, N-1 \end{aligned} \tag{3}$$

The M × N medical images' Inverse Discrete Fourier Transform (IDFT) is defined by:

$$\begin{aligned} &f(x, y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)} \\ &x = 0, 1, \ldots, M-1; \; y = 0, 1, \ldots, N-1 \end{aligned} \tag{4}$$

where $f(x, y)$ corresponds to the value of the medical image at point (x, y) and $F(u, v)$ matches the DFT coefficient at point (u, v) in frequency domain. Digital images are usually expressed in pixels square, so we set $M = N$.

2.4 Non-parametric Probabilistic Models

The Logistic map is one of the most famous 1D chaotic maps. It is a simple dynamic nonlinear return with complex chaotic behavior so that we can reproduce it if we have its parameters and initial values. Its mathematical definition can be expressed in the following equation:

$$x_{k+1} = x_k(1 - x_k) \tag{5}$$

where $0 \leq \mu \leq 4$ and $x_k \in (0, 1)$ are the system variable and parameter respectively, and k is the number of iteration.

Logistic Map system works under chaotic condition when $3.569945 \leq \mu \leq 4$. It can be seen that a small difference in initial conditions would lead to a significant difference of chaotic sequences. These statistical characteristics are the same as white noise, so the above sequence is an ideal secret-key sequence. In this paper, we set $\mu = 4$, and the chaotic sequences are generated by different initial values.

3 The Algorithm

In this section, we propose a robust image zero-watermarking scheme in the DWT-DFT encrypted domain. As shown in Fig. 1, the original image I is firstly encrypted by the homomorphic cryptosystem. A scrambled watermark image E[w] is generated from a Logistic sequence $Y(j)$. The watermark embedding is performed in the encrypted domain by a third party, e.g. a cloud server. In order to ensure information security, we have to make sure that the watermark provided to the server is an encrypted binary sequence consists of 0 and 1. Each watermark bit is encrypted separately. Based on the homomorphic property of the cryptosystem, the output of watermark embedding procedure would be an encrypted version of the watermarked image, $E[I_w]$. After decryption, the user can acquire the decrypted image which can meets application requirements.

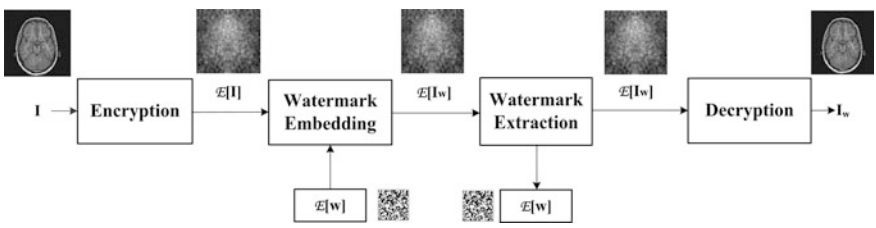

Fig. 1 Watermarking scheme in the encrypted domain

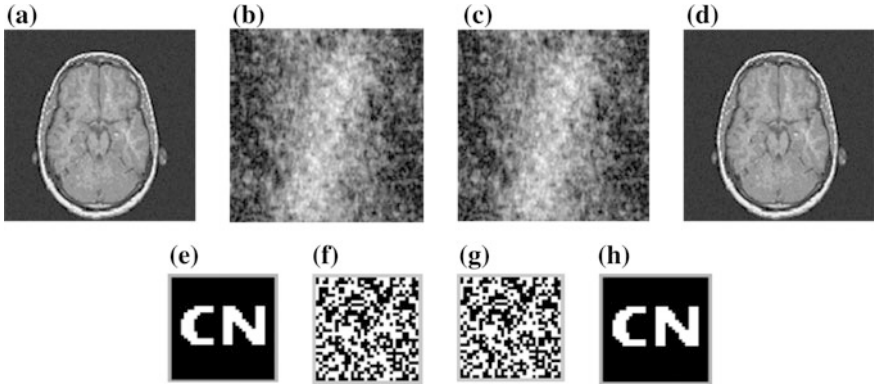

Fig. 2 Watermarking in the encrypted domain: **a** the original medical image "mir-1", **b** encrypted "mir-1" image, **c** watermarked image, **d** decrypted watermarked image, **e** original watermark, **f** plaintext domain extraction, **g** encrypted domain extraction and **h** decrypted watermarking robustness performance

3.1 Encryption Algorithm of the Original Medical Images

In order to protect the original medical images, we conduct our watermarking algorithm in the encrypted domain. Figure 2 illustrates the encryption scheme for medical images, detailed encryption scheme are described as follows:

Step 1: Perform DWT on the original medical images to acquire the cA, cH, cV and cD sub-band wavelet coefficients.
Step 2: Apply DFT on each wavelet sub-band coefficients cA, cH, cV and cD to decompose the sub-band coefficients.
Step 3: Encrypt all the decomposed sub-band coefficients by dot multiplication operation with a binary matrix C (i, j) generated from a Logistic sequence X(j).
Step 4: Perform inverse DFT (IDFT) on each coefficients to reconstruct the sub-band.
Step 5: Perform inverse DWT (IDWT) on the reconstructed coefficients to acquire the encrypted medical images.

3.2 Acquire the Feature Vector of Encrypted Medical Images

Taking both the robustness and visual quality into account, we extracted the low-frequency coefficients after applying DWT-DFT hybrid operation. The implementation is given as:

Step 1: Perform DWT on the original medical images to acquire the cA, cH, cV, cD sub-band wavelet coefficients;

$$\{\text{cA, cH, cV, cD}\} = \text{DWT2}\left(\text{I}(i,j)\right) \tag{6}$$

Step 2: Apply DFT to the low frequency coefficients cA(i,j);

$$\text{cA}'\left(i,j\right) = \text{DFT2}\left(\text{cA}(i,j)\right) \tag{7}$$

Step 3: Extract the low and middle frequency coefficients of DFT matrix cA′(i, j), after binary processing represented in Eq. (8), we can obtain a binary sign sequence of coefficients as the feature vector V(j).

$$\text{sgn}(x) = \begin{cases} 1, & x(i,j) \geq 0 \\ 0, & x(i,j) < 0 \end{cases} \tag{8}$$

$$\text{V}(j) = \text{sign}(\text{cA}'\left(i,j\right)) \tag{9}$$

As shown in Table 1. After numerous experiments, we found that the value of DWT-DFT low-frequency coefficients may change after attacking the encrypted image, while the signs of the coefficients still remain unchanged. Let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient. We can obtain the sign sequence of low-frequency coefficients, as shown in the column "Sequence of coefficient signs" in Table 1. After attack, the sign sequence is unchanged, and the Normalized Cross-correlation (NC) is equal to 1.0. Thus we can adopt the coefficient signs as the feature vector of the encrypted medical images.

3.3 Watermark Embedding Algorithm in the Encrypted Domain

Medical image is a special kind of image which strictly requires image integrity. Thus, we adopt the zero-watermarking technique to finish watermark embedding. During the process, we embed the watermark by correlating image feature vector and the encrypted watermark ew(j), rather than by modifying the image pixel values. Note that, once the key is generated, the watermark is embedded in. The watermark embedding algorithm are described as follows:

Step 1: Extract the encrypted medical image's feature vector V(j) through DWT-DFT transform.

Step 2: Watermark scrambling. Firstly, we generate a binary logistic sequence L(j) by using Logistic map; After that, perform hash XOR operation

Table 1 Change of DWT-DFT coefficients under different attacks for encrypted medical images

Image processing	PSNR (dB)	C(1, 1)	C(1, 2)	C(1, 3)	C(1, 4)	C(1, 5)	Sequence of coefficient signs	NC
Encrypted image without attacks	90.21	7.04 + 0.00i	−2.40 − 0.07i	0.11 + 0.06i	−0.21 + 0.02i	−0.25 − 0.01i	11 00 11 01 00	1.00
Gaussian noise (3 %)	16.02	7.31 + 0. 00i	−2.24 − 0.08i	0.17 + 0.04i	−0.17 + 0.04i	−0.22 − 0.01i	11 00 11 01 00	1.00
JPEG compression (30 %)	19.27	4.98 + 0.00i	−2.09 − 0.07i	0.33 + 0.05i	−0.15 + 0.01i	−0.15 − 0.00i	11 00 11 01 00	1.00
Median filter [3 × 3] (10 times)	24.83	6.96 + 0.00i	−2.44 − 0.07i	0.09 + 0.06i	−0.21 + 0.02i	−0.24 − 0.01i	11 00 11 01 00	1.00
Rotation (clockwise, 2°)	19.78	7.02 + 0.00i	−2.39 − 0.08i	0.07 + 0.07i	−0.18 + 0.01i	−0.27 − 0.00i	11 00 11 01 00	1.00
Scaling (× 0.5)	–	1.76 + 0.00i	−0.62 − 0.02i	0.02 + 0.01i	−0.06 + 0.00i	−0.06 − 0.00i	11 00 11 01 00	1.00
Translation (5 %, down)	15.94	6.98 + 0.00i	−2.39 − 0.07i	0.11 + 0.06i	−0.21 + 0.02i	−0.25 − 0.01i	11 00 11 01 00	1.00
Cropping (5 %, Y direction)	–	6.99 + 0.00i	−2.39 − 0.07i	0.11 + 0.06i	−0.21 + 0.02i	−0.25 − 0.01i	11 00 11 01 00	1.00
DWT-DFT transform coefficient unit: 1.0e + 005								

between L(j) and the original watermark w(j) to acquire the scrambled watermark ew(j).

$$\mathrm{ew}(j) = \mathrm{w}(j) \oplus \mathrm{L}(j) \tag{10}$$

Step 3: Generate the Key(j). Employ hash XOR operation between V(j) and ew (j) to acquire Key(j).

$$\mathrm{Key}(j) = \mathrm{ew}(j) \oplus \mathrm{V}(j) \tag{11}$$

3.4 Watermark Extraction Algorithm in the Encrypted Domain

The implementation of watermark extraction in the encrypted domain can be described as:

Step 1: Perform DWT-DFT on the test image to extract its feature vector V′(j).
Step 2: Employ hash XOR operation between $V'(j)$ and Key(j) to extracted the scrambled watermark $ew'(j)$.
Step 3: Watermark recovery. Decrypt the watermark by applying XOR operation between ew′(j) and the binary Logistic sequence Y(j), so we can get the decryption version of extracted watermark $w'(j)$.

3.5 Watermarking Evaluation

We use the peak signal-to-noise ratio (PSNR) value to evaluate the visual quality of the watermarked images, and the robustness of the scheme is measured by the Normalized Cross-correlation (NC), which can be described as follows:

$$\mathrm{NC} = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j W^2(i,j)} \tag{12}$$

After detecting W′(i,j), compute the NC values between W (i,j) and W′(i,j) to determine whether the watermark is embedded in.

The Peak Signal to Noise Ratio (PSNR) is used for measuring the distortion of the watermarked image, which is defined as:

$$PSNR = 10\lg\left[\frac{MN\max_{i,j}(\mathrm{I}(i,j))^2}{\sum_i\sum_j(\mathrm{I}(i,j)-\mathrm{I}'(i,j))^2}\right] \quad (13)$$

where I(*i*,*j*) and I′(*i*,*j*) denote the pixel grey values of the coordinates (*i*,*j*) in the original images and the watermarked images respectively; M, N represents the image row and column numbers of pixels respectively.

4 Experiments

In our experiment, we select the tenth slice of one medical volume medical data as the original medical image (128 × 128) and choose a significant binary image (32 × 32) as the original watermark image. Figure 2a–d shows the original medical image, encrypted medical image. Figure 2e–h shows the original binary image $W = \{W(i,j)|W(i,j) = 0,\ 1;\ 1 \le i \le 32, 1 \le j \le 32\}$.The parameters for encrypting the binary watermark images are: $x_0 = 0.2$, $\mu = 4$; and $x_0' = 0.135$, $\mu' = 4$ for encrypting the medical images respectively. To verify our algorithm, we run the watermarking scheme on Matlab R2014a platform with a computer contains four Intel(R) Core i5-4590 CPUs at 3.30 GHz.

Experimental results are illustrated in Table 2, in which we compared the robustness performance of watermark attacks in the plaintext and encrypted domains. From the table, we can observe that the watermarking scheme in the encrypted domain achieves good robustness performance which is close to that in the plaintext domain.

To test the computational cost of our algorithm, we conduct our experiment in eight selected images. In the case of embedding a 32 × 32 watermark into a 128 × 128 × 8 bits' host image, the encryption time is about 0.2 s and the

Table 2 PSNR and NC values under watermark attacks in the DWT-DFT encrypted domain

Attacks	Parameters	PSNR		NC	
		Plaintext domain	Encrypted domain	Plaintext domain	Encrypted domain
Gaussian noise	5 %	14.68	13.98	0.71	0.88
JPEG	20 %	21.50	19.23	0.96	1.00
Median filter	[3 × 3],10 times	24.98	24.84	0.90	1.00
Rotation	4°	20.59	18.84	0.94	0.88
Scaling	×0.8	–	–	0.88	0.88
Translation	6 %	14.83	15.69	0.36	0.81
Cropping	10 %	–	–	0.61	0.81

decryption time is about 0.08 s. And the execution time of encrypted domain watermark embedding is about 0.25 s and the extraction time is about 0.05 s in the encrypted domain.

5 Conclusions

Most of the existing watermarking schemes were designed to embed the watermark information in the plaintext domain, which leaves a latent risk of exposing the host image. In this paper, we proposed a robust watermarking scheme in the DWT-DFT encrypted domain. The main contributions are listed as follows.

(1) The proposed watermarking algorithm in the DWT-DFT encrypted domain is robust against watermark attacks in the encrypted domain.
(2) We adopted the zero-watermarking technique to embed the watermark by correlating image feature vector with a logistic sequence, rather than by changing the image pixel values, thus it can be used in special conditions like medical images etc. that strictly requires image integrity.
(3) By utilizing our algorithm, the computational speed can easily meets practical requirements.

Acknowledgments This work was supported by National Natural Science Foundation of China (No.61263033), International Science and Technology Cooperation Project of China (NO. KJHZ 2015-04) and the Institutions of Higher Learning Scientific Research Special Project of Hainan province, China (NO. Hnkyzx2014-2).

References

1. Bianchi, T., Piva, A.: Secure watermarking for multimedia content protection: a review of its benefits and open issues. Sig. Process. **30**(2), 87–96 (2013)
2. Li, S., Chen, G., Cheung, A., Bhargava, B., Lo, K.-T.: On the design of perceptual MPEG video encryption algorithms. IEEE Trans. Circ. Syst. Video Technol. **17**, 214–223 (2007)
3. Zhang, G., Liu, Q.: A novel image encryption method based on total shuffling scheme. Opt. Commun. **284**, 2775–2780 (2011)
4. Rial, A., Deng, M., Bianchi, T., Piva, A., Preneel, B.: A provably secure anonymous buye-seller watermarking protocol. IEEE Trans. Inform. Forensics Sec. **5**(4), 920–931 (2010)
5. Deng, M., Bianchi, T., Piva, A., Preneel, B.: An efficient buyer-seller watermarking protocol based on composite signal representation. In: Proceedings of 11th ACM Workshop Multimedia and Security, pp.9–18. Princeton, NJ (2009)
6. Abdallah, Hanaa A., Faragallah, Osama S., Elsayed, Hala S., et al.: Robust image watermarking method using homomorphic block-based KLT. Optik **127**(4), 2374–2381 (2016)
7. Li, Z., Zhu, X., Lian, Y., et al.: Constructing secure content-dependent watermarking scheme using homomorphic encryption. IEEE Int. Conf. Multimedia Expo, 627–630 (2007)

8. Zheng, Peijia, Huang, Jiwu: Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. IEEE Trans. Image Process. **22**(6), 2455–2468 (2013)
9. Bianchi, T., Piva, A., Barni, M.: On the implementation of the discrete Fourier transform in the encrypted domain. IEEE Trans. Inf. Forensics Secur. **4**(1), 86–97 (2009)
10. Zheng, P., Huang, J.: Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking. In: Proceedings of 14th Information Hiding Conference, pp. 240–254 (2012)
11. Kang, X., Huang, J., Shi, Y., Lin, Y.: A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE Trans. Circ. Syst. Video Technol. **13** (8), 776–786 (2003)
12. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. Found. Secure Comput. **4**(11), 169–180 (1978)
13. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. Advances in Cryptology—EUROCRYPT' 99, pp. 223–238. Springer(1999)
14. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984)
15. Failla, P., Sutcu, Y., Barni, M.: Esketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics. In: Proceedings of the 12th ACM Workshop on Multimedia and Security, ACM, pp.241–246 (2010)