A Distribution Outsourcing Scheme Based on Partial Image Encryption

Xuan Li[1], Zhihua Xia[1]

[1] Jiangsu Engineering Center of Network Monitoring, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer and Software, Nanjing University of Information Science & Technology, China
lixuan0023@163.com, xia_zhihua@163.com

Abstract

The digital watermark technology is widely used in copyright protection. However, with the rapid increasing of user demands and the explosive growth of data, it is difficult for the low-performance machine of the data provider to deal with business in real time. Therefore, it can be a good alternative that the task with high computing complexity and large resource consuming is outsourced to the professional cloud server. As far as known, the cloud server is considered as the honest-but-curious entity which may have some potential security issues. In order to solve these problems, we proposed a distribution outsourcing scheme based on partial image encryption. The wavelet coefficients of the image are divided into two parts, the watermarking part and the encrypting part, based on the requirement of security and robustness. The encrypting part is encrypted by the data owner, and the fingerprint watermark is embedded by the cloud server. When the data user is authorized, the visible image with the fingerprint watermark will be restored by decrypting the encrypted one. By analyzing the security of image data and the practicability of the scheme, our scheme is immediately practical.

Keywords: Digital watermark, Partial encryption, Distribution outsourcing, Discrete wavelet transform

1 Introduction

With the digitalization of information media and the rapid growth of computer networks, the way of creation, reproduction, and transmission of works has been changed greatly. The unauthorized duplication of digital productions has inevitably happened. In order to protect the content of digital media, encryption and digital watermarking technology are widely applied in different situations. Cryptography deals with the concealment and protection of digital information [1]. Even if an unauthorized user receives encrypted information, the content of the information will not be known without decryption. Watermarking is the process of embedding metadata (or controlled distortion) into a multimedia element such as image, audio and video [2]. The main applications of watermark include identification of the origin of content and tracing illegally distributed copies [3].

For copyright protection of digital multimedia works, the metadata contains information about the copyright owner [4]. It is imperceptibly embedded as a watermark in the cover work to be protected [5]. If users of digital content (music, images, and video) have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content. In this case, an honest user can use that watermark information to contact the copyright owner to request permission to use the image. When the embedded watermark is used to trace illegally distributed copies, different from copyright notice, the additional information associated with a digital content should contain information about the end user, rather than about the owner of a digital content [6]. Once a leaked version of the watermarked digital multimedia works is found in the market, it is easy to trace the source by extracting and identifying the watermark of the leaked copy [7].

In recent years, the throughput of multimedia data is increasing dramatically with the rapid increasing of users and the explosive growth of data. The content provider may not be able to provide quality services to customers when their server can not solved all requests in time with limited computing resource [8], and even some providers do not have enough servers to make response quickly. Therefore, it is a beneficial choice to outsource the workloads into the cloud that customers could enjoy the literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays in the purchase of both hardware and software and/or the operational overhead therein [9]. However, security and privacy are always the inevitable issue of cloud computing. To combat against

*Corresponding Author: Zhihua Xia; E-mail: xia_zhihua@163.com
DOI: 10.3966/160792642018051903016

unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end-to-end data confidentiality assurance in the cloud and beyond [10].

In some application, encryption and digital watermarking need be applied at the same time to ensure the outsourced data security. Commutative watermarking and encryption (CWE) [11] can meet the demand that the watermark need be embedded in outsource encrypted data. The process of commutative watermarking and encryption satisfies the following condition:

$$\begin{cases} X_W = f_W(X,W) \\ X_E = f_G(X,k) \\ X_{W,E} = f_W(f_C(X,k),W) = f_C(f_W(X,W),k) \end{cases} . \quad (1)$$

Here, X, X_W, X_E and $X_{W,E}$ denote the original media, watermarked media, cipher media and watermarked cipher media, respectively; and f_W, f_C, W and k denote the watermark embedding function, encryption function, watermark and encryption key, respectively. The order of watermark embedding and encryption does not affect the result of $X_{W,E}$. In term of image, some partial encryption algorithms have been proposed that encrypt only some significant parts of the image [12]. Although a large portion of the image data is left unencrypted, it is difficult to recover the original data without decrypting the encrypted part [13]. Consider that the watermark need be applied as well, it is possible to embed the watermark in unencrypted portion.

In our paper, we proposed a distribution outsourcing scheme based on partial image encryption. The copyright of image is guaranteed by the watermark and encryption in the cloud. The two procedures provide different levels of security. On the one hand, discrete wavelet transformation (DWT) [14] is firstly performed to calculate the coefficients of the low-frequency and high-frequency bands of the image. Depending on the requirements of security and robustness, the lowest frequency band of the image must be encrypted to prevent leaking from the cloud. On the other hand, balancing between the quality of the image and the robustness of the watermark, the appropriate frequency band of the image need be chosen to embed the watermark.

2 Problem Statement

In our scheme, most problems including data security, copyright dispute and computational efficiency, arise from outsourcing to the third part cloud server. To maximize the profit of outsourcing as for as possible, it is necessary to balance those problems. We will describe the system model, the thread model and the design goals to explain the relation of problems caused by outsourcing.

2.1 System Model

The data owner is the copyright holder of the image content who benefits from authorizing access to certain images. However, there are always illegal data users who try to get profit by distributing unauthorized data. In order to mitigate losses, it is necessary to apply the watermark technology to restrict the illegal distribution. On the other hand, watermark embedment and data distribution may be performed efficiently when the number of user request increases dramatically in a short time.

The cloud server is the employed part who can provide effective and efficient customer service. When the authorized request from the user have been verified, the specified images will be retrieved and deliver to the user. During this phase, the watermark as the fingerprint need be embedded in the specified images for marking the identity of the end user. The fingerprint watermark will be key role when copyright issues happen between the data owner and the data user.

The data user wants to purchase the copy of the image from the data owner. As a legal user, he has a responsibility for protecting authorized images from leaking.

2.2 Thread Model

Data privacy. We consider the cloud server to be "honest-but-curious" [15] which means that the cloud server correctly follows the protocol specification but keeps and analyzes the communication data so as to obtain the sensitive information [16]. Thus, the privacy of the image content needs to be properly protected. In our scheme, the solution is encrypting the image before outsourcing.

Copyright. In the proposed scheme, we consider the data user who correctly follows the protocol specification but may distribute the purchased images to others for illegal benefits. The watermarking technology is adopted to deter the illegal distribution.

2.3 Design Goals

It is not difficult to embed the watermark in a single image. However, when the requirements from the massive amounts of users are increasing sharply in a short time, it is hard or even impossible to implement the watermarking embedment by many low-performance servers. There are two difficulties: one is the computational performance, another one is the load capacity. In order to ensure the security and practicability of our scheme, the following conditions have to be guaranteed.

Privacy. The image information from the data owner cannot be leakage by the cloud server.

Efficiency. The service provided by the cloud server should be efficient enough to meet the expectation of the data owner and user.

3 Proposed Scheme

This section presents three stages of our scheme which are the interactive process among three roles. The assignment stage is the preparation of the outsourcing data involving the data owner and the cloud server. The authorization stage is the purchase process that the data user pays for image contents from the data owner, then the delivering stage is that the user obtains the image from the cloud server. Here, I,W and I_W denote the original image, the watermark and the watermarked image, respectively; and X and Y denote the encrypting part and the watermarking part. The details are given as Figure 1.

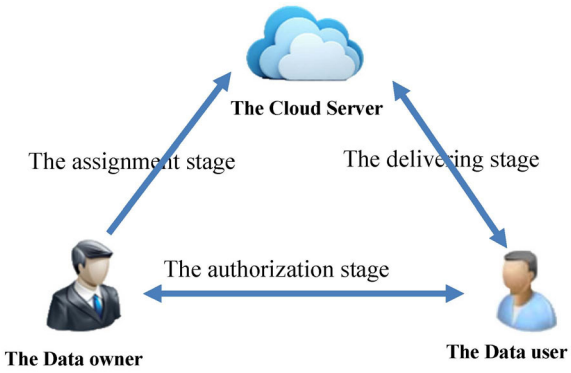


Figure 1. The model of three roles and three stages

3.1 The Assignment Stage

Before outsourcing the image data, the data owner need make preparations including three steps: watermarking, encrypting and uploading. And the transforming procedure of data is shown as Figure 2.

The embedment of the ownership watermark. The information of owner such as a logo or a signature will be embedded as the watermark W_A. In this step, any appropriate watermarking method might be applied on the original image I as long as the ownership watermark will not affect the fingerprint watermark mentioned later.

The partial encryption. In our scheme, the image data are encrypted in the wavelet domain, so the image I_{W_A} is transformed by discrete wavelet transform (DWT) firstly. The wavelet coefficients of images are divided into the encrypting part X and the watermarking part Y based on the requirement of security and robustness. On the one hand, it has to be ensured that the encrypting part contains most of main information about the image to avoid the leaking of image content. On the other hand, under the premise of the security of image content, the robustness of watermark and the quality of image need be guaranteed. After generating the key k of the image, the encrypting part X and the watermarking part Y are encrypted respectively.

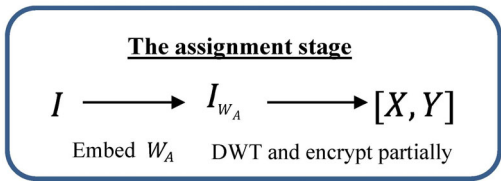


Figure 2. The partial image encryption in the assignment stage

In our scheme, we refer to the encryption method proposed by Lian et al. [11]. The watermarking part Y includes the subbands in the middle level (LH_2,LH_2,LH_2) which are suitable for applying the watermark proved by the experience in [11]. The part Y can be encrypted with sign encryption keeping the coefficient amplitudes unchanged. The rest of subbands, the encrypting part X, are encrypted. The encryption algorithms proposed in [17] and [18] can be used. The way of data partition is illustrated in Figure 3. The main procedure of the partial encryption is described in Table 1.

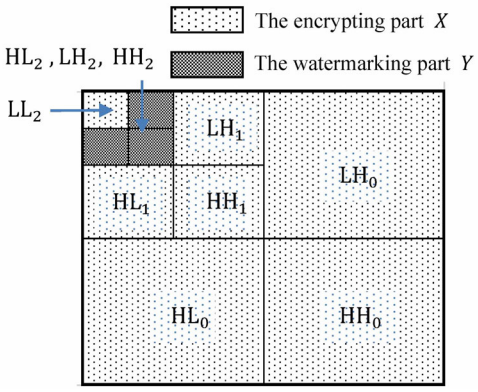


Figure 3. The partial encryption in the wavelet domain

Table 1. The partial encryption algorithm

Input:	I_{W_A} , $[k_E,k_W]$
Output:	$[X,Y]$.

Begin

1. Perform 3-level DWT on I_{W_A} and calculate the coefficient [LL_2, LH_2, HL_2, HH_2, LH_1, HL_1, HH_1, LH_0, HL_0, HH_0].
2. (The encrypting part X) Encrypt the subbands [LL_2, LH_1, HL_1, HH_1, LH_0, HL_0, HH_0].
   (a) Concatenate the coefficient [LL_2, LH_1, HL_1, HH_1, LH_0, HL_0, HH_0] into a single coefficient vector V .
   (b) Encrypt V by AES with the key k_E .
3. (The watermarking part Y) Encrypt the subbands [LH_2, HL_2, HH_2].
   (1) Concatenate the coefficient [LH_2, HL_2, HH_2,] into a single coefficient vector W .
   (2) (Sign encryption) Change the sign of the coefficient in W according to the key k_W .
4. Output $[X,Y]$.

End;

The key k includes two part, the encryption key k_E and the watermark key k_W. The key k_W is the position where the sign of the wavelet coefficient need be changed.

Data upload. When all of images are encrypted completely, the data owner upload them to the cloud server. Note that the encrypted image is the form of $[X,Y]$.

3.2 The Authorization Stage

This stage is also called the payment process, the data user chooses images he wants and pays for them. After the payment, the data user will be authorized the corresponding key k to the image. And the transaction information will be saved as well. Finally, the transaction details, including the users' identity, the image ID and so on, will be sent to the cloud server.

3.3 The Delivering Stage

The stage is the process of the image transaction, and the transforming procedure of data is shown as Figure 4. A valid user will receive the encrypted image from the cloud server. But before the received image is visible, there are still three steps.

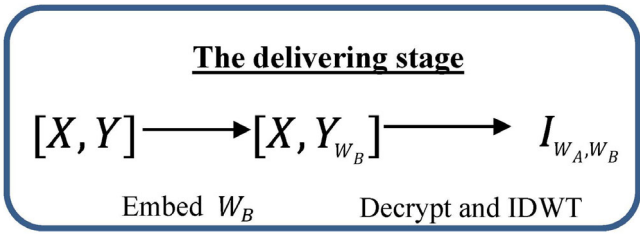


Figure 4. The watermarking and decryption in the delivering stage

The verification of user. After receiving the transaction details, only if the validity of the data user is confirmed, the image will be retrieved and watermarked by the cloud server.

The embedment of the fingerprint watermark. The fingerprint watermark W_B is the unique identification of each transaction. It is embedded in the watermarking part Y of the encrypted image by the cloud server. Here, the watermark method such as the quantization index modulation (QIM) method [19] and the spread spectrum method [20] can be applied.

The delivery and decryption. The encrypted image $[X,U_{W_B}]$ is sent to the data user from the cloud server. Finally, the data user decrypts the image by the key k authorized by the data owner and gets the image I_{W_A,W_B} by inverse discrete wavelet transform (IDWT).

4 Performance Analysis

4.1 Theoretic Analysis

Data owner side overhead. According to our scheme, data owner side computation overhead and time consumption consist of the ownership watermark embedment, the key generation, the partial encryption and data upload.

The computation overhead of the ownership watermark depends on the watermark algorithm applied in practice, so it will not be discussed here. The key generation only requires a random generation, and its computation complexity is $O(n)$. The discrete wavelet transform (DWT) is linear, its computation complexity is $O(n)$ as well.

We have no access to a high-performance server, so speed estimates for the partial encryption are executed on a 3.5 GHz AMD CPU, 64-bit Windows platform using Python. The time consumption of encryption and decryption is shown in Table 2.

Table 2. The performance of encryption and decryption

Key/Block Length	Speed of encryption	Speed of decryption
(128,128)	60000 Kbit/s	75000 Kbit/s
(192,128)	58000 Kbit/s	70000 Kbit/s
(256,128)	55000 Kbit/s	65000 Kbit/s

Apart from computation overhead, data upload operation need consume some time according to the internet speed and the image data size. Because these operations are performed in the preparation stage, it doesn't affect the efficiency of the distribution.

Server side overhead. The computation complexity of the fingerprint watermark is $O(n)$ in our scheme. The time consumption in the cloud server includes the watermark operation and the data transmission.

When the data throughput is high, the cloud server need guarantee that the distribution service is provided without delay. So the data owner should choose the cloud server as required.

Data user overhead. The computational operations executed by the data user are decryption and inverse discrete wavelet transform (IDWT). As the forward discrete wavelet transform, the computation complexity of IDWT is $O(n)$. And the speed of decryption is shown in Table 2. The computation complexity is acceptable for most terminal devices.

4.2 Security Analysis

Data privacy. The wavelet coefficients of image are divided into the encrypting part X and the watermarking part Y. The part X includes the lowest frequency subband (LL_2) which is of higher sensitivity to images' understandability and is very suitable for

encryption. In this paper, we use AES as the encryption algorithm to encrypt the part X. The block ciphers AES has high security against statistic or differential attack [21]. So the security of the image can be guaranteed if the key is not revealed.

Copyright. There are two kinds of watermark applied in the image, the ownership watermark and the fingerprint watermark. As the name suggests, the ownership watermark is used to prove the ownership of the data owner, the fingerprint watermark contains the information of the data user.

With the precondition of the watermark technologies' validity, when the pirated copy is found in the market, the first thing is extracting its watermark. There will be three different situations as follow.

(1) **No watermark in the copy**. Because of security problems in the data owner, the original data are stolen by the hacker.

(2) **Only the ownership watermark in the copy**. If the cloud server executed correctly according to our scheme, the fingerprint watermark should be found in the image. In addition, the image can be distributed only if the validity of the data user is confirmed. There are two possibilities causing the pirated copy:

① Malicious collusion between the cloud server and the data user. The data user provides the cloud server with the key, and the cloud server dose not embed the fingerprint watermark in return.

② Data leakage in the cloud server. Because of security problems in the cloud server, the storage data are stolen by the hacker. And the hacker gets the key through certain means.

When these situation occur, the cloud server should be responsible for the data leakage.

(3) **Two watermarks in the copy**. When the ownership watermark and the fingerprint watermark are extracted from the pirated copy, the fingerprint watermark will be shown who is the source of the pirated copy.

5 Experimental Results

In order to evaluate the performance of watermark detection and robustness to attacks in our scheme, we used test images with size 512 × 512, as shown in Figure 5. A binary message of length 30×30 bits is embedded into each image.

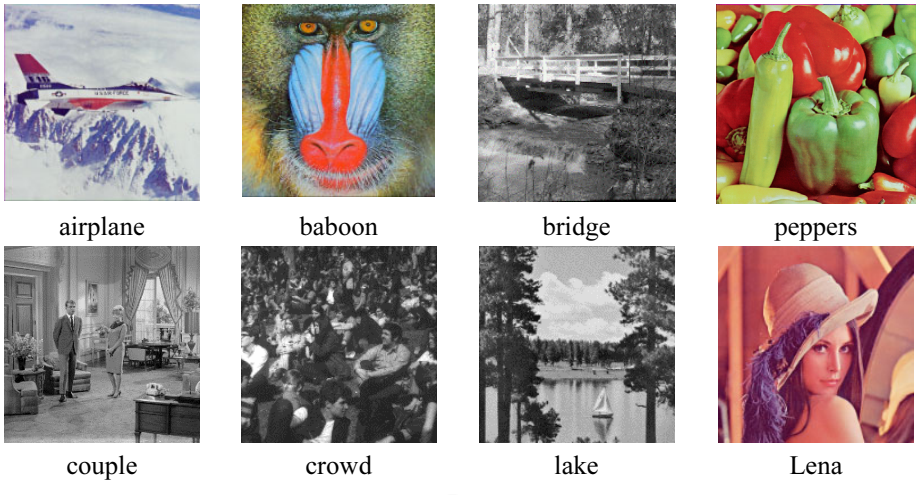


Figure 5. Testing images with size 512×512 and the binary watermark with size 30×30

Simulation results were conducted to demonstrate the image quality assessment after watermarking, the robustness of the technique under JPEG compression with different quality factors and the time consumption among the data owner, the data user and the cloud server.

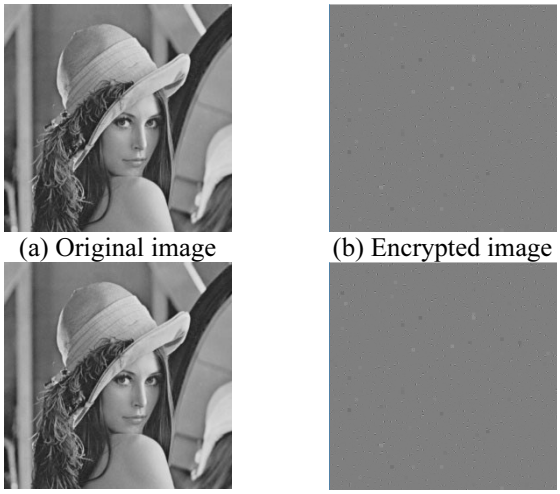
5.1 Image Quality Assessment

The Peak Signal to Noise Ratio (PSNR) is used as distortion measurement between the original and the watermarked image. It is define as:

$$PNSR = 10 \times \log_{10}\left(\frac{255^2}{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(x_{i,j} - y_{i,j})^2}\right) \quad (2)$$

Where M and N are the height and the width of the image, $x_{i,j}$ is the i-th row and the j-th column pixel in the original image, and the $y_{i,j}$ is the pixel in the watermarked original.

Figure 6 shows the original image, the watermarked image, the encrypted image and the watermarked encrypted image. The PSNR of the watermarked image is 49.27 dB and the watermarked image is undistinguishable from the original image. Note that the encrypted image is normed by mapping the value of the encrypted result E that is generated by transforming the encrypted wavelet coefficient with inverse discrete wavelet transform (IDWT) in the range 0-255 as follow.



(a) Original image (b) Encrypted image

(c) Watermarked image PSNR = 49.27 dB (d) Watermarked encrypted image

Figure 6. (a) Original image (b) Encrypted image (c) Watermarked image (d) Watermarked encrypted image

$$E = IDWT([X,Y]) \tag{3}$$

$$I_{Enc} = \text{mapminmax}(E) \times 255 \tag{4}$$

Where $[X,Y]$ is the wavelet coefficient of the image, X is the encrypted encrypting part, E is the encrypted result and IDWT is performing inverse discrete wavelet transform; $mapminmax(E)$ is the normalization referring to the same name function in MATLAB and I_{Enc} is the encrypted image. In fact, I_{Enc} is only for demonstration.

5.2 Robustness

In our scheme, the normalized correlation (NC) to evaluate the performance of the robustness. The NC measures the correlation between the original and the extracted watermark, and can be calculated according to:

$$NC = \frac{\sum_{i=1}^{Nw}\sum_{j=1}^{Mw} W(i,j) \times \hat{W}(i,j)}{\sum_{i=1}^{Nw}\sum_{j=1}^{Mw} (W(i,j)^2} \tag{5}$$

Where $Nw \times Mw$ is the size of the binary image watermark.

As show in Table 3. We can observe that our algorithm has good robustness against JPEG compression. These extracted watermarks are distinct from the original watermark, even when the quality factor for JPEG compression is low. And the NC values of the testing images in different quality factors are shown in Figure 7, our scheme has less sensitivity to JPEG compression.

Table 3. Watermarks retrieved after JPEG compression

Quality factor	100	90	80	70	60	50	0
airplane							
baboon							
bridge							
couple							
crowd							
lake							
Lena							
peppers							

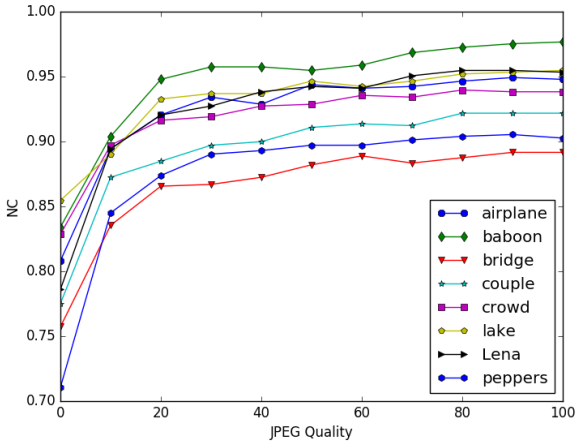


Figure 7. Robustness against compression attacks in different quality factors

5.3 Time Consumption

In order to compare the time consumption between the data owner and the cloud server, we calculate the average time consumption for embedding different size watermarks as shown in Figure 8, and the average time consumption for encrypting different size images as shown in Figure 9.

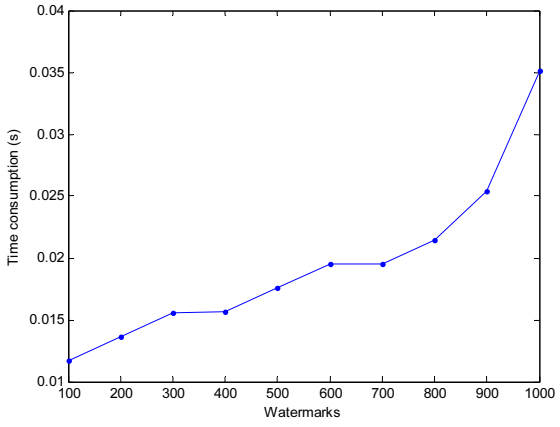


Figure 8. Time consumption for embedding different size watermarks in the cloud server

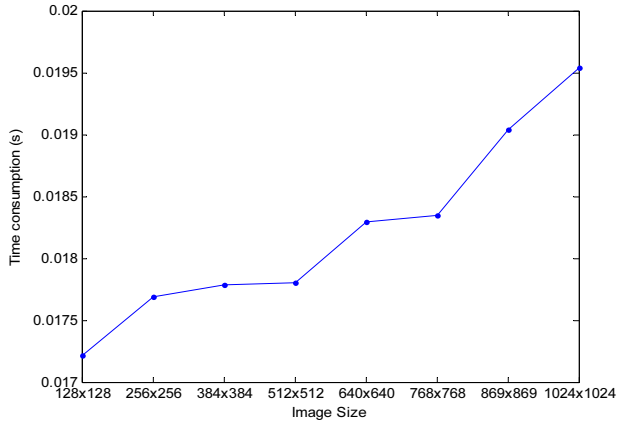


Figure 9. Time consumption for encrypting different size images in the data owner

Note that these results of time consumption were calculate in our machine mentioned in Section 4.1. We can observed that the watermarking time consumption is increasing along with the increase of watermark size, and the encrypting time consumption is increasing along with the increase of image size. The experiments above were implemented on 512×512 images which are embedded 900 bits watermark, we can find out that the encrypting time is approximately 0.017 seconds, and the watermarking time is approximately 0.021 seconds. In this case, the time consumption in the cloud server is 1.23 times to the time consumption in the data owner.

6 Conclusion

In this paper, we propose a distribution outsourcing scheme based on partial image encryption. To deal with distribution business in real time, image data are outsourced to the cloud server. We adopt the partial encryption to solve the privacy of image data caused by the outsourcing service. The wavelet coefficients of image are divided into the encrypting part and the watermarking part. The encrypting part is encrypted with AES by the data owner, and the fingerprint watermark of the data user is embedded in the watermarking part by the cloud server. Through the performance analysis, outsourcing the image data reduces the burden of the data owner. Meanwhile, the computation overhead of the data user is acceptable for most terminal devices. The copyright of the image data is protected that the illegal distribution can be limited successfully.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China under grant numbers 61672294, 61502242, 61702276, U1536206, U1405254, 61772283, 61602253, 61601236, and 61572258, in part by Six peak talent project of Jiangsu Province (R2016L13), in part by NRF-2016R1D1A1 B03933294, in part by the Jiangsu Basic Research Programs-Natural Science Foundation under grant numbers BK20150925 and BK20151530, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China. Zhihua Xia is supported by BK21+ program from the Ministry of Education of Korea.

References

[1] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[2] W. Zeng, S. Lei, Efficient Frequency Domain Selective Scrambling of Digital Video, *IEEE Transactions on Multimedia*, Vol. 5, No. 1, pp. 118-129, March, 2003.

[3] F. A. P. Petitcolas, Watermarking Schemes Evaluation, *IEEE Signal Processing Magazine*, Vol. 17, No. 5, pp. 58-64, September, 2000.

[4] H. C. Huang, W. C. Fang, Metadata-based Image Watermarking for Copyright Protection, *Simulation Modelling Practice & Theory*, Vol. 18, No. 4, pp. 436-445, April, 2010.

[5] B. Hu, Z.-H. Guan, N. Xiong, H.-C. Chao, Intelligent Impulsive Synchronization of Nonlinear Interconnected Neural Networks for Image Protection, *IEEE Transactions on Industrial Informatics*, Vol. PP, No. 99, pp. 1-1, February, 2018.

[6] C. I. Podilchuk, E. J. Delp, Digital Watermarking: Algorithms and Applications, *IEEE Signal Processing Magazine*, Vol. 18, No. 4, pp. 33-46, July, 2001.

[7] S. A. Moskowitz, *Multiple Transform Utilization and Applications for Secure Digital Watermarking*, EP, US 6205249 B1, 2001.

[8] Z. Xia, Y. Zhu, X. Sun, Z. Qin, K. Ren, Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing, *IEEE Transactions on Cloud Computing*, Vol. 6, No. 1, pp. 276-286, January-March, 2018.

[9] Z. Xia, N. N Xiong, A. V. Vasilakos, X. Sun, EPCBIR: An Efficient and Privacy-preserving Content-based Image Retrieval Scheme in Cloud Computing, *Information Sciences*, Vol. 387, pp. 195-204, May, 2017.

[10] C. Wang, K. Ren, J. Wang, Secure and Practical Outsourcing of Linear Programming in Cloud Computing, *IEEE International Conference on Computer Communications*, Shanghai, China, 2011, pp. 820-828.

[11] S. Lian, Z. Liu, R. Zhen, H. Wang, Commutative Watermarking and Encryption for Media Data, *Optical Engineering*, Vol. 45, No. 8, p. 080510, August, 2006.

[12] H. Cheng, X. Li, Partial Encryption of Compressed Images and Videos, *IEEE Transactions on Signal Processing,* Vol. 48, No. 8, pp. 2439-2451, August, 2000.

[13] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. D. Natale, A. Neri, A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain, *Signal Processing Image Communication*, Vol. 26, No. 1, pp. 1-12, January, 2011.

[14] A. K. Singh, B. Kumar, M. Dave, A. Mohan, Multiple Watermarking on Medical Images Using Selective Discrete Wavelet Transform Coefficients, *Journal of Medical Imaging & Health Informatics*, Vol. 5, No. 3, pp. 607-614, June, 2015.

[15] Z. Xia, X. Wang, X. Sun, Q. Wang, A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 27, No. 2, pp. 340-352, February, 2016.

[16] Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, Y.-Q. Shi, Fingerprint Liveness Detection Using Gradient-based Texture Features, *Signal, Image and Video Processing*, Vol. 11, No. 2, pp. 381-388, February, 2017.

[17] M. A.Wright, The Advanced Encryption Standard, *Network Security*, Vol. 2001, No. 10, pp.11-13, October, 2001.

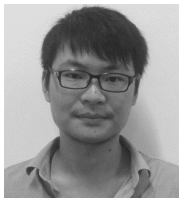
[18] B. Chen, G. W. Wornell, Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding, *IEEE Transactions on Information Theory*, Vol. 47, No. 4, pp. 1423-1443, May, 2001.

[19] A. Pommer, A. Uhl, Selective Encryption of Wavelet-packet Encoded Image Data: Efficiency and Security, *Multimedia Systems*, Vol. 9, No. 3, pp. 279-287, September, 2003.

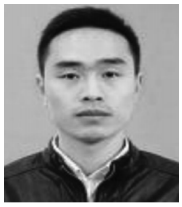
[20] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, December, 1997.

[20] C. C. Chang, T. X. Yu, Cryptanalysis of an Encryption Scheme for Binary Images, *Pattern Recognition Letters*, Vol. 23, No. 14, pp. 1847-1852, December, 2002.

Biographies



Xuan Li received the B.E. degree in intelligence science and technology from the Wuhan Institute of Technology in 2015, China. He is currently working towards the MS degree in computer science and technology at the College of Computer and Software, in Nanjing University of Information Science & Technology, China. His research interest includes network and information security.



Zhihua Xia received the B.E. degree in Hunan City University, China, in 2006, the PhD degree in computer science and technology from Hunan University, China, in 2011. He works as an associate professor in the School of Computer & Software, Nanjing University of Information Science & Technology. His research interests include cloud computing security, and digital forensic. He is a member of the IEEE.