2022 21st International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)

Secure Verifiable Outsourced Watermark Embedding Framework in Multi-User Settings

Wanxi Yan, Hang Cheng*, Meiqing Wang
College of Mathematics and Statistics
Fuzhou University
Fuzhou, China
Email: 200320038@fzu.edu.cn;
hcheng@fzu.edu.cn;
mqwang@fzu.edu.cn

Hehui Ye, Qinjian Huang, Li Wu
College of Computer Science and Big Data
Fuzhou University
Fuzhou, China
Email: yehehui@qq.com;
821403552@qq.com;
1724081294@qq.com

***Abstract*—With the development of the mobile Internet, supporting multi-user has become a popular concern for Internet-based algorithms. In this paper, an efficient watermark embedding framework is proposed to achieve secure outsourced image watermarking in multi-user settings. In addition, an authentication mechanism for authorized users is designed to ensure the security and correctness of the information. The proposed method enables watermarking operations in complex outsourced environments while embedding watermarks in encrypted images of multiple users. The experimental results show that the framework is feasible and scalable.**

***Keywords*-multi-user; verifiable; watermarking; edge computing; safety.**

I. Introduction

Currently, the Internet is closely related to our work, study and life, where inevitably generates a large amount of information on the Internet [1–3]. Every minute, there are about 1.1 million tweets, 684,478 contents shared on Facebook, and 3.2 million queries searched on Google, nearly 48h of videos uploaded to YouTube [4]. The protection of digital copyright has become an urgent problem to be solved. An effective means to protect one's digital copyright is to embed a watermark on one's data. The traditional watermark embedding scheme needs a lot of computing power. It is a difficult task for users with limited computing resources to add digital watermark to a large amount of multimedia information they own locally. Therefore, it is an effective solution to combine digital watermarking technology [5] with powerful cloud computing technology. For example, transferring the watermark embedding operation of massive images to the cloud, which can not only ensure the copyright ownership of users but also reduce the consumption of local computing/storage resources. This way, higher processing efficiency can be obtained [6]. However, cloud outsourcing data often involves trade secrets and user-sensitive data. It is left to the cloud to process plaintext data, resulting in the risk of data security and privacy leakage [7]. Obviously, it is important to protect one's privacy and legitimate rights and interests through a secure watermark embedding scheme.

At present, there are many effective ciphertext watermarking schemes [8–11], but most of them do not take the multi-user scenario into consideration, which is more desired today with the increase of mobile devices. The involvement of multiple users will affect the legitimacy of users. So, it is necessary to design a secure authorization verification mechanism.

Due to the low efficiency and inconvenience for single-user solutions, this work extends the scheme proposed by Cheng [12] to multi-user scenario and realizes the privacy protection of the original image data as well as secure watermark embedding. The main contributions of our work can be summarized as follows:

- Aiming at multi-user scenario, this paper designs a key conversion mechanism based on reversible matrix. With this mechanism, the data encrypted by each data owner can be further scrambled and prevent the leakage between data owners.
- This paper introduces the hash and digital signature algorithms to develop a reliable authorization verification method, which solves the authentication error during watermark extraction.

II. Related Work

Digital watermarking technology mainly includes spatial domain algorithm [13, 14] and transform domain algorithm. Among them, the spatial domain algorithm mainly uses the redundancy between pixels to embed the watermark, where the transform domain algorithm [15] employs the frequency of the image to perform watermark embedding. Most ciphertext watermarking schemes focus on the watermark embedding in the spatial domain, and the security mainly depends on the Paillier encryption system. Due to huge computing/storage costs, it is difficult for users with limited resources to construct a complete secure watermark embedding framework based on Pailler encryption. Therefore, Cheng et al.[12] proposed a privacy-preserving outsourced image watermark embedding framework based on edge computing. In this framework, the data owner simply encrypts the host/watermark image and uploads the ciphertext image to the edge computing server. Without knowing the actual plaintext content, the edge computing server can perform the discrete wavelet transform on the encrypted host image, and

2473-3636/22/$31.00 ©2022 IEEE
DOI 10.1109/DCABES57229.2022.00072

then carry out the secure singular value decomposition. Finally the ciphertext watermark image is embedded into the singular values of the encrypted host image.

Alg.1 shows the privacy-preserving outsourced image watermark embedding algorithm of Cheng [12]. Please refer to this reference for more details.

Algorithm 1: Privacy-preserving outsourced image watermark embedding.

Initialization: a integer γ_1, two large primes D and F, $key = \{\gamma_1, D, F\}$, host image I, watermark image W
Input: $\{key = \{\gamma_1, D, F\}, I, W\}$
Output: watermarked encryption image $[I_W]$
CO computes encryption host image $[I]$, encryption watermark image $[W]_l$.
for $p \leftarrow I[0]$ to $I[n]$ **do**
  randomly select $c, y \in (1, t), t = 2^{\gamma_1}$
  $[p] = p + c \cdot D + y \cdot F$
end for
for $m \leftarrow W[0]$ to $W[n]$ **do**
  $X^{'}(0) = (X_W(0) + X(0))/2$
  $logistickey = \left\{X^{'}(0), u\right\}$
  $[m] \leftarrow Logistic(m)$
end for
$\mathbf{S}_2$ computes A_1, A_2 by HDWT.
$[I] \rightarrow [LL]/[HL]/[LH]/[HH]$
$A_1 = [LL] \cdot [LL]^T, A_2 = [LL]^T \cdot [LL]$
$\mathbf{S}_1, \mathbf{S}_3$ compute $[\Sigma_1 Q]$, $V_1$by SVD.
$\mathbf{S}_2$ watermarks $[\Sigma_1]$ as $[\Sigma_n] = [\Sigma_1 Q] + [\alpha Q] \cdot [W]$, sends $[\Sigma_n] \cdot [\Sigma_n]^T$ to $\mathbf{S}_1$, sends $[\Sigma_n]^T \cdot [\Sigma_n]$ to $\mathbf{S}_3$
$\mathbf{S}_1$ computes $[U_1 \Sigma_2 Q] \leftarrow [\Sigma_n] \cdot [\Sigma_n]^T$ by SVD.
$\mathbf{S}_3$ computes $[V_1 Q] \leftarrow [\Sigma_n]^T \cdot [\Sigma_n]$ by SVD.
$\mathbf{S}_2$ computes watermarked ciphertext $[I_W] \leftarrow [LL_{new}] = [U_1 \Sigma_2 Q] \cdot [V_1 Q]^T \cdot \beta$ by IHDWT.
return $[I_W]$.

III. Multi-user Oriented Secure Watermark Outsourced Embedding Scheme

Figure 1 shows the multi-user privacy-preserving watermark outsourced scheme proposed in this paper, including multiple data owners (CO_s), three edge computing servers (S_1, S_2, S_3), and trusted third party (TTP) and authorized users (AU_s). TTP is responsible for distributing keys. CO_i encrypts data and uploads it to the edge servers. The edge servers carry out secure HDWT and SVD algorithm. AU_s decrypt the ciphertext from servers to gain the image plaintext with watermark.

Security model assumptions in this paper is that TTP is a trusted third party, and the three servers in the edge computing server are supposed to be honest and curious. That is, they will faithfully follow the specified procedures while curious about the existing data. The edge server will not collude with users to perform data analysis by sharing information; each user will pay attention to protect their image data information.

A. system initialization

In the multi-user system, when the data owner cluster CO_s of k users initiates a batch watermark embedding request to TTP, in addition to the integer Γ_1 and two large prime numbers D and F, the TTP also generates a reversible matrix key pair $\{M, M^{-1}\}$. For each CO_i, $i \in (1, k)$, TTP generates encryption keys $\left\{M_{CO_i}, M^{'}_{CO_i}\right\}$, $M = M_{CO_i} \cdot M^{'}_{CO_i}$. The designated data owner CO_i receives $M^{'}_{CO_i}$, S_2 receives $\left\{M^{'}_{CO_i}, M^{-1}\right\}$, and TTP transmits information through a secure channel.

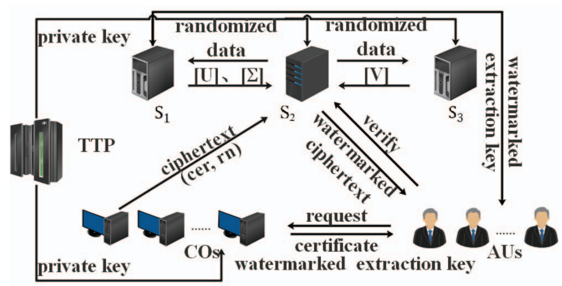

Figure 1. Multi-user verifiable secure watermark outsourced embedding framework

B. image encryption

In Cheng's secure watermark outsourced embedding framework [12], for a host image I sized of $m \times n$, $[I]$ is the encrypted version of I, and its size remains unchanged. CO_i uses M_{CO_i} to scramble the ciphertext matrix $[I]$ twice, as shown in Equation 1. $[I]_i$ will then be sent to the edge server.

$$[I]_i = M^{'}_{CO_i} \cdot [I]. \tag{1}$$

C. multi-user key decryption and watermark embedding

After receiving the encrypted image $[I]_i$ of each data owner, the edge server S_2 uses the Equation 2 to decrypt with the decryption key $\{M_{CO_i}, M^{-1}\}$ corresponding to $[I]_i$ and obtains the encrypted matrix $[I]_i$ of the uploaded image of CO_i.

$$\begin{aligned} & M^{-1} \cdot M_{CO_i} \cdot [I]_i \\ & = M^{-1} \cdot M_{CO_i} \cdot M^{'}_{CO_i} \cdot [I] \\ & = M^{-1} \cdot M \cdot [I] = [I]. \end{aligned} \tag{2}$$

After S_2 obtains the original one-time encrypted image matrix $[I]$, it performs the wavelet transformation under the ciphertext and the secure singular value decomposition process. Finally, it embeds the watermark under the ciphertext and reconstructs the ciphertext image matrix to complete the watermark embedding.

IV. Authorized User Authentication

In this section, we introduce the verifiable features of the multi-user secure outsourced watermarking framework. It mainly includes three steps, the user submits an authorization application to CO_i, the edge server verifies the authorization, and the authorized user verifies the key.

A. user authorization application

The process for an AU_i to submit an authorization application to CO_i is as follows.
(**i**) AU_i requests to initiate an authorization application, and attaches its own ID_{AU_i}.
(**ii**) After CO_i receives the request, if it agrees to the application, it will generate a random number rn. The certificate's information is composed of ID_{CO_i} and $HASH\left(ID_{AU_i}, ID_{CO_i}, rn\right)$. Equation 3 shows the specific generated certificate information.

$$cer = \left(ID_{CO_i}, HASH\left(ID_{AU_i}, ID_{CO_i}, rn\right)\right), \quad (3)$$

(**iii**) After CO_i generates the certificate, it will use the public key encryption system to perform the signature algorithm on the certificate. For a pair of keys $\{PK_i, SK_i\}$, CO_i uses SK_i to encrypt the certificate to obtain $Sign\left(cer, SK_i\right)$, and other users can use the public key PK_i to verify the signature.
(**iv**) CO_i sends certificate (cer, rn) to edge server S_2 and sends cer to AU_i at the same time. In order to ensure the security of the certificate, CO_i encrypts the message through the AES encryption method and sends it.

B. edge server validation authorization

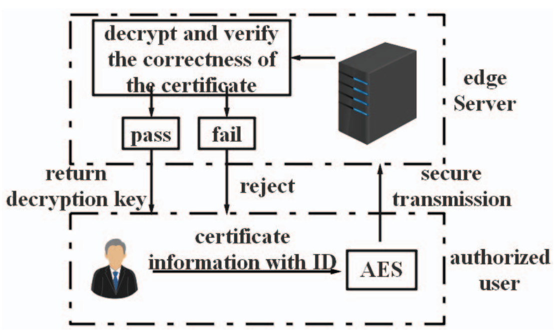

Figure 2. Edge server authentication process

The process of AU_i showing its certificate to the edge computing server S_2 to request the ciphertext image embedded with the watermark is as follows.
(**i**) AU_i encrypts the (cer, ID_{AU_i}) data information through the advanced encryption standard AES and sends it to the server.
(**ii**) S_2 compares the certificate information cer obtained from AU_i and CO_i, then combines the random number rn obtained from CO_i with ID_{AU_i} obtained from AU_i. Use $Hash\left(ID_{AU_i}, ID_{CO_i}, rn\right)$ to calculate the hash value, then compare it with the value in cer. If all are consistent, then AU_i is determined to be a legitimate authorized user.
(**iii**) After S_2 verifies AU_i is a legitimate authorized user, it will notify AU_i to send the key for extracting watermark to AU_i. Figure 2 shows the authorization process.

C. authorized user authentication key

As discussed in the preliminaries, authorized users need to verify that the keys received are correct to prevent false positives. The keys required to extract the watermark information in Cheng's article [12] are U_2, V_2^T, Σ_1, and α, where α is the key that CO_i securely sends to AU_i, an error in Σ_1 will cause the watermark extraction to fail, so U_2, V_2^T need to be verified. Verifying the singular value decomposition of U and V components is as follows.
(**i**) Edge server S_1 first performs XOR operation on all vectors $\boldsymbol{u_i}$ in $\mathbf{U} = \{\boldsymbol{u_1}, \boldsymbol{u_2}, \cdots, \boldsymbol{u_m}\}$. It denotes the vector generated after XOR as $\boldsymbol{u_{xor}}$. Performing XOR operation on the singular value vector $\boldsymbol{\sigma}$ composed of singular values on the diagonal of Σ and $\boldsymbol{u_{xor}}$. If the $\boldsymbol{\sigma}$ element is not enough, fill it with 0. If the $\boldsymbol{\sigma}$ element is too much, it will be discarded. The final generated vector is denoted as $\boldsymbol{u_{ver}}$, let $u_{hash} = Hash\left(\boldsymbol{u_{ver}^T}\right)$, and u_{hash} is sent to the AU.
(**ii**) The edge server S_3 is similar to S_1. The component $\mathbf{V} = \{\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_m}\}$ of the SVD is denoted as $\boldsymbol{v_{xor}}$ after performing the XOR operation. Performing the XOR operation on $\boldsymbol{v_{xor}}$ and $\boldsymbol{\sigma}$. The result is denoted as $\boldsymbol{v_{ver}}$. Finally, S_3 sends $v_{hash} = Hash\left(\boldsymbol{v_{ver}^T}\right)$ to AU.
(**iii**) After the AU receives the U and V used to extract the watermark, the verified hash values u_{hash} and v_{hash}. The AU performs the XOR operation of (**i**) (**ii**) on the U and V, respectively, with the Σ_{ext} extracted from the embedded watermark image by the AU. After the operation, it is compared with the hash values u_{hash} and v_{hash}. If they are consistent, the verification is passed, and the extracted watermark is the correct watermark image. Figure 3 shows the authorized user verification process.

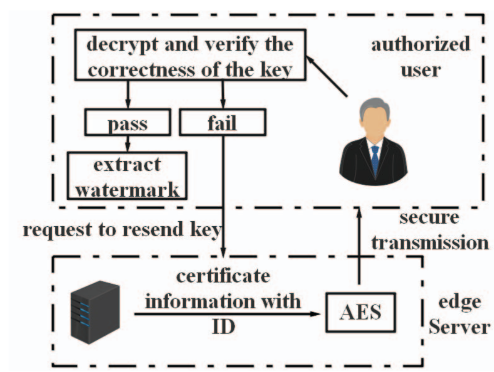

Figure 3. The key verification process for authorized users

V. Experimental Results And Discussion

A. multi-user encryption framework performance

In this section, the encryption time, decryption time, and ciphertext bits of the multi-user encryption scheme are experimentally evaluated and compared with the same indicators in Cheng's single-user scheme [12], as shown in Table I.

As can be seen from Table I, the ciphertext expansion in the multi-user scheme is about 500 bits longer than that of a single user. This is because the process of scrambling by multiplying the original ciphertext matrix so as to increase the expansion of the ciphertext. However, compared with

Table I
PERFORMANCE COMPARISON OF ENCRYPTION SCHEMES

Encryption schemes	Encryption times	Decryption times	Ciphertext bits
Single-users	$0.0139s$	$0.0355s$	$1045\ bit$
Multi-users	$0.0168s$	$0.0554s$	$1554\ bit$

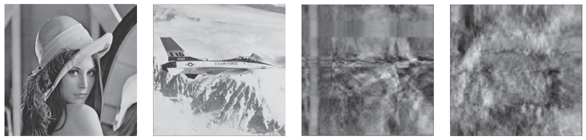
(a) (b) (c) (d)

Figure 4. False positive problem of singular value watermark, (a) original watermark image; (b) attacker watermark image; (c) attackers only replace component U; (d) attackers only replace component V.

the 2048-bit ciphertext extension of the Paillier encryption system, the multi-user ciphertext extension is within an acceptable range. In addition, the increase in encryption time is because the multi-user framework performs two rounds of encryption on the original image matrix. Decryption is more complicated than encryption, so the time increases.

B. the false positive experiement of singular value

When the attacker replaces the correct components originally sent to the AU with their own U and V components, the AU will not be able to extract the correct watermark, resulting in a wrong image copyright determination.

The experiments take Lena and Airplane as the original watermarked image and the attack watermarked image, as shown in Figure 4(a) and 4(b) respectively. It can be seen from Figure 4(c) and 4(d) that when attackers only replace one of U and V components of the original watermark image, the extracted watermark cannot visually identify the specific information. This result shows the importance of AU increasing the extraction watermark key verification step. It can reduce the possibility of the attacker to replace the original watermark information. When the attacker cannot simultaneously replace U and V components with their information, the copyright of the original data owner will be valid protection.

CONCLUSION

For the multi-user scenario, this paper uses the critical conversion method based on the invertible matrix to ensure the data isolation between each data owner while completing the wavelet transform and secure singular value decomposition operations under the ciphertext. To better and effectively disseminate ideas under the premise of protecting copyrights, this paper designs a verification mechanism to ensure the correct extraction of image watermarks to protect copyright information's integrity.

VI. ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 62172098; in part by the Natural Science Foundation of Fujian Province under Grant 2020J01497; Artificial Intelligence Education Technology Innovation Sharing Platform construction project of Fuzhou University; Corresponding author: Hang Cheng.

REFERENCES

[1] Erkin Z, Piva A, Katzenbeisser S, et al. Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing[J]. EURASIP Journal on Information Security, 2007, 2007: 1-20.

[2] Yao A C. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982: 160-164.

[3] Piva A, Katzenbeisser S. Signal processing in the encrypted domain[J]. EURASIP Journal on Information Security, 2007,: 1-1.

[4] Rewaria S. Data Privacy in Social Media Platform: Issues and Challenges[J]. Available at SSRN 3793386, 2021.

[5] Begum M, Uddin M S. Digital image watermarking techniques: a review[J]. Information, 2020, 11(2): 110.

[6] Peiyi HAN, Chuanyi LIU, Jiahui W, et al. Research on data encryption system and technology for cloud storage[J]. Journal on Communications, 2020, 41(8): 55.

[7] Yuanzhi YAO, Feng W, Wenbo YAN, et al. Image privacy preservation scheme based on QR code and reversible visible watermarking[J]. Journal on Communications, 2019, 40(11): 65.

[8] Xiao M, Li X, Wang Y, et al. Reversible data hiding based on pairwise embedding and optimal expansion path[J]. Signal Processing, 2019, 158: 210-218.

[9] Ishtiaq M, Ali W, Shahzad W, et al. Hybrid predictor based four-phase adaptive reversible watermarking[J]. IEEE Access, 2018, 6: 13213-13230.

[10] Nguyen T S, Chang C C, Yang X Q. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain[J]. AEU-International Journal of Electronics and Communications, 2016, 70(8): 1055-1061.

[11] Zhang X. Reversible data hiding in encrypted image[J]. IEEE signal processing letters, 2011, 18(4): 255-258.

[12] Cheng H, Huang Q, Chen F, et al. Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing[J]. IEEE Access, 2022, 10: 18570-18582.

[13] Xiao M, Li X, Wang Y, et al. Reversible data hiding based on pairwise embedding and optimal expansion path[J]. Signal Processing, 2019, 158: 210-218.

[14] Ishtiaq M, Ali W, Shahzad W, et al. Hybrid predictor based four-phase adaptive reversible watermarking[J]. IEEE Access, 2018, 6: 13213-13230.

[15] Nguyen T S, Chang C C, Yang X Q. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain[J]. AEU-International Journal of Electronics and Communications, 2016, 70(8): 1055-1061.