Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 3219042, 7 pages
http://dx.doi.org/10.1155/2016/3219042

Research Article

A Privacy-Preserving Outsourcing Data Storage Scheme with Fragile Digital Watermarking-Based Data Auditing

Xinyue Cao,[1] Zhangjie Fu,[1,2] and Xingming Sun[1,2]

[1]*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China*
[2]*Jiangsu Engineering Centre of Network Monitor, Nanjing University of Information Science and Technology, Nanjing 210044, China*

Correspondence should be addressed to Xingming Sun; sunnudt@163.com

Received 9 December 2015; Revised 6 March 2016; Accepted 12 April 2016

Academic Editor: Isao Echizen

Cloud storage has been recognized as the popular solution to solve the problems of the rising storage costs of IT enterprises for users. However, outsourcing data to the cloud service providers (CSPs) may leak some sensitive privacy information, as the data is out of user's control. So how to ensure the integrity and privacy of outsourced data has become a big challenge. Encryption and data auditing provide a solution toward the challenge. In this paper, we propose a privacy-preserving and auditing-supporting outsourcing data storage scheme by using encryption and digital watermarking. Logistic map-based chaotic cryptography algorithm is used to preserve the privacy of outsourcing data, which has a fast operation speed and a good effect of encryption. Local histogram shifting digital watermark algorithm is used to protect the data integrity which has high payload and makes the original image restored losslessly if the data is verified to be integrated. Experiments show that our scheme is secure and feasible.

1. Introduction

With the development of cloud computing, outsourcing data to cloud storage servers has become a popular way for firms and individuals. Cloud storage reduces data storage and maintenance costs. And cloud storage can provide a flexible and convenient way for users to access their data anywhere. However, the cloud service providers (CSPs) may not be honest and the data should not be disclosed to the CSPs. So the data must be encrypted before it is uploaded to the cloud. Encryption is a fundamental method to preserve data confidentiality. For privacy preserving concerned, data owner can encrypt the data before outsourcing it to CSPs. Many problems of querying over encrypted domain are discussed in research literatures [1–3]. In addition, data owners worry whether the outsourcing data is modified or revealed by the CSPs. It is necessary to add the data auditing service in outsourcing data storage scheme.

In the existing outsourcing data storage schemes, the data auditing methods can be classified into three categories: message authentication code- (MAC-) based methods, RSA-based homomorphic methods, and Boneh-Lynn-Shacham signature- (BLS-) based homomorphic methods [4]. In these methods, the data is calculated using MAC or digital signature and the verification information needs to be attached to the original data. If the data is digitally signed, any change in the data after signature invalidates the signature. Furthermore, these methods increase the data sizes and the time to sign, which is inconvenient in digital media (images, video, audio, etc.). So we use digital watermarking technology to offset the deficiency. Digital watermarking technology hides watermark information in the digital media without affecting data utilization. And it reduces the communication and computation costs. This means digital watermarking technology can provide a more effective auditing method than other cryptographic protocols for auditing.

Many works on outsourcing data storage schemes with digital watermarking are proposed. N. Singh and S. Singh [5] point out that collaboration of digital watermarking and cloud computing can significantly increase the robust of system as well as security of user's data. Boopathy and Sundaresan [6] propose a model of data storage and access process with digital watermarking technology in the cloud. Though they do not give concrete realization, it shows the broad

prospects of applying digital watermarking technology into the cloud environment. In addition, digital watermarking technology is used for data auditing in cloud environment. Wang and Lian [7] focus on the application scenarios of multiwatermarking in cloud environment by investigating the secure media distribution models. Ren et al. [8] propose a provable data possession scheme based on self-embedded digital watermark for auditing service. However, they do not provide privacy preserving with encryption methods. It is believed that supporting privacy preserving is of vital importance to outsourcing data storage.

In this paper, logistic map-based chaotic cryptography algorithm is used to preserve the privacy of outsourcing data, which has a fast operation speed and a good effect of encryption. Traditional encryption techniques such as AES, DES, and RSA have low speed to encrypt media data. And they are not suitable for high real time in media data transmission. Chaotic cryptography has many good characteristics such as sensitivity to initial value, pseudorandom properties, and ergodicity. Logistic map-based chaotic cryptography is a simple nonlinear model, but it has complex dynamics, which is widely used in image encryption. In this paper, logistic map-based chaotic cryptography method is used to permute the positions of the image pixels in the spatial domain. It is suitable for embedding watermark information with local histogram shifting digital watermark algorithm later. Local histogram shifting digital watermark algorithm is utilized to protect the data integrity. It has high payload and makes the original image restored losslessly if the data is verified to be integrated.

We propose an outsourcing data storage scheme supporting auditing service by using fragile digital watermarking technology. Meanwhile, the scheme uses encryption methods to preserve privacy. In this scheme, digital watermarking technology and encryption methods are used to enhance the integrity and privacy of outsourcing data storage. Our contributions are as follows.

(i) We propose an outsourcing data storage scheme supporting privacy-preserving and auditing service. In this scheme, we use the scrambling encryption algorithm based on logistic chaotic map, which has a fast operation speed and a good effect of encryption. Besides, local histogram shifting digital watermark algorithm [9] is used to embed the watermark, which has high payload and makes the original image restored losslessly if the data is verified to be integrated.

(ii) To reduce data owners' overhead cost, a third-party auditor (TPA) is used to verify the integrity of data in cloud. And TPA verifies the data integrity in encryption domain, which ensures the data confidentiality in the auditing process.

The rest of this paper is organized as follows. Section 2 summarizes the related work. Section 3 introduces the proposed scheme. Experiment results are given in Section 4. Section 5 concludes the paper and the future work.

2. Related Work

Many secure outsourcing data storage schemes are proposed these years. The privacy and integrity of data in cloud are the most concerns of data owners. Outsourcing data is often distributed geographically in different locations. CPSs can access the stored data if it is stored in plain format. Data owners have lost control over their data after it is uploaded to the cloud. So data privacy information [10] or sensitivity information [11] causes the outsourcing data to be encrypted in the data storage schemes.

To verify the data integrity, data auditing is considered in outsourcing data storage schemes. Ateniese et al. [12] first define the provable data possession (PDP) model for auditing service in untrusted storages. Juels and Kaliski Jr. [13] describe a proof of retrievability (POR) model, which ensures both "possession" and "retrievability" of data files. Sravan Kumar and Saxena [14] propose a proof of data integrity in the cloud, which could be agreed upon by both clients and the server via the Service Level Agreement (SLA). Hao et al. [15] propose the first protocol that provides public verifiability without TPA. Lu et al. [16] exploit the secure provenance model, which consists of the following modules: system setup, key generation, anonymous authentication, authorized access, and provenance tracking. Their scheme is based on the bilinear pairing techniques. And it records the ownership and the process history of data objects to increase the trust from public users. But all these methods have additional data to verify the data integrity and are not suitable for multimedia file. Digital watermarking technology can offset the deficiency, which is an effective method for data auditing. Digital watermarking can be divided into spatial domain and frequency domain [17]. Spatial domain digital watermark directly embeds watermark information into the image pixels. Frequency domain [18] algorithm embeds watermark information into coefficients of transform domain.

Encryption is a fundamental method to preserve data confidentiality in outsourcing data storage schemes. Digital watermarking technology is an effective method for data auditing. The methods of embedding digital watermark in encryption domain are proposed [6, 19, 20]. In medical domain, many healthcare information systems (HISs) [21] are proposed. Haas et al. [22] propose a privacy-protecting information system for controlled disclosure of personal data to third parties. This scheme uses authentic log files to check the completeness of data. And digital watermarking is used for tracing nonauthorized data disclosure. In the field of information hiding, Zhang [19] uses the simple encryption algorithm of exclusive-OR operation by a stream cipher and embedded watermark information by flipping the 3 LSBs of each encrypted pixel. Zhang [20] further proposes a scheme which makes watermark extraction independent from image decryption. That means a user can extract data from the encrypted image directly. Yin et al. [9] propose a scheme with the multigranularity encryption algorithm and local histogram shifting digital watermark algorithm, which ensures larger embedding capacity and better embedding quality. But chaotic-based scrambling encryption is widely used in

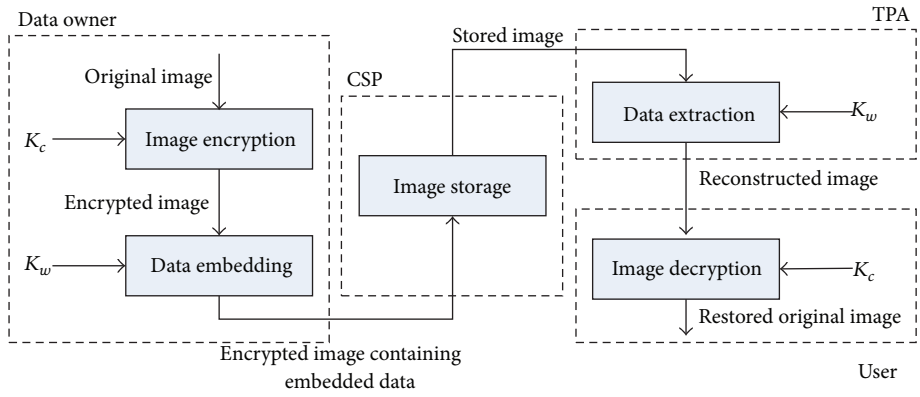

Figure 1: Sketch of the proposed scheme.

image encryption. The common encryption algorithms are one-dimensional logistic map, two-dimensional Smale and Henon map, and three-dimensional Lorenz map. The logistic map-based chaotic cryptography is a simple nonlinear model, but it has complex dynamics, which has good effect and fast speed.

In our scheme, we combine encryption technology with watermark technology. Data owner encrypts the image before transmission. CSP embeds some additional message into the encrypted image without knowing the original image content. TPA is required to extract the watermark from the encrypted image. A user can first decrypt the encrypted image containing watermark information with the decryption key and then extract the embedded watermark from the decrypted version with the extraction key. The transmission of encryption keys is assumed to be secure and is not discussed here. Here the logistic map-based chaotic cryptography method is used to permute the positions of the image pixels in the spatial domain. So the histogram of the encryption version is the same as the original image. The histogram statistical property makes the encryption method suitable for embedding watermark information with local histogram shifting digital watermark algorithm [9]. And this is a blind fragile watermark algorithm. The extraction of the watermark does not need the original image and original watermark information. Its error-free decryption can be used for military, remote sensing, and medicine data.

3. Proposed Scheme

In this section, we first analyze the framework of the system and then give the main steps of our scheme.

3.1. System Model. We first give the sketch of the proposed scheme in Figure 1. Then four parties in the scheme are described as follows.

(i) Data owner encrypts an original image with an encryption key K_c, computes a verification information as watermark information W for the encrypted image, embeds W to the encrypted image with the embedding key K_w, and upload the encrypted image to CSP.

(ii) CSP stores the watermark-embedded encrypted image.

(iii) TPA extract the watermarking information W' with K_w in the encrypted domain to verify the integrity and reconstructed the image if it is integrated.

(iv) Data user receives the reconstructed image from TPA and exactly decrypts the data to the original image with the decryption key K_c.

3.2. Main Steps of Proposed Scheme. The proposed scheme contains four modules: image encryption, watermarking embedding, watermarking extraction, and image decryption. The main steps of the proposed scheme are shown as follows.

3.2.1. Image Encryption. Data owner creates an original image I. Assume I is a gray image sized $M \times M$ pixels in uncompressed format.

The process of image encryption is as follows.

(i) Connect the jth row to the $(j-1)$th row, where $j = 2, 3, \ldots, M$, and generate the sequence of length $M \times M$.

(ii) Generate a chaotic sequence of length $M \times M$ with

$$x_{n+1} = x_n \times \mu \times (1 - x_n), \quad (1)$$

where $x_n \in (0, 1)$, $n = 0, 1, 2, \ldots$, $\mu \in (0, 4]$. x_0 is the initial value. n is the number of iterations. μ is growth parameter and when $\mu \in [3.5699456, 4]$, the generated sequence is in the state of pseudorandom distribution.

(iii) Sort the chaotic sequence and record the location set.

(iv) Scramble the sequence of image with the same location set.

The encryption key K_c consists of x_0 and μ. The encrypted image E is generated. This algorithm is simple and has good performance. The algorithm keeps the image histogram statistical properties.

3.2.2. Watermarking Embedding. The embedded watermarking information should be unpredictable and random. Arnold transforming or chaotic-based encryption can be used in this paper to improve the security of image watermarking algorithm. The above-mentioned encryption algorithm preserves the same image histogram statistical properties. Therefore, local histogram shifting watermarking algorithm is suitable for embedding data into the encrypted image [6].

When data owner embeds watermarking information W into the encrypted image E, the steps are as follows.

(i) Divide the encrypted image E into blocks $\{B_i\}_{i=1}^{N}$ of pixels in the size of $m \times m$. Two basic pixels $b_{i,L}$ and $b_{i,R}$ are randomly selected in each block B_i with the seed of random permutation k.

(ii) Calculate the difference $d_i = |b_{i,L} - b_{i,R}|$ to estimate the smoothness of each block. Blocks with smaller d_i are smoother than blocks with larger d_i. Blocks with smaller d_i have higher priority to be chosen for carrying data.

(iii) Determine the two peaks $(p_{i,L}, p_{i,R})$ in each block with

$$\begin{aligned} p_{i,L} &= \min\left(b_{i,L}, b_{i,R}\right) \\ p_{i,R} &= \max\left(b_{i,L}, b_{i,R}\right). \end{aligned} \tag{2}$$

If $p_{i,L} = p_{i,R}$, $p_{i,R} = p_{i,R} + 1$.

(iv) Saturated pixels q ($q = 0$ or $q = 255$) have to be preprocessed by modifying one grayscale unit. Then they will be recorded in a location map L to avoid saturated pixels from overflow or underflow during embedding process. Scan the pixels block by block and append bit "1" to L when $q \in \{1, 254\}$. Then append bit "0" to L when $q \in \{0, 255\}$ and modify q to q' using

$$q' = \begin{cases} 1, & q = 0 \\ 254, & q = 255 \\ q, & \text{otherwise.} \end{cases} \tag{3}$$

The embedding capacity of each block is the number of pixels whose values are equal to peak points in each block.

(v) Embedded information S consists of the location map L and the histogram information H of the image. Scan the nonbasic pixels in each block. If the scanned pixel r is valued $p_{i,L}$ or $p_{i,R}$, a bit $s \in \{0, 1\}$ from S will be embedded. Modify r to r' as

$$r' = \begin{cases} r - 1, & r < p_{i,L} \\ r - s, & r = p_{i,L} \\ r, & p_{i,L} < r < p_{i,R} \\ r + s, & r = p_{i,R} \\ r + 1, & r > p_{i,R}. \end{cases} \tag{4}$$

The encrypted image $\widehat{E}$ with embedded data is obtained. The embedding key K_w consists of the parameter m, $|L|$, $|H|$, and the seed k. The data owner outsources the encrypted image $\widehat{E}$ with embedded watermarking information to the cloud. Then the watermark embedding key K_w is transferred to TPA and the decryption key K_c is shared with the legal users.

3.2.3. Watermarking Extraction and Data Auditing. TPA extracts the watermarking information W' with the extraction key K_w before the user downloads the data from the cloud. The watermarking information can only be extracted from the encrypted domain by TPA that ensures data privacy.

This blind extracting algorithm is shown as follows.

(i) Divide the image $\widehat{E}$ into blocks $\{B_i'\}_{i=1}^{N}$ of pixels in size $m \times m$. Determine the basic pixels $b_{i,L}'$ and $b_{i,R}'$ in each block B_i'.

(ii) The difference $d_i' = |b_{i,L}' - b_{i,R}'|$ is calculated to estimate the smoothness of each block. Blocks with smaller d_i' have higher priority to be chosen for extracting data.

(iii) Determine the two peaks $(p_{i,L}', p_{i,R}')$ in each block with

$$\begin{aligned} p_{i,L}' &= \min\left(b_{i,L}', b_{i,R}'\right), \\ p_{i,R}' &= \max\left(b_{i,L}', b_{i,R}'\right). \end{aligned} \tag{5}$$

If $p_{i,L}' = p_{i,R}'$, $p_{i,R}' = p_{i,R}' + 1$.

(iv) Scan nonbasic pixels in each block B_i'. If the scanned pixel is r', embedding information S will be extracted according to

$$s = \begin{cases} 0, & r' = p_{i,L}' \text{ or } r' = p_{i,R}' \\ 1, & r' = p_{i,L}' - 1 \text{ or } r' = p_{i,R}' + 1. \end{cases} \tag{6}$$

The extracted $|S|$ bits consist of location map L and histogram information H.

TPA verifies the data integrity after extracting the watermark information W'.

The auditing process is as follows.

(i) Scan nonbasic pixels in each block B_i'. If the scanned pixel is r', the restored pixel r can be computed by

$$r = \begin{cases} r' - 1, & r' > p_{i,R} \\ r', & p_{i,L} < r' < p_{i,R} \\ r' + 1, & r' < p_{i,L}. \end{cases} \tag{7}$$

Figure 2: (a) Original image; (b) encrypted image; (c) encrypted image containing watermark; (d) reconstructed image; (e) decrypted image.

(ii) Restore the saturated pixels q with the location map L. If the pixel $q' \in \{1, 254\}$, extract a bit l from L. q is computed by

$$q = \begin{cases} 0, & l = 0,\ q' = 1 \\ 1, & l = 1,\ q' = 1 \\ 255, & l = 0,\ q' = 254 \\ 254, & l = 1,\ q' = 254. \end{cases} \tag{8}$$

The reconstructed encrypted image E' is generated.

(iii) Compute the histogram information H' of the image E'. Then compute the Euclidean distance by (9) and compare the value with the preset threshold θ:

$$D\left(H, H'\right) = \text{sqrt}\left(\sum_{i=1}^{n}\left(H\left[i\right] - H'\left[i\right]\right)^2\right), \tag{9}$$

where $H = (H(1), H(2), \ldots, H(N))$, $H' = (H'(1), H'(2), \ldots, H'(N))$.

If the value $D(H, H') < \theta$, the watermark information is correct and the data is verified to be integrated.

3.2.4. Image Decryption. The legal users can decrypt the reconstructed encrypted image E' using the decryption key K_c and can also obtain the original image I. The decryption process is as follows.

(i) Generate a chaotic sequence of length $M \times M$ with the decryption key K_c.

(ii) Sort the chaotic sequence and record the location set.

(iii) Scramble the sequence of image and restore a decrypted image with the location set.

Then the original image I is obtained by the legal users.

4. Experimental Results

To study the performance of the proposed scheme, MATLAB software 7 is used. The test image Lena of 8-bit gray level sized 512 × 512 pixels is selected as original image and it is shown in Figure 2(a). We use logistic map-based chaotic cryptography algorithm to generate an encrypted image ($x_0 = 0.5$, $\mu = 3.7$), which is shown in Figure 2(b). The encrypted image containing watermarking information is shown in Figure 2(c). After the watermarking information is extracted by TPA, a reconstructed image is shown in Figure 2(d). Then the legal user can decrypt the reconstructed image. The decrypted image is shown in Figure 2(e).

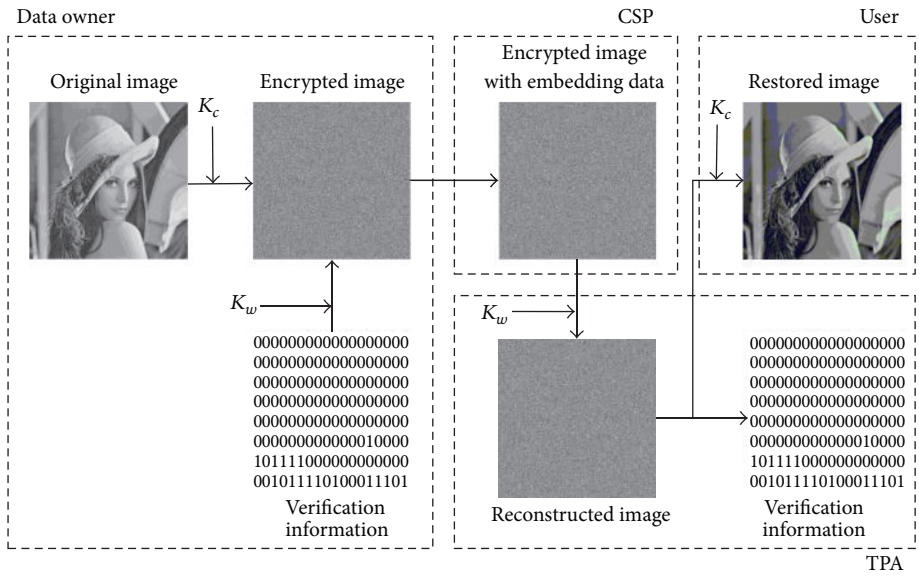

Figure 3: Experimental results of the proposed scheme.

Table 1: Payload bits and MSE.

Image	Payload bits (dB)	Payload bpp	MSE
Lena	2892	0.0110	0
Bridge	8234	0.0314	0
Aerial	4252	0.0162	0
Dollar	2892	0.0110	0

The experimental results of proposed scheme are shown in Figure 3.

The quality of encrypted image can be evaluated by Peak Signal-to-Noise Ratio (PSNR):

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right),$$
$$\text{MSE} = \frac{1}{M \times M}\sum_{i=1}^{M}\sum_{j=1}^{M}\left(I(i,j) - I'(i,j)\right)^2, \quad (10)$$

where I is the original image and I' is the image with watermark information. The size of image I is $M \times M$ pixels. The mean square error (MSE) can evaluate the error between the original image and decrypted image.

Table 1 lists the embedding payloads and MSEs for image Lena, bridge, aerial, and dollar without any attacks.

From Table 1, the MSEs between the decrypted version and the original image are 0. This means the encrypted image will be reconstructed error-free during watermark extraction and data auditing process if the data in cloud is not attacked. The payload is enough for embedding verification information.

In this paper, the watermark algorithm is fragile, which cannot resist any attacks. This can be used in military, remote sensing, and medicine images.

5. Conclusion and Future Work

In this paper, we propose a privacy-preserving and auditing-supporting outsourcing data storage scheme by using encryption and digital watermarking. The proposed scheme combines digital watermark technology with encryption methods for outsourcing data storage. And the scheme supports auditing service and privacy preserving. We adopt the logistic map-based chaotic cryptography algorithm for image encryption and local histogram shifting watermarking algorithm [6] for embedding data integrity verification information. This scheme has high authentication precision which can be used in high quality images.

In the future, we will add semifragile watermark to verify the integrity of images, which can resist some good image operations, such as JPEG compression. We can also apply some algorithms for the sake of supporting tamper localization and recovery.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the NSFC (U1536206, 61232016, U1405254, 61373133, and 61502242), BK20150925, and PAPD fund.

References

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *Proceedings of the IEEE INFOCOM*, pp. 829–837, Shanghai, China, April 2011.

[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2015.

[3] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. E98B, no. 1, pp. 190–200, 2015.

[4] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," *World Wide Web-Internet & Web Information Systems*, vol. 15, no. 4, pp. 409–428, 2012.

[5] N. Singh and S. Singh, "The amalgamation of digital watermarking & cloud watermarking for security enhancement in cloud computing," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 4, pp. 333–339, 2013.

[6] D. Boopathy and M. Sundaresan, "Data encryption framework model with watermark security for data storage in public cloud model," in *Proceedings of the 8th International Conference on Computing for Sustainable Global Development (INDIACom '14)*, pp. 903–907, New Delhi, India, March 2014.

[7] J. Wang and S. Lian, "On multiwatermarking in cloud environment," *Concurrency Computation Practice and Experience*, vol. 24, no. 17, pp. 2151–2164, 2012.

[8] Y. Ren, J. Shen, J. Wang, J. Xu, and L. Fang, "Security data auditing based on multifunction digital watermark for multimedia file in cloud storage," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 9, pp. 231–240, 2014.

[9] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *The Scientific World Journal*, vol. 2014, Article ID 604876, 8 pages, 2014.

[10] N. Thiranant, M. Sain, and H. J. Lee, "A design of security framework for data privacy in e-health system using web service," in *Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT '14)*, pp. 40–43, PyeongChang, South Korea, February 2014.

[11] R. L. de Souza, H. V. Netto, L. C. Lung et al., "SSICC: sharing sensitive information in a cloud-of-clouds," in *Proceedings of the 9th International Conference on Systems (ICONS '14)*, pp. 185–191, Nice, France, February 2014.

[12] G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 598–610, November 2007.

[13] A. Juels and B. S. Kaliski Jr., "Pors: proofs of retrievability for large files," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 584–597, November 2007.

[14] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage," in *Proceedings of the 3rd International Conference on Communication Systems and Networks (COMSNETS '11)*, pp. 1–4, Bangalore, India, January 2011.

[15] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 9, pp. 1432–1437, 2011.

[16] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS '10)*, pp. 282–292, Beijing, China, April 2010.

[17] W. N. Cheung, "Digital image watermarking in spatial and transform domains," in *Proceedings (TENCON '00)*, vol. 3, pp. 374–378, IEEE, Kuala Lumpur, Malaysia, 2000.

[18] S.-H. Wang and Y.-P. Lin, "Wavelet tree quantization for copyright protection watermarking," *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154–165, 2004.

[19] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[20] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[21] C.-L. Hsu, M.-R. Lee, and C.-H. Su, "The role of privacy protection in healthcare information systems adoption," *Journal of Medical Systems*, vol. 37, no. 5, article 9966, 2013.

[22] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *International Journal of Medical Informatics*, vol. 80, no. 2, pp. e26–e31, 2011.