

FairCMS: Cloud Media Sharing with Fair Copyright Protection

Xiangli Xiao¹, Yushu Zhang², Leo Yu Zhang², Zhongyun Hua³, Zhe Liu⁴, and Jiwu Huang⁵

Abstract—The onerous media sharing task prompts resource-constrained media owners to seek help from a cloud platform, i.e., storing media contents in the cloud and letting the cloud do the sharing. There are three key security/privacy problems that need to be solved in the cloud media sharing scenario, including data privacy leakage and access control in the cloud, infringement on the owner’s copyright, and infringement on the user’s rights. In view of the fact that no single technique can solve the above three problems simultaneously, two cloud media sharing schemes are proposed in this paper, named FairCMS-I and FairCMS-II. By cleverly utilizing the proxy re-encryption technique and the asymmetric fingerprinting technique, FairCMS-I and FairCMS-II solve the above three problems with different privacy/efficiency trade-offs. Among them, FairCMS-I focuses more on cloud-side efficiency while FairCMS-II focuses more on the security of the media content, which provides owners with flexibility of choice. In addition, FairCMS-I and FairCMS-II also have advantages over existing cloud media sharing efforts in terms of optional IND-CPA (indistinguishability under chosen-plaintext attack) security and high cloud-side efficiency, as well as exemption from needing a trusted third party. Furthermore, FairCMS-I and FairCMS-II allow owners to reap significant local resource savings and thus can be seen as the privacy-preserving outsourcing of asymmetric fingerprinting. Finally, the feasibility and efficiency of FairCMS-I and FairCMS-II are demonstrated by experiments.

Index Terms—Cloud media sharing, asymmetric fingerprinting, proxy re-encryption, copyright protection.

I. INTRODUCTION

In day-to-day life, people are encountering an ever-growing volume of media big data through various social media platforms such as Facebook, Twitter, and WeChat. As a result, it has become increasingly common for media owners to share their contents with multiple users. To handle the vast number of users and media contents, the owner is typically required to deploy high-performance servers and broadband networks to cope with the onerous computing, storage, and communication

demands of copyright-protected media sharing solutions [1], [2]. While this may not be a challenge for media companies, it can be prohibitively expensive for individuals.

An intuitive approach to reduce overhead for the owner is to store the media contents in a cloud platform and, with the help of the cloud, share the media contents to the authorized users. It is evolving into an emerging technique called cloud media sharing [3], [4]. In this technique, on the one hand, the owner can make full use of the abundant software, hardware, and bandwidth resources of the cloud, thereby avoiding the expense of deploying servers and networks; on the other hand, the cloud can earn economic benefits by collecting rent from owners.

Despite the benefits of cloud media sharing, due to a variety of reasons such as curiosity, financial incentive, and reputation damage, there are still several security/privacy problems that have to be solved, as shown below.

Problem 1: Data privacy leakage and access control in the cloud. On the one hand, the cloud service provider could be curious about the data it encounters. On the other hand, it is a challenge to implement access control over the media content without direct control by the owner.

Problem 2: The infringement on the data owner’s copyright. Upon receiving the media content from the cloud, the authorized user could redistribute the owner’s media content arbitrarily. Clearly, it damages the owner’s copyright.

Problem 3: The infringement on the user’s rights. The owner may frame any user by falsely alleging that the user’s watermark has been found in an unauthorized content copy, while the fact is that this user’s watermark had been abused by the owner or adversaries. The possibility of launching a malicious incrimination on an honest user harms the user’s rights.

To solve *Problem 1*, cryptosystems implementing privacy-protected access control are required. Attribute-Based Encryption (ABE) [5], [6] is such a cryptosystem, in which a user’s credentials are described by attributes. A ciphertext can be decrypted by the user when the attributes pass the ciphertext’s access structure. Proxy Re-encryption (PRE) [7], [8] is another common cryptographic access control system, which allows the cloud to convert the owner’s ciphertext into a user’s ciphertext without knowing the plaintext version.

We then move on to discuss possible solutions to *Problems 2 and 3*. A watermarking technique being able to safeguard the user’s rights while maintaining the owner’s copyright is called Asymmetric Fingerprinting (AFP) [9]–[14]. AFP mainly relies on cryptographic tools including public key cryptosystem and homomorphic encryption, in which the embedding operation is performed in the ciphertext domain so that only the user

This work has been published in IEEE Transactions on Computational Social Systems, DOI: 10.1109/TCSS.2024.3374452.

This work was supported in part by the National Key R&D Program of China under Grant 2021YFB3100400 and in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant KYCX23_0397. (Corresponding author: Yushu Zhang and Leo Yu Zhang.)

X. Xiao, Y. Zhang, and Z. Liu are with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China (e-mail: xiaoxiangli@nuaa.edu.cn; yushu@nuaa.edu.cn; zhe.liu@nuaa.edu.cn).

L. Zhang is with the School of Information and Communication Technology, Griffith University, Southport QLD 4215, Australia (e-mail: leoci-tyu@gmail.com).

Z. Hua is with the School of Computer Science and Technology, Shenzhen Campus of Harbin Institute of Technology, Shenzhen 518055, China (e-mail: huazhongyun@hit.edu.cn).

J. Huang is with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: jwhuang@szu.edu.cn).

has access to his/her own fingerprint. Since the owner cannot acquire the user's personal fingerprint, he/she has no ability to frame honest users. Nevertheless, if the owner later finds a suspicious media copy, the malicious user can still be identified and proved guilty in front of a judge.

As discussed above, AFP seems to solve *Problems 2 and 3* perfectly. However, this is no longer the case when media contents are remotely hosted by the cloud since existing AFP schemes were designed without taking the cloud's involvement into consideration. Thus it remains to be further explored how to develop a novel AFP solution compatible with the system model of cloud media sharing. This is a challenging task, not even to mention that we also have to simultaneously protect the privacy of the data in the cloud, i.e., solving *Problem 1*.

There are two extra challenges that need to be addressed. For one thing, considering that the original purpose of cloud's involvement is to help resource-constrained owners efficiently share their media contents, the owner-side overhead needs to be carefully controlled to ensure that owners can obtain significant resource savings. For another, since the number and identity composition of target users generally cannot be determined accurately in advance, a practical cloud media sharing scheme should be scalable in the sense its capacity expands in real time as the number of subscriptions increases. PRE is better than ABE if the access policy changes frequently [3], [15]. Therefore, we tend to use PRE for scheme construction in this paper.

In this paper, facing these problems and challenges, we set out to solve them. First, to achieve data protection and access control, we adopt the lifted-ElGamal based PRE scheme, as discussed in [16]–[20], whose most prominent characteristic is that it satisfies the property of additive homomorphism. Then this homomorphism property is fully exploited to facilitate the integration with the Look-Up Table (LUT) based AFP scheme put forward by Bianchi *et al.* [10]. In this way, the cloud is successfully introduced to participate in the AFP solution, and the combination of the two technologies provides an approach to solve *Problems 1, 2, and 3* simultaneously.

According to the above idea, we propose two cloud media sharing schemes in this paper, i.e., FairCMS-I and FairCMS-II, which solve the above three problems with different privacy/efficiency trade-offs. Among them, FairCMS-I consumes fewer cloud resources, while FairCMS-II achieves better protection for the media content. The different encryption methods used by the two schemes for the media content stored in the cloud are responsible for this performance difference.

From the point of view of the owner side, both FairCMS-I and FairCMS-II can be regarded as the outsourcing of the LUT-based AFP [10], i.e., the owner can reap significant savings in the local storage, communication, and computing resources. Therefore, both schemes meet the requirement of owner-side efficiency, which is validated by the comprehensive theoretical analysis in Section VII and the experimental evaluation in Section VIII. Meanwhile, the two schemes meet the scalability requirement by performing re-encryption operations for each user. In addition, experiments are also carried out to demonstrate the excellent performance of the proposed two schemes in terms of perception quality and success tracing rate.

Finally, the major contributions of this paper are summarized as follows:

- Aiming at the situation that the existing techniques cannot fully meet the security/privacy requirements of cloud media sharing, we propose two novel schemes, namely FairCMS-I and FairCMS-II, to solve *Problems 1, 2, and 3* with different privacy/efficiency trade-offs, which are also qualified in terms of owner-side efficiency and scalability. Compared to existing schemes, FairCMS-I and FairCMS-II possess the advantages outlined in Table I.
- By delegating the management of the media content to the cloud, FairCMS-I and FairCMS-II can also be seen as an instantiation of privacy-preserving outsourcing of AFP, thereby solving the problem caused by insufficient local resources of the owner in media sharing.

The rest of this paper is outlined below. The next section reviews the related work. Section III describes the system model, threat model, and design goals. Subsequently, Section IV introduces the involved fundamental techniques. The two schemes are constructed in Section V. The performance of the two schemes regarding the three problems is evaluated in Section VI followed by the efficiency analysis in Section VII. The experimental results are reported in Section VIII. The last section concludes the paper.

II. RELATED WORK

Firstly, this work inherits from the privacy-protected cloud media sharing solutions based on ABE or PRE. Wu *et al.* [21] came up with an ABE scheme with multi-message ciphertext policy, which was implemented for scalable media sharing and access control based on the user's attributes. Polyakov *et al.* [22] proposed two multihop unidirectional PRE schemes for controlled publication and subscription of cloud data, which supports the transfer of proxy access rights. Liang *et al.* [23] defined and constructed a deterministic finite automata-based functional PRE scheme for public cloud data sharing without privacy leakage. After that, Li *et al.* [24] constructed a fine-grained and accountable access control system in the cloud, which traces suspicious access behaviors while ignores redistribution behaviors. Clearly, *Problems 2 and 3* are not considered in these works.

Secondly, this work is related to the AFP schemes. Rial *et al.* [13] proposed a provably secure anonymous AFP scheme based on the ideal-world/real-world paradigm. Poh *et al.* [25] designed an innovative user-side AFP scheme based on the symmetric Chameleon encryption technique, which achieves significant gains in owner-side computing and communication efficiency. Afterwards, Bianchi *et al.* [10] proposed a LUT-based AFP scheme without involving a Trusted Third Party (TTP) based on homomorphic encryption, which also implements AFP within the user-side framework. Despite the fact that *Problems 2 and 3* are solved in these works, *Problem 1* is not mentioned.

Thirdly, there are also studies that deal with both privacy-protected access control and traitor tracing. Xia *et al.* [26] introduced the watermarking technique to privacy-protected content-based ciphertext image retrieval in the cloud, which

TABLE I
COMPARISON WITH RELATED EXISTING SCHEMES

Schemes	Cloud's involvement	Problem 1		Cloud-side efficiency	TTP-free	Problems 2 and 3	
		Privacy protection	Access control			Protect the owner's copyright	Protect the user's rights
[21]–[24]	✓	✓	✓	✓	✓	×	×
[25]	×	—*	—*	—*	×	✓	✓
[10], [13]	×	—*	—*	—*	✓	✓	✓
[26]	✓	✓*	✓	✓	×	✓	✓
[27]	✓	✓	✓	×	×	✓	✓
[28]	✓	✓*	✓	×	✓	✓	✓
[3]-I*	✓	✓	✓	×	×	✓	✓
[3]-II*	✓	✓	✓	×	✓	✓	✓
FairCMS-I	✓	✓*	✓	✓	✓	✓	✓
FairCMS-II	✓	✓	✓	×	✓	✓	✓

* ‘—’ indicates that the property is not scored because the involvement of cloud is not considered. ✓ means that the privacy of cloud media is protected, but that protection is not IND-CPA secure. [3]-I and [3]-II represent the first scheme and the second scheme in [3], respectively. Compared with [3]-II, the main advantage of FairCMS-II is that it solves the problem that users can escape traceability by generating two different fingerprints, as discussed in the third last paragraph of Section V-A.

can prevent the user from illegally distributing the retrieved images. However, the fairness of the traitor tracing is only realized by the involvement of a TTP in the scheme. Moreover, the encryption of image features in the scheme is not IND-CPA secure. Zheng *et al.* [27] aimed to achieve differential access control and access history hiding on the cloud while enabling fair redistribution tracing by embedding watermarks homomorphically. However, the computing overhead on the cloud side would be onerous due to the need of performing re-encryption operations and homomorphic operations on the media content. Additionally, a TTP is still required to generate and encrypt watermarks for every user. Frattolillo *et al.* [28] proposed a multi-party watermarking scheme for the cloud's environment, which is able to solve the aforementioned three problems simultaneously. However, IND-CPA security is not satisfied in the scheme due to the adoption of commutative cryptosystem. Zhang *et al.* [3] combined PRE and fair watermarking to realize privacy-protected access control and combat content redistribution in the cloud, which also solves all three problems successfully. For one thing, compared with the first scheme of Zhang *et al.*, neither of our schemes requires the participation of a TTP. For another, compared with the second scheme of Zhang *et al.*, which does not require a TTP, in our proposed scheme FairCMS-I, the cloud only needs to perform homomorphic operations and re-encryption operations on the encrypted LUT and fingerprint instead of the encrypted media content. As LUTs and fingerprints are far shorter than the media content itself, FairCMS-I consumes much fewer cloud resources than that of [3] (the cloud-side overhead of the two schemes in [3] is the same). Furthermore, in the second scheme of Zhang *et al.*, the user can escape traceability by generating two different fingerprints (we discuss this in detail in the third last paragraph of Section V-A), and both FairCMS-I and FairCMS-II solve this problem.

Finally, the comparison between the two proposed schemes and the existing relevant schemes is summarized in Table I. As can be seen therein, the two proposed schemes FairCMS-I and FairCMS-II have advantages over the existing works. In addition, the two proposed schemes offer owners the flexibility

to choose. If the security requirements for the media content are not excessively rigorous and the size of the media content is small (e.g., images with a moderate pixel count), the owner can choose FairCMS-I to minimize the cost of renting cloud resources; otherwise, the owner can choose FairCMS-II. There is no fixed security requirement or content size threshold to guide the selection between these two options. Instead, it is up to the owner to make a decision based on the objective application scenario and his/her subjective considerations. In Section VIII, we conduct a comparative experiment on the cloud-side efficiency of FairCMS-I and FairCMS-II to provide a quantitative reference for the owner's decision-making.

III. PROBLEM STATEMENT

A. System Model

As illustrated in Fig. 1, our system model mainly consists of four entities: the owner, the cloud, users, and the judge. Their roles are elaborated as follows.

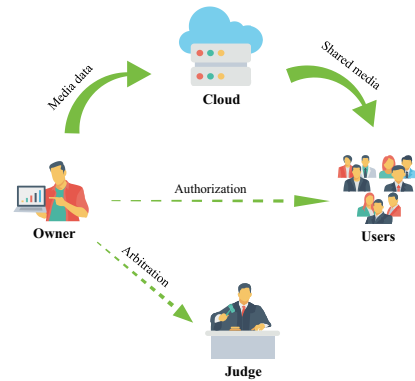


Fig. 1. System Model.

- **Owner.** The owner, who might be a media producer or trader, plans to store the media content in the cloud and let the cloud do the content distribution. First, the owner requires that the cloud not be able to obtain the plaintext about the media content and the LUTs, and that access to

the media content is controlled by his/her authorization. Second, the owner asks for significant overhead savings from cloud media sharing. Third, the owner demands traitor tracing of users who violate copyright. If a suspicious redistributed copy of the media content is found, the owner can file an arbitration claim with the judge.

- **Cloud.** The cloud has a wealth of hardware, software, and bandwidth resources, part of which are lent to the owner through a pay-per-use way to help the owner carry out media sharing.
- **Users.** Users want to access the owner's media content. To this end, users request authorization from the owner, for example by paying for purchases. If successful, users can get the desired shared media content from the cloud. Users require that the plaintext of their fingerprints not be accessed by the owner or the cloud, to prevent malicious framing by the owner.
- **Judge.** The judge is a trusted entity who is only responsible for arbitration in the case of illegal redistribution, as in existing traitor tracing systems [3], [10]–[14]. After receiving the owner's request for arbitration, the judge makes a fair judgment based on the evidence provided by the owner. Although only the encrypted version of the user's watermark is disclosed, the encrypted watermark can be converted into a ciphertext that can be decrypted by the judge based on PRE (for details, please see Figs. 3 and 4), thus enabling traitor tracing. Once the judge detects a copyright infringement, the unfaithful user will be prosecuted in accordance with the law.

B. Threat Model

The threats considered in this paper come from three entities: users, the owner, and the cloud. First, users are assumed to be malicious, who could illegally redistribute the owner's media content with the hope that this behavior will not be detected. Second, the owner is also assumed to be malicious, who may try to obtain the users' fingerprints and maliciously embed the fingerprints into any media content to frame honest users for copyright infringement. Third, the cloud is assumed to be honest-but-curious, which is the same as other privacy-preserving cloud media sharing schemes based on ABE or PRE [7], [15], [21], [23], [29]. Although the honest-but-curious cloud faithfully performs its assigned duties, he/she could try to steal the plaintext about the owner's media content. Moreover, the cloud is also curious about other information it encounters, including the users' fingerprints and the LUTs. Finally, as in [28], we assume that there may exist collusion among individual users and collusion between the owner and the cloud, while there is no collusion between users and the cloud.

C. Design Goals

Under the above system model and threat model, we summarize the design goals as follows.

- **Implement privacy-preserving access control.** On the one hand, the cloud should be prevented from obtaining the private plaintext of the data it encounters, including

the owner's media content, the users' fingerprints, and the LUTs. On the other hand, only users authorized by the owner can access the media content.

- **Protect the owner's copyright.** We need to embed the user's fingerprint in the owner's media content to enable traitor tracing. As long as an unfaithful user makes an unauthorized redistribution, he/she can be detected by the embedded fingerprint in the media content.
- **Protect the user's right.** We need to prevent the owner from framing an honest user for copyright infringement by embedding this user's fingerprint in any media content.
- **Ensure efficiency gains and scalability.** For one thing, we need to carefully control the owner-side overhead to ensure that the owner can gain significant local resource savings from cloud media sharing. For another, we need to ensure that the two proposed schemes are scalable to handle real-time requests from users.
- **TTP-free.** The two proposed schemes should not require any TTP to participate in the media sharing process. The TTP mentioned here does not cover the judge, who is only responsible for handing down sentences in cases of suspected redistribution and is not involved in the media sharing process. The judge is an indispensable participant. In contrast, the existing schemes [3], [26], [27] that are not TTP-free all require a TTP to remain online during media sharing to generate watermarks for users.

IV. FUNDAMENTAL TECHNIQUES

A. LUT-Based Secure Embedding

For better understanding, we start with the introduction of a LUT-based watermarking scheme [30], [31], which is the basis of the AFP scheme proposed by Bianchi *et al.* [10].

1) *Key Generation:* First, the owner creates a $T \times 1$ encryption LUT (E-LUT) $\mathbf{E}$ with its entry $\mathbf{E}(t)$ ($0 \leq t \leq T-1$) following the Gaussian distribution $N(0, \sigma_E)$. Then, for the k -th user, his/her personalized decryption LUT (D-LUT) $\mathbf{D}_k$ is obtained by modifying the E-LUT as

$$\mathbf{D}_k = -\mathbf{E} + \mathbf{W}_k,$$

where $\mathbf{W}_k$ is the k -th user's personalized watermarking LUT (W-LUT) that is generated by

$$\mathbf{W}_k = \mathbf{G}\mathbf{w}_k,$$

where $\mathbf{G}$ is a $T \times L$ encoding matrix [10], [32], [33] and the vector $\mathbf{w}_k = [w_{k,l}]_{l=0}^{L-1}$ is computed by $w_{k,l} = \sigma_W(2b_{k,l} - 1)$. Here, σ_W is a public parameter utilized to set the standard deviation of $\mathbf{W}_k$ and $\mathbf{b}_k = [b_{k,l}]_{l=0}^{L-1}$ is the k -th user's L -bit uniform binary fingerprint.

2) *Encryption:* Based on the E-LUT $\mathbf{E}$, the owner encrypts the media content using the single-value alteration method. Assume that the media content can be represented as a vector $\mathbf{m}$ of length M , the encryption method used here can be expressed as

$$\mathbf{c} = \mathbf{m} + \mathbf{B}^m \mathbf{E}, \quad (1)$$

where $\mathbf{B}^m$ is a $M \times T$ binary matrix defined as

$$\mathbf{B}^m(i, j) = \begin{cases} 1, & j = t_{ih}, \\ 0, & \text{otherwise,} \end{cases}$$

where t_{ih} ($0 \leq i \leq M-1, 0 \leq h \leq S-1$) is a set of $M \times S$ values in the range $[0, T-1]$. The generation of t_{ih} is controlled by an index generator under a session key SK_m .

3) *Joint Decryption and Fingerprinting*: Upon receiving the k -th user's request, the owner sends $\mathbf{c}$ to the k -th user who performs joint decryption and fingerprinting with the D-LUT $\mathbf{D}_k$ to obtain his/her personalized fingerprinted media content $\mathbf{m}^k$ by performing

$$\mathbf{m}^k = \mathbf{c} + \mathbf{B}^m \mathbf{D}_k. \quad (2)$$

Note that Eq. (2) can be calculated as

$$\begin{aligned} \mathbf{m}^k &= \mathbf{c} + \mathbf{B}^m \mathbf{D}_k \\ &= \mathbf{m} + \mathbf{B}^m \mathbf{E} + \mathbf{B}^m \mathbf{D}_k \\ &= \mathbf{m} + \sigma_W \bar{\mathbf{G}} (2\mathbf{b}_k - 1), \end{aligned} \quad (3)$$

where $\bar{\mathbf{G}} = \mathbf{B}^m \mathbf{G}$. It is clear from Eq. (3) that the fingerprint $\mathbf{b}_k$ has been successfully embedded into the original media content $\mathbf{m}$ under the modulation of the secret matrix $\bar{\mathbf{G}}$.

4) *Fingerprint Detection and Traitor Tracing*: Once a copy-right dispute occurs between the owner and the user, they delegate a judge that is credible for both parties to make a fair arbitration. Due to the possible noise effect during data transmission, the received suspicious media content copy is assumed to be contaminated by the an additive noise $\mathbf{n}$, i.e.,

$$\begin{aligned} \tilde{\mathbf{m}}^k &= \mathbf{m} + \bar{\mathbf{G}} \tilde{\mathbf{w}}_k + \mathbf{n} \\ &= \mathbf{m} + \sigma_W \bar{\mathbf{G}} (2\tilde{\mathbf{b}}_k - 1) + \mathbf{n}, \end{aligned}$$

where $\tilde{\mathbf{b}}_k$ is the suspicious user's fingerprint.

In order to detect the fingerprint $\tilde{\mathbf{b}}_k$, the judge can leverage the suboptimal decoders such as the Matched Filter decoder and the Pseudo-Inverse decoder [10], which are respectively formulated as

$$\tilde{\mathbf{b}}_k = \text{sgn} \{ \bar{\mathbf{G}}^T (\tilde{\mathbf{m}}^k - \mathbf{m}) \}, \quad (4)$$

and

$$\tilde{\mathbf{b}}_k = \text{sgn} \{ (\bar{\mathbf{G}}^T \bar{\mathbf{G}})^{-1} \bar{\mathbf{G}}^T (\tilde{\mathbf{m}}^k - \mathbf{m}) \}, \quad (5)$$

where

$$\text{sgn} \{ \zeta \} = \begin{cases} 1, & \zeta > 0, \\ 0, & \zeta \leq 0. \end{cases}$$

If $\tilde{\mathbf{b}}_k = \mathbf{b}_k$ is established within the allowable error range, the judge rule that the k -th user has illegally redistributed the owner's media; otherwise, the k -th user is proved innocent.

B. AFP Based on User-Side Embedding

Given the above arithmetics of the LUT-based user-side embedding in the plaintext domain, the additive homomorphism is used to implement the secure distribution of D-LUTs in the ciphertext domain [10].

1) *Additive Homomorphism*: Suppose that $E_{PK}(\cdot)$ is the additive homomorphic encryption under the public key PK . By saying additive homomorphism, $E_{PK}(\cdot)$ satisfies the following equations:

$$\begin{aligned} E_{PK}(m_1 + m_2) &= E_{PK}(m_1) \cdot E_{PK}(m_2), \\ E_{PK}(a \cdot m) &= E_{PK}(m)^a, \end{aligned} \quad (6)$$

where m_1, m_2 , and m are plaintexts, and a is an integer.

2) *Secure Distribution of D-LUTs*: First, the k -th user generates his/her fingerprint $\mathbf{b}_k$ locally and encrypts it with his/her public key PK_{U_k} , i.e., $E_{PK_{U_k}}(\mathbf{b}_k) = [E_{PK_{U_k}}(b_{k,0}), E_{PK_{U_k}}(b_{k,1}), \dots, E_{PK_{U_k}}(b_{k,L-1})]$. Then, the k -th user sends $E_{PK_{U_k}}(\mathbf{b}_k)$ to the owner. After receiving $E_{PK_{U_k}}(\mathbf{b}_k)$, the owner calculates $\mathbf{w}_k$ in the ciphertext domain by

$$\begin{aligned} E_{PK_{U_k}}(w_{k,l}) &= E_{PK_{U_k}}(2b_{k,l} - 1)^{\sigma_W} \\ &= E_{PK_{U_k}}(b_{k,l})^{2\sigma_W} \cdot E_{PK_{U_k}}(1)^{-\sigma_W}, \end{aligned} \quad (7)$$

and further calculates

$$\begin{aligned} E_{PK_{U_k}}(\mathbf{D}_k(t)) &= E_{PK_{U_k}}(\mathbf{E}(t))^{-1} \cdot \prod_{l=0}^{L-1} E_{PK_{U_k}}(w_{k,l})^{\mathbf{G}(t,l)}, \end{aligned} \quad (8)$$

where $0 \leq t \leq T-1$. $E_{PK_{U_k}}(\mathbf{D}_k(t))$ is then sent to the k -th user, who can acquire his/her personalized D-LUT through decryption with his/her private key SK_{U_k} .

Through the above steps, the owner and the k -th user are prevented from knowing the plaintext of $\mathbf{b}_k$ and the plaintext of $\mathbf{G}$ (and $\bar{\mathbf{G}}$) respectively, i.e., neither of them know the value of the embedded watermark $\bar{\mathbf{G}}\mathbf{w}_k$, thus achieving simultaneous protection of the owner's copyright and the users' rights.

C. Additive Homomorphic PRE

The lifted-ElGamal based PRE scheme [16]–[20] is summarized as follows.

Let G_1, G_2 be two multiplicative cyclic groups of prime order q with a bilinear map $e : G_1 \times G_1 \rightarrow G_2$, and g be a random generator of G_1 . The mapping e has three properties. 1) Bilinearity: for any $a, b \in \mathbb{Z}_q$, $e(g^a, g^b) = e(g, g)^{ab}$. 2) Non-degeneracy: $e(g, g) \neq 1$. 3) Computability: e can be efficiently computed.

With bilinear pairing, the lifted-ElGamal based PRE technique is comprised of the following algorithms by using the public parameters G_1, G_2, q, e, g and $Z = e(g, g) \in G_2$.

- **Key Generation (KG)**. A user A 's key pair is of the form $PK_A = (Z^{a_1}, g^{a_2})$ and $SK_A = (a_1, a_2)$, and a user B 's key pair is of the form $PK_B = (Z^{b_1}, g^{b_2})$ and $SK_B = (b_1, b_2)$.
- **Re-encryption Key Generation (RG)**. A user A authorizes B access to A 's data by publishing the re-encryption key $rk_{A \rightarrow B} = (g^{b_2})^{a_1} = g^{a_1 b_2} \in G_1$, computed from A 's private key and B 's public key¹.
- **First-Level Encryption (E^1)**. To encrypt a message $m \in \mathbb{Z}_q$ under PK_A in such a way that it can only be decrypted by the holder of SK_A , the scheme computes $E_{PK_A}^1(m) = (Z^{a_1 r}, Z^m Z^r)$, where r is a random number from $\mathbb{Z}_q$.
- **Second-Level Encryption (E^2)**. To encrypt a message $m \in \mathbb{Z}_q$ under PK_A in such a way that it can be decrypted by A and his/her delegates, the scheme outputs $E_{PK_A}^2(m) = (g^r, Z^m Z^{a_1 r})$.

¹One single user A can also generate a re-encryption key for himself to change the second-level ciphertext into the first-level, we denote this key as $rk_{A^2 \rightarrow A^1} = (g^{a_2})^{a_1} = g^{a_1 a_2}$.

- **Re-encryption (R).** Anyone can change a second-level ciphertext for A into a first-level ciphertext for B with $rk_{A \rightarrow B} = g^{a_1 b_2}$. From $E_{PK_A}^2(m) = (g^r, Z^m Z^{a_1 r})$, the scheme computes $e(g^r, g^{a_1 b_2}) = Z^{b_2 a_1 r}$ and publishes $E_{PK_B}^1(m) = (Z^{b_2 a_1 r}, Z^m Z^{a_1 r}) = (Z^{b_2 r'}, Z^m Z^{r'})$.
- **Decryption (D^1, D^2).** To decrypt a first-level ciphertext $E_{PK_A}^1(m) = (Z^{a_i r}, Z^m Z^r) = (\alpha, \beta)$ with private key $a_i \in SK_A$, the scheme computes $m' = Z^m = \frac{\beta}{\alpha^{1/a_i}}$ for $i \in \{1, 2\}$. To decrypt a second-level ciphertext $E_{PK_A}^2(m) = (g^r, Z^m Z^{a_1 r}) = (\alpha, \beta)$ with secret key $a_1 \in SK_A$, the scheme outputs $m' = Z^m = \frac{\beta}{e(\alpha, g)^{a_1}}$.

To get the plaintext m , the above mentioned PRE scheme requires computing the discrete logarithm of m' in the base Z , i.e., $m = \log_Z m'$. Although this sounds restrictive, there is no limitation to the use of the lifted-ElGamal based PRE scheme as long as the plaintext space is small, as also pointed out by many other literature works [17]–[20]. In our experiment, the lookup table method [34] is used to solve the discrete logarithm. It is worth emphasizing that the private key is still secure because of its huge value space. For example, in the experiment we quantify the plaintext to 20 bits, whereas the private key is typically 1,024 bits or longer. Note that the value space doubles for each additional bit.

The most important feature of this PRE scheme is that both the first-level ciphertext and the second-level ciphertext satisfy the property of additive homomorphism, i.e.,

$$\begin{aligned} E_{PK_A}^1(m_1) \cdot E_{PK_A}^1(m_2) &= (Z^{a_i r_1} \cdot Z^{a_i r_2}, Z^{m_1} Z^{r_1} \cdot Z^{m_2} Z^{r_2}) \\ &= (Z^{a_i(r_1+r_2)}, Z^{m_1+m_2} Z^{r_1+r_2}) \\ &= E_{PK_A}^1(m_1 + m_2), \\ E_{PK_A}^2(m_1) \cdot E_{PK_A}^2(m_2) &= (g^{r_1} \cdot g^{r_2}, Z^{m_1} Z^{a_i r_1} \cdot Z^{m_2} Z^{a_i r_2}) \\ &= (g^{r_1+r_2}, Z^{m_1+m_2} Z^{a_i(r_1+r_2)}) \\ &= E_{PK_A}^2(m_1 + m_2), \end{aligned}$$

where r_1 and r_2 are random numbers in Z_q , and $i \in \{1, 2\}$. In addition, we emphasize that the second line in Eq. (6) is also satisfied, and the verification is similar to the above.

V. SCHEME CONSTRUCTION

In this section, we bring forward two cloud media sharing schemes, namely FairCMS-I and FairCMS-II. FairCMS-I essentially delegates the re-encryption management of LUTs to the cloud, thus significantly reducing the overhead of the owner side. Nevertheless, FairCMS-I cannot achieve IND-CPA security for the media content. Therefore, we further propose a more secure scheme FairCMS-II, which delegates the re-encryption management of both media content and LUTs to the cloud.

A. Scheme of FairCMS-I

In the user-side embedding AFP, since the encrypted media content shared with different users is the same, the encryption of the media content is only executed once. In contrast, due to the personalization of D-LUTs, once a new user initiates a request, the owner must interact with this user to securely distribute the D-LUT under the support of homomorphic encryption. This cost scales linearly with the number of users.

It is clear that the biggest source of overhead for the owner is the management and distribution of LUTs. Therefore, the focus of implementing resource-saving cloud media sharing is to find ways to transfer this overhead to the cloud. Based on this observation, the first scheme is as follows.

Key, Fingerprint, E-LUT, and Encoding Matrix Generation:

Based on the lifted-ElGamal based PRE scheme introduced in Section IV-C, the k -th user U_k generates his/her public key $PK_{U_k} = (Z^{a_1}, g^{a_2})$ and private key $SK_{U_k} = (a_1, a_2)$. In addition, the owner O generates his/her own public key $PK_O = (Z^{b_1}, g^{b_2})$ and private key $SK_O = (b_1, b_2)$, and the judge J also generates the key pair as $PK_J = (Z^{c_1}, g^{c_2})$ and $SK_J = (c_1, c_2)$. Moreover, the k -th user generates his/her private fingerprint $\mathbf{b}_k$ locally, and the owner generates a E-LUT $\mathbf{E}$ and a encoding matrix $\mathbf{G}$ locally.

Calculation and Distribution of D-LUTs:

The k -th user encrypts his/her private fingerprint $\mathbf{b}_k$ into a second-level ciphertext $E_{PK_{U_k}}^2(\mathbf{b}_k)$ using his/her public key Z^{a_1} , namely $E_{PK_{U_k}}^2(\mathbf{b}_k) = [(g^{r_0}, Z^{b_{k,0}} Z^{a_1 r_0}), \dots, (g^{r_{L-1}}, Z^{b_{k,L-1}} Z^{a_1 r_{L-1}})]$, and then sends $E_{PK_{U_k}}^2(\mathbf{b}_k)$ to the cloud. In addition, the k -th user also generates a re-encryption key $rk_{U_k^2 \rightarrow U_k^1} = g^{a_1 a_2}$ with his/her private key $SK_{U_k} = a_1$ and his/her public key $PK_{U_k} = g^{a_2}$, and generates another re-encryption key $rk_{U_k \rightarrow J} = g^{a_1 c_2}$ with his/her private key $SK_{U_k} = a_1$ and the judge's public key $PK_J = g^{c_2}$, then sends the two re-encryption keys to the cloud.

The owner encrypts the E-LUT $\mathbf{E}$ into a second-level ciphertext $E_{PK_O}^2(\mathbf{E}(t))$ ($0 \leq t \leq T-1$) using his/her public key $PK_O = Z^{b_1}$, i.e., $E_{PK_O}^2(\mathbf{E}(t)) = (g^r, Z^{\mathbf{E}(t)} Z^{b_1 r})$, and sends $E_{PK_O}^2(\mathbf{E}(t))$ together with $\mathbf{G}$ to the cloud, who then stores $E_{PK_O}^2(\mathbf{E}(t))$ and $\mathbf{G}$. In addition, the owner O generates a re-encryption key $rk_{O \rightarrow U_k}$ under his/her private key $SK_O = b_1$ and the k -th user's public key $PK_{U_k} = g^{a_2}$, i.e., $rk_{O \rightarrow U_k} = g^{b_1 a_2}$, and then sends $rk_{O \rightarrow U_k}$ to the cloud.

The cloud uses the re-encryption key $rk_{O \rightarrow U_k}$ to change the received encrypted E-LUT under the owner's key, i.e., $E_{PK_O}^2(\mathbf{E}(t))$, into $E_{PK_{U_k}}^1(\mathbf{E}(t))$, which is the first-level ciphertext of the k -th user. Furthermore, the cloud changes $E_{PK_{U_k}}^2(\mathbf{b}_k)$ into $E_{PK_{U_k}}^1(\mathbf{b}_k)$ using $rk_{U_k^2 \rightarrow U_k^1}$ and changes $E_{PK_{U_k}}^2(\mathbf{b}_k)$ into $E_{PK_J}^1(\mathbf{b}_k)$ using $rk_{U_k \rightarrow J}$, and then stores $E_{PK_J}^1(\mathbf{b}_k)$ into a set $\mathcal{F}$. Subsequently, the cloud calculates $E_{PK_{U_k}}^1(\mathbf{D}_k(t))$ with $E_{PK_{U_k}}^1(\mathbf{E}(t))$, $E_{PK_{U_k}}^1(\mathbf{b}_k)$, and $\mathbf{G}$ by Eqs. (7) and (8). We emphasize that this process can be performed successfully because the first level ciphertext of the lifted-ElGamal based PRE scheme satisfies the property of additive homomorphism. Finally, the cloud sends $E_{PK_{U_k}}^1(\mathbf{D}_k(t))$ back to the k -th user, who acquires his/her personalized D-LUT $\mathbf{D}_k$ through decryption with his/her private key $SK_{U_k} = a_2$.

Cloud-Based Media Sharing:

The owner encrypts the media content collection $\{\mathbf{m}\}$ to be shared using the single-value alteration method and sends the resulting encrypted media content collection $\{\mathbf{c}\}$ to the cloud, who then stores the encrypted media content collection. In addition, the owner sends the binary matrix collection $\{\mathbf{B}^m\}$ used in the encryption process to the cloud, which is generated

Input: Security parameter λ .
Output: The cloud stores $\{\bar{\mathbf{G}}\}$, $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{\mathbf{c}\}$.
Procedure:
Owner:

- Generate $(\mathbf{E}, \mathbf{G}, PK_O, SK_O, \{SK_m\})$,
- $E_{PK_O}^2(\mathbf{E}(t)) \leftarrow (\mathbf{E}(t), PK_O)$,
- $\{t_{ih}\} \leftarrow \{SK_m\}$,
- $\{\mathbf{B}^m\} \leftarrow \{t_{ih}\}$,
- $\{\mathbf{c}\} \leftarrow (\{\mathbf{m}\}, \{\mathbf{B}^m\}, \mathbf{E})$,
- Send $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{\mathbf{c}\}$ to the cloud.

Cloud:

- $\{\bar{\mathbf{G}}\} \leftarrow (\{\mathbf{B}^m\}, \mathbf{G})$,
- Store $\{\bar{\mathbf{G}}\}$, $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{\mathbf{c}\}$.

Fig. 2. FairCMS-I: Media storage (**Part 1**).

locally by the owner based on the session keys and is utilized for encrypting each media content.

The cloud calculates the secret matrix collection $\{\bar{\mathbf{G}}\}$ with the binary matrix collection $\{\mathbf{B}^m\}$ and the encoding matrix $\mathbf{G}$, and then stores the secret matrix collection and the binary matrix collection. Suppose the k -th user expects to access one of the owner's media content $\mathbf{m}$. The cloud then extracts the encryption result $\mathbf{c}$ of the media content $\mathbf{m}$ from the encrypted media content collection, i.e., $\mathbf{c} = \mathbf{m} + \mathbf{B}^m \mathbf{E}$, and sends $\mathbf{c}$ to this user. Meanwhile, the corresponding binary matrix $\mathbf{B}^m$ is also extracted from the binary matrix collection by the cloud and sends to the k -th user. Finally, the k -th user decrypts $\mathbf{c}$ with his/her personalized D-LUT $\mathbf{D}_k$ and the binary matrix $\mathbf{B}^m$ based on Eq. (3) to get the fingerprint embedded media content $\mathbf{m}^k$.

Arbitration and Traitor Tracing:

Upon the detection of a suspicious media content copy $\tilde{\mathbf{m}}^k$, the owner resorts to the judge for violation identification. To this end, the proofs that the owner needs to provide the judge includes the original media content $\mathbf{m}$ with no fingerprints embedded, the corresponding secret matrix $\bar{\mathbf{G}}$, and the set $\mathcal{F}$ that holds all the users' fingerprints. Among them, $\bar{\mathbf{G}}$ and $\mathcal{F}$ is available for download by the owner from the cloud. It is worth mentioning that the fingerprints stored in set $\mathcal{F}$ are encrypted by the judge's public key PK_J , so the user's fingerprint will not be leaked to the owner and the cloud, but the plaintext of the fingerprints can be decrypted by the judge with his/her own private key $SK_J = c_2$. With these materials, the judge can make a fair judgment by Eq. (4) or (5).

Summary and Discussion:

The whole FairCMS-I scheme is summarized as follows. First, suppose an owner rents the cloud's resources for media sharing, the owner and the cloud execute **Part 1** as shown in Fig. 2. Then, suppose the k -th user makes a request indicating that he/she wants to access one of the owner's media content $\mathbf{m}$, the involved entities execute **Part 2** after the k -th user is authorized by the owner as shown in Fig. 3. Once a suspicious media content copy $\tilde{\mathbf{m}}^k$ is detected, the owner resorts to the judge for violation arbitration, i.e., the owner and the judge jointly execute **Part 3** as shown in Fig. 4.

Input: Security parameter λ , $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{\mathbf{c}\}$.
Output: The k -th user obtains the watermarked media content $\mathbf{m}^k$.
Procedure:
 k -th User:

- Generate $(\mathbf{b}_k, PK_{U_k}, SK_{U_k})$,
- $E_{PK_{U_k}}^2(\mathbf{b}_k) \leftarrow (\mathbf{b}_k, PK_{U_k})$,
- $rk_{U_k^2 \rightarrow U_k^1} \leftarrow (SK_{U_k}, PK_{U_k})$,
- $rk_{U_k \rightarrow J} \leftarrow (SK_{U_k}, PK_J)$,
- Send $E_{PK_{U_k}}^2(\mathbf{b}_k)$, $rk_{U_k^2 \rightarrow U_k^1}$, and $rk_{U_k \rightarrow J}$ to the cloud.

Owner:

- $rk_{O \rightarrow U_k} \leftarrow (SK_O, PK_{U_k})$,
- Send $rk_{O \rightarrow U_k}$ to the cloud.

Cloud:

- $E_{PK_{U_k}}^1(\mathbf{E}(t)) \leftarrow (E_{PK_O}^2(\mathbf{E}(t)), rk_{O \rightarrow U_k})$,
- $E_{PK_{U_k}}^1(\mathbf{b}_k) \leftarrow (E_{PK_{U_k}}^2(\mathbf{b}_k), rk_{U_k^2 \rightarrow U_k^1})$,
- $E_{PK_J}^1(\mathbf{b}_k) \leftarrow (E_{PK_{U_k}}^2(\mathbf{b}_k), rk_{U_k \rightarrow J})$,
- Store $E_{PK_J}^1(\mathbf{b}_k)$ into a set $\mathcal{F}$,
- $E_{PK_{U_k}}^1(\mathbf{D}_k(t)) \leftarrow (E_{PK_{U_k}}^1(\mathbf{E}(t)), E_{PK_{U_k}}^1(\mathbf{b}_k), \mathbf{G})$,
- Extract the corresponding $\mathbf{c}$ from $\{\mathbf{c}\}$,
- Extract the corresponding $\mathbf{B}^m$ from $\{\mathbf{B}^m\}$,
- Send $E_{PK_{U_k}}^1(\mathbf{D}_k(t))$, $\mathbf{c}$, and $\mathbf{B}^m$ to the k -th user.

k -th User:

- $\mathbf{D}_k(t) \leftarrow (E_{PK_{U_k}}^1(\mathbf{D}_k(t)), SK_{U_k})$,
- $\mathbf{m}^k \leftarrow (\mathbf{c}, \mathbf{B}^m, \mathbf{D}_k)$.

Fig. 3. FairCMS-I: Media sharing (**Part 2**).

Input: The suspicious media content $\tilde{\mathbf{m}}^k$, $\{\bar{\mathbf{G}}\}$, the original media content $\mathbf{m}$, and the set of fingerprints $\mathcal{F}$.
Output: The judge finds the copyright violator.
Procedure:
Owner:

- Extract and download the corresponding $\bar{\mathbf{G}}$ from the cloud,
- Download the set $\mathcal{F}$ from the cloud,
- Send $\mathbf{m}$, $\bar{\mathbf{G}}$, and $\mathcal{F}$ to the judge.

Judge:

- Decrypt the fingerprints in the set $\mathcal{F}$ with the private key SK_J of the judge,
- $\tilde{\mathbf{b}}_k \leftarrow (\tilde{\mathbf{m}}^k, \bar{\mathbf{G}}, \mathbf{m})$,
- Compare $\tilde{\mathbf{b}}_k$ to the decrypted fingerprints in $\mathcal{F}$.

Fig. 4. FairCMS-I: Traitor tracing (**Part 3**).

We emphasize that **Part 1** is just an initialization step that only needs to be executed once before media sharing begins, while **Part 2** is executed upon requesting of media content copy from each authorized user. **Part 3** is only executed for each detected suspicious media content copy. Therefore, in the case of a large number of users, the owner's overhead in **Part 2** should be the primary concern for a media sharing system. Fortunately, in our design, by delegating the operations

securely to the cloud, now in **Part 2** the owner only needs to calculate and send a re-encryption key, which only incurs negligible overhead. As a result, this scheme well solves the bottleneck caused by insufficient owner-side resources. Also, since **Part 2** is executed online for each user, this scheme clearly meets the scalability requirements. The achievement of the three security goals of FairCMS-I will be discussed in detail in Section VI.

In addition, it is noted that two re-encryption keys $rk_{U_k \rightarrow U_k^1}$ and $rk_{U_k \rightarrow J}$ are used in the scheme to protect the users' fingerprints. Among them, $rk_{U_k \rightarrow U_k^1}$ is used to change $E_{PK_{U_k}}^2(\mathbf{b}_k)$ into $E_{PK_{U_k}}^1(\mathbf{b}_k)$, and $rk_{U_k \rightarrow J}$ is used to change $E_{PK_{U_k}}^2(\mathbf{b}_k)$ into $E_{PK_J}^1(\mathbf{b}_k)$. In comparison, the method adopted in [3] is that the k -th user encrypts his/her fingerprint $\mathbf{b}_k$ with his/her public key PK_{U_k} and judge's public key PK_J respectively, and then sends the two results $E_{PK_{U_k}}^1(\mathbf{b}_k)$ and $E_{PK_J}^1(\mathbf{b}_k)$ to the cloud. However, in this case, an unfaithful user can evade traitor tracing by producing two different fingerprints, i.e., a $\mathbf{b}'_k$ is used to produce $E_{PK_{U_k}}^1(\mathbf{b}'_k)$ and another $\mathbf{b}''_k$ is used to produce $E_{PK_J}^1(\mathbf{b}''_k)$. Our proposed scheme avoids this vulnerability because the user only has freedom to generate one fingerprint $\mathbf{b}_k$, and $E_{PK_{U_k}}^1(\mathbf{b}_k)$ (for fingerprint embedding) and $E_{PK_J}^1(\mathbf{b}_k)$ (for traitor tracing) are re-encryption results of the same second-level ciphertext $E_{PK_{U_k}}^2(\mathbf{b}_k)$.

Moreover, FairCMS-I does not perform any processing on the encrypted media content stored in the cloud, but only performs homomorphic operations and re-encryption operations on the encrypted LUT and fingerprint that are much smaller in size, which results in outstanding cloud-side efficiency. In contrast, the two schemes proposed by Zhang *et al.* [3] both require homomorphic operations and re-encryption operations on the media content, which obviously consumes a lot more cloud resources. This means that FairCMS-I can save users a large amount of cost of renting cloud resources, thus achieving one of the prominent advantages of our work.

Finally, we emphasize that the attack from the communication channel is not considered in the adopted threat model, so $\mathbf{B}^m$, $\mathbf{G}$, and $\bar{\mathbf{G}}$ are all transmitted in plaintext. In practical applications, if the communication channel does not meet this assumption, simple modifications can be made to the proposed scheme. On the one hand, we can use public key cryptography to encrypt the transmitted plaintext. For example, in **Part 1** the owner can encrypt $\mathbf{G}$ with the cloud's public key PK_C before sending it to the cloud, who then decrypts $E_{PK_C}(\mathbf{G})$ with his/her own private key SK_C . On the other hand, the same $\mathbf{B}^m$ can be generated on different entities by sharing the session key SK_m , in the same way as in the AFP scheme. Meanwhile, bandwidth savings can also be obtained by transferring SK_m instead of $\mathbf{B}^m$. Apart from the above, message authentication code and digital signature can also be added if integrity and source authentication are needed.

B. Scheme of FairCMS-II

The encryption and decryption on the media content $\mathbf{m}$ in FairCMS-I are essentially symmetric-key cipher although the E-LUT and D-LUT used are different, so it is highly efficient since only the single-value additive operation is used in this

cipher. However, the IND-CPA security of the encrypted media content collection $\{\mathbf{c}\}$ stored in the cloud cannot be achieved [30]. In applications with high media privacy requirements, a more secure cloud media sharing scheme is desired. In this concern, we propose the second cloud media sharing scheme FairCMS-II, in which all media content stored in the cloud are encrypted by the lifted-ElGamal based encryption scheme.

In FairCMS-II, the key, fingerprint, E-LUT, and encoding matrix are all generated in the same way as in FairCMS-I. In addition, the calculation and management process for D-LUTs is also the same as in FairCMS-I, except that there is no need to distribute the resulting D-LUTs to users. That is, the cloud is not required to send the last calculated $E_{PK_{U_k}}^1(\mathbf{D}_k(t))$ (**Part 2** of FairCMS-I) to the k -th user, but instead storing it in a set $\mathcal{D}$. As will be shown in the following detailed discussion, this trick will enable the full usage of the computational power of the cloud and reduce bandwidth usage.

Cloud-Based Media Sharing:

The owner encrypts the media content collection $\{\mathbf{m}\}$ to be shared with his/her public key $PK_O = Z^{b_1}$, and then sends the resulting encrypted media content collection $\{E_{PK_O}^2(\mathbf{m})\} = \{(g^r, Z^m Z^{b_1 r})\}$ to the cloud. In addition, the owner use the session keys he/she selects to generate the binary matrix collection $\{\mathbf{B}^m\}$, which is then sent to the cloud.

The cloud calculates the secret matrix collection $\{\bar{\mathbf{G}}\}$ with $\{\mathbf{B}^m\}$ and $\mathbf{G}$, and then stores $\{\bar{\mathbf{G}}\}$ and $\{\mathbf{B}^m\}$. In addition, the cloud calculates the encrypted ciphertext media content collection $\{E_{PK_O}^2(\mathbf{c})\}$ from $\{E_{PK_O}^2(\mathbf{m})\}$, $E_{PK_O}^2(\mathbf{E}(t))$, and $\{\mathbf{B}^m\}$ by

$$E_{PK_O}^2(c_i) = E_{PK_O}^2(m_i) \cdot \prod_{t=0}^{T-1} E_{PK_O}^2(\mathbf{E}(t))^{\mathbf{B}^m(i,t)},$$

where c_i (resp. m_i) is the i -th element of $\mathbf{c}$ (resp. $\mathbf{m}$) and $i \in \{0, 2, \dots, M-1\}$. We emphasize that this process can be accomplished successfully as the second-level ciphertext of the lifted-ElGamal based PRE scheme satisfies the property of additive homomorphism. Afterwards, the cloud stores $\{E_{PK_O}^2(\mathbf{c})\}$.

Suppose the k -th user want to acquire one of the owner's media content $\mathbf{m}$. The cloud then extracts the corresponding encrypted ciphertext media content $E_{PK_O}^2(\mathbf{c})$ from the encrypted ciphertext media content collection. Subsequently, the cloud converts $E_{PK_O}^2(\mathbf{c})$ into $E_{PK_{U_k}}^1(\mathbf{c})$ with the received re-encryption key $rk_{O \rightarrow U_k}$ using the PRE technique. Joint decryption and fingerprinting is then processed by the cloud in the ciphertext domain as follows:

$$E_{PK_{U_k}}^1(m_i^k) = E_{PK_{U_k}}^1(c_i) \cdot \prod_{t=0}^{T-1} E_{PK_{U_k}}^1(\mathbf{D}_k(t))^{\mathbf{B}^m(i,t)}.$$

The cloud then sends the resulting $E_{PK_{U_k}}^1(\mathbf{m}^k)$ to the k -th user, who decrypts $E_{PK_{U_k}}^1(\mathbf{m}^k)$ with his/her own private key $SK_{U_k} = a_2$ to obtain the media content $\mathbf{m}^k$ embedded with his/her personal fingerprint. We emphasize that the cloud cannot get the plaintext version $\mathbf{m}^k$ of the watermarked media content as the cloud does not have the private key SK_{U_k} of the k -th user to decrypt the resulting $E_{PK_{U_k}}^1(\mathbf{m}^k)$.

Input: Security parameter λ .
Output: The cloud stores $\{\tilde{\mathbf{G}}\}$, $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{E_{PK_O}^2(\mathbf{c})\}$.
Procedure:
Owner:

- Generate $(\mathbf{E}, \mathbf{G}, PK_O, SK_O, \{SK_m\})$,
- $E_{PK_O}^2(\mathbf{E}(t)) \leftarrow (\mathbf{E}(t), PK_O)$,
- $\{E_{PK_O}^2(\mathbf{m})\} \leftarrow (\{\mathbf{m}\}, PK_O)$,
- $\{t_{ih}\} \leftarrow \{SK_m\}$,
- $\{\mathbf{B}^m\} \leftarrow \{t_{ih}\}$,
- Send $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{E_{PK_O}^2(\mathbf{m})\}$ to the cloud.

Cloud:

- $\{\tilde{\mathbf{G}}\} \leftarrow (\{\mathbf{B}^m\}, \mathbf{G})$,
- $\{E_{PK_O}^2(\mathbf{c})\} \leftarrow (\{E_{PK_O}^2(\mathbf{m})\}, E_{PK_O}^2(\mathbf{E}(t)), \{\mathbf{B}^m\})$,
- Store $\{\tilde{\mathbf{G}}\}$, $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{E_{PK_O}^2(\mathbf{c})\}$.

Fig. 5. FairCMS-II: Media storage (**Part 1**).

The whole FairCMS-II scheme is summarized as follows. First, suppose an owner rents the cloud's resources for media sharing, the owner and the cloud execute **Part 1** as shown in Fig. 5. Then, suppose the k -th user makes a request indicating that he/she wants to access one of the owner's media content $\mathbf{m}$, the entities execute **Part 2** after the k -th user is authorized by the owner as shown in Fig. 6. Finally, the arbitration and traitor tracing process follows the same approach of FairCMS-I and is thus omitted here.

The owner-side efficiency and scalability performance of FairCMS-II are directly inherited from FairCMS-I, and the achievement of the three security goals of FairCMS-II is also shown in Section VI. Comparing to FairCMS-I, it is easy to see that in FairCMS-II the cloud's overhead is increased considerably due to the adoption of re-encryption operations and homomorphic operations on the ciphertext of the media content, which means it will cost more for the owner on renting the cloud's resources. We regard this as the trade-off between security and cost. In actual use, the two proposed schemes can be selected according to different security requirements. The flexibility of choice in cloud-side efficiency also constitutes one of the prominent advantages of our work.

We emphasize that the joint decryption and fingerprinting operation can also be transferred to users. That is, in **Part 2**, the cloud can send $\{E_{PK_{U_k}}^1(\mathbf{c})\}$ to the k -th user instead of calculating $E_{PK_{U_k}}^1(\mathbf{m}^k)$ in the ciphertext domain. Subsequently, the k -th user needs to decrypt $\{E_{PK_{U_k}}^1(\mathbf{c})\}$ with his/her own private key, and then performs joint decryption and fingerprinting operation with his/her personal D-LUT, which can be obtained from the cloud as in FairCMS-I. In this case, some of the overhead is transferred from the cloud to the user. In general, it is recommended that the cloud performs the joint decryption and fingerprinting operation in the ciphertext domain so as to take full advantage of the power of the cloud.

VI. ACHIEVING THE SECURITY GOALS

This section proves that both FairCMS-I and FairCMS-II can solve the three security/privacy problems with different

Input: Security parameter λ , $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$, $\{\mathbf{B}^m\}$, and $\{E_{PK_O}^2(\mathbf{c})\}$.
Output: The k -th user obtains the watermarked media content $\mathbf{m}^k$.
Procedure:
 k -th User:

- Generate $(\mathbf{b}_k, PK_{U_k}, SK_{U_k})$,
- $E_{PK_{U_k}}^2(\mathbf{b}_k) \leftarrow (\mathbf{b}_k, PK_{U_k})$,
- $rk_{U_k \rightarrow U_k^1} \leftarrow (SK_{U_k}, PK_{U_k})$,
- $rk_{U_k \rightarrow J} \leftarrow (SK_{U_k}, PK_J)$,
- Send $E_{PK_{U_k}}^2(\mathbf{b}_k)$, $rk_{U_k \rightarrow U_k^1}$, and $rk_{U_k \rightarrow J}$ to the cloud.

Owner:

- $rk_{O \rightarrow U_k} \leftarrow (SK_O, PK_{U_k})$,
- Send $rk_{O \rightarrow U_k}$ to the cloud.

Cloud:

- $E_{PK_{U_k}}^1(\mathbf{E}(t)) \leftarrow (E_{PK_O}^2(\mathbf{E}(t)), rk_{O \rightarrow U_k})$,
- $E_{PK_{U_k}}^1(\mathbf{b}_k) \leftarrow (E_{PK_{U_k}}^2(\mathbf{b}_k), rk_{U_k \rightarrow U_k^1})$,
- $E_{PK_J}^1(\mathbf{b}_k) \leftarrow (E_{PK_{U_k}}^2(\mathbf{b}_k), rk_{U_k \rightarrow J})$,
- Store $E_{PK_J}^1(\mathbf{b}_k)$ into a set $\mathcal{F}$,
- $E_{PK_{U_k}}^1(\mathbf{D}_k(t)) \leftarrow (E_{PK_{U_k}}^1(\mathbf{E}(t)), E_{PK_{U_k}}^1(\mathbf{b}_k), \mathbf{G})$,
- Extract the corresponding $E_{PK_O}^2(\mathbf{c})$ from $\{E_{PK_O}^2(\mathbf{c})\}$,
- Extract the corresponding $\mathbf{B}^m$ from $\{\mathbf{B}^m\}$,
- $E_{PK_{U_k}}^1(\mathbf{c}) \leftarrow (E_{PK_O}^2(\mathbf{c}), rk_{O \rightarrow U_k})$,
- $E_{PK_{U_k}}^1(\mathbf{m}^k) \leftarrow (E_{PK_{U_k}}^1(\mathbf{c}), E_{PK_{U_k}}^1(\mathbf{D}_k(t)), \mathbf{B}^m)$,
- Send $E_{PK_{U_k}}^1(\mathbf{m}^k)$ to the k -th user.

k -th User:

- $\mathbf{m}^k \leftarrow (E_{PK_{U_k}}^1(\mathbf{m}^k), PK_{U_k})$.

Fig. 6. FairCMS-II: Media sharing (**Part 2**).

privacy/efficiency trade-offs.

A. Problem 1: Data Privacy Leakage and Access Control

As discussed in Section III, the private data in this paper consists of the users' fingerprints, the LUTs, and the owner's media content.

Theorem 1. *The users' fingerprints and the LUTs in both schemes, as well as the owner's media content in FairCMS-II are privacy-assured against the chosen-plaintext attack by the cloud under the assumptions of extended Decisional Bilinear Diffie-Hellman (eDBDH) [35] and discrete logarithm.*

Proof. In FairCMS-I and FairCMS-II, the k -th user encrypts his/her fingerprint $\mathbf{b}_k$ into $E_{PK_{U_k}}^2(\mathbf{b}_k)$ with his/her own public key PK_{U_k} , and then sends $E_{PK_{U_k}}^2(\mathbf{b}_k)$ together with two re-encryption key $rk_{U_k \rightarrow U_k^1}$ and $rk_{U_k \rightarrow J}$ to the cloud. As a result, different encrypted versions of the fingerprint accessed by the cloud are $E_{PK_{U_k}}^2(\mathbf{b}_k)$, $E_{PK_{U_k}}^1(\mathbf{b}_k)$, and $E_{PK_J}^1(\mathbf{b}_k)$.

We then check the privacy of LUTs, i.e., the E-LUT and D-LUTs. In the two proposed schemes, the owner shares the E-LUT $\mathbf{E}$ in the encrypted form $E_{PK_O}^2(\mathbf{E}(t))$ to the cloud who then utilizes the PRE technique to convert $E_{PK_O}^2(\mathbf{E}(t))$ into $E_{PK_{U_k}}^1(\mathbf{E}(t))$ with the re-encryption key $rk_{O \rightarrow U_k}$. In addition,

the cloud calculates $E_{PK_{U_k}}^1(\mathbf{D}_k)$ in the ciphertext domain with the homomorphic property, as shown in Eqs. (7) and (8). To sum up, only $E_{PK_O}^2(\mathbf{E}(t))$, $E_{PK_{U_k}}^1(\mathbf{E}(t))$, and $E_{PK_{U_k}}^1(\mathbf{D}_k)$ are exposed to the cloud.

By a similar analysis, the ciphertexts about media content available to the cloud are $E_{PK_O}^2(\mathbf{m})$, $E_{PK_O}^2(\mathbf{c})$, $E_{PK_{U_k}}^1(\mathbf{c})$, and $E_{PK_{U_k}}^1(\mathbf{m}^k)$. As a result, the problem of proving that the users' fingerprints, the LUTs, and the owner's media content are protected against the honest-but-curious cloud translates to the problem of proving that both first-level and second-level ciphertexts of the lifted-ElGamal based PRE scheme are all secure, which can be achieved by the reduction below.

Let Π denote the lifted-ElGamal based PRE scheme used in this paper and Π' denote the native ElGamal based PRE scheme proposed in [8], where the difference only lies in whether the message m is lifted. Then we construct a probabilistic polynomial-time (PPT) adversary $\mathcal{A}'$ who attacks Π' by using the PPT adversary $\mathcal{A}$ who attacks Π as a subroutine. We further show if the subroutine $\mathcal{A}$ breaks the definition of indistinguishability of Π , then the constructed adversary $\mathcal{A}'$ will break the indistinguishability of Π' , which is always false since Π' is secure. The details of constructing $\mathcal{A}'$ is as follows.

The experiment that $\mathcal{A}'$ attacks Π' :

1. Run $\mathcal{A}(1^\lambda)$ to obtain a pair of messages m_0 and m_1 .
2. Compute $m'_0 = Z^{m_0}$ and $m'_1 = Z^{m_1}$, then outputs a pair of messages m'_0 and m'_1 .
3. Forward m'_0 and m'_1 to $\mathcal{A}'$'s encryption oracle $\mathcal{O}'$ and get $E_{PK}^1(m_b)$ and $E_{PK}^2(m_b)$, give them to $\mathcal{A}$.
4. Whenever $\mathcal{A}$ queries the encryption of other messages m , $\mathcal{A}'$ answers this query in the following way:
 - (a) Compute $m' = Z^m$ locally,
 - (b) Query $\mathcal{O}'$ with m' and obtain responses $E_{PK}^1(m)$ and $E_{PK}^2(m)$, then return them to $\mathcal{A}$.
5. Continue answering encryption oracle queries of $\mathcal{A}$ as before until $\mathcal{A}$ gives its output. If $\mathcal{A}$ outputs 0, $\mathcal{A}'$ outputs $b' = 0$; otherwise, $\mathcal{A}'$ output $b' = 1$.

The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If $\text{PubK}_{\mathcal{A}', \Pi'}^{\text{cpa}}(\lambda) = 1$, we say that $\mathcal{A}'$ succeeds. Note that the view of $\mathcal{A}$ when run as a subroutine of $\mathcal{A}'$ is distributed identically to the view of $\mathcal{A}$ when it interacts with Π itself, and $\mathcal{A}'$ directly takes the final output of $\mathcal{A}$ as its final output b' . So

$$\Pr[\text{PubK}_{\mathcal{A}', \Pi'}^{\text{cpa}}(\lambda) = 1] = \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cpa}}(\lambda) = 1]. \quad (9)$$

According to the proof result by Ateniese *et al.* [8], if and only if the assumptions of eDBDH and discrete logarithm are established, the native ElGamal based PRE scheme meets the IND-CPA security, i.e.,

$$\left| \frac{1}{2} - \Pr[\text{PubK}_{\mathcal{A}', \Pi'}^{\text{cpa}}(\lambda) = 1] \right| \leq \text{negl}(\lambda),$$

where $\text{negl}(\lambda)$ denotes a negligible function parameterized by λ . Thus, based on Eq. (9), we have

$$\left| \frac{1}{2} - \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cpa}}(\lambda) = 1] \right| \leq \text{negl}(\lambda),$$

which concludes the proof. $\square$

We then turn to analyze the privacy protection performance of the owner's media content in FairCMS-I, where the owner encrypts the media content $\mathbf{m}$ based on $\mathbf{B}^m$ and $\mathbf{E}$ using the single-value alteration encryption, namely Eq. (1). Although the IND-CPA security of $\mathbf{c}$ cannot be rigorously proved, this is not considered a major vulnerability for the following two reasons. For one thing, as long as the variance $\sigma_{\mathbf{E}}^2$ of $\mathbf{E}$ is set large enough, the statistical hiding can be achieved [36], i.e., a PPT adversary cannot distinguish the statistical difference between two different encryption results. The security of the single-value alteration encryption can be further enhanced by computing $\mathbf{c}$ modulo an integer R [10]. In this way, as long as $R \ll \sigma_{\mathbf{E}}$, regardless of the signal values in plaintext, the values of the encrypted signals are approximately uniformly distributed on $[0, R - 1]$. In addition, the linear estimation attack on ciphertext $\mathbf{c}$ was also analyzed in [30], and the result shows that the attack quality is poor as long as the size T of the LUTs (w.r.t. the size M of the media content) is set large enough. For another, as also argued in [30], [37], [38], it is not always necessary to perfectly guarantee the security of $\mathbf{c}$ in general scenarios (in other words, non-highly confidential scenarios), but rather, it would be sufficient to make cracking the encryption as difficult as removing the watermark from the watermarked media content. In FairCMS-I, the watermark is embedded into $\mathbf{m}$ based on Eq. (2), i.e., $\mathbf{m}_k = \mathbf{m} + \mathbf{B}_m \mathbf{W}_k$, which is identical in form with Eq. (1) used for media content encryption, i.e., $\mathbf{c} = \mathbf{m} + \mathbf{B}_m \mathbf{E}$. As a result, if an attacker succeeds in cracking $\mathbf{c}$ without knowing the E-LUT $\mathbf{E}$, then he/she can remove the embedded watermark from $\mathbf{m}_k$ in the same way without knowing the W-LUT $\mathbf{W}_k$ to obtain $\mathbf{m}$, and vice versa. Furthermore, it might be harder to crack $\mathbf{c}$ because the variance of $\mathbf{E}$ is much larger than that of $\mathbf{W}_k$. Therefore, we conclude that the protection of media content privacy in FairCMS-I is sufficient for general scenarios.

We finally analyze the effect of the two schemes on access control. For FairCMS-I, access control is achieved by having the owner distribute D-LUTs only to authorized users, which can be realized here because distributing D-LUTs requires the owner to give the re-encryption key $rk_{O \rightarrow U_k}$. Unauthorized users who do not own the D-LUT cannot access the media content because they cannot perform the media decryption calculation, namely Eq. (2). Furthermore, users with D-LUTs are prevented from accessing the media content outside the authorized scope because different media contents correspond to different $\mathbf{B}^m$. In fact, this access control mechanism is entirely inherited from the original AFP scheme [10]. This mechanism is not resistant to collusion between users, in which case $\mathbf{B}^m$ can be obtained from other authorized users. FairCMS-II solves this flaw by having the cloud compute Eq. (2) in the ciphertext domain and send only $E_{PK_{U_k}}^1(\mathbf{m}^k)$ to authorized users.

B. Problems 2 and 3: Owner's Copyright and Users' Rights

In the absence of any collusion between the owner, users, and the cloud, the two proposed schemes naturally inherit the performance of the TTP-free AFP [10] in protecting the media owner's copyright and the users' rights.

In FairCMS-I and FairCMS-II, on the one hand, although the user generates the fingerprint $\mathbf{b}_k$ on his/her own, the user is unable to know the sequence $\bar{\mathbf{G}}\mathbf{w}_k$ that embedded in the watermarked media content due to the secrecy of $\mathbf{G}$. In the case of non-collusion, the linear assessment attack is a commonly used attack strategy for users to remove their own watermarks from the watermarked content. In this regard, Celik *et al.* [30] proved through detailed theoretical analysis that this attack strategy hardly works as long as the power of the watermark (w.r.t. the signal power) and the size of the LUTs (w.r.t. the content size) are set large enough. A more difficult situation to prevent is **collusion** attack, where a coalition of dishonest users compare their respective D-LUTs with each other in the hope of obtaining an untraceable copy of the content. The anti-collusion performance of the AFP scheme used in this paper is similar to that of a generic spread-spectrum watermark [30], and at the same time, it is compatible with mainstream anti-collusion approaches. Following this idea, two anti-collusion solutions for the LUT-based AFP scheme were later proposed by Bianchi *et al.* [39].

On the other hand, since the owner has no knowledge of the k -th user's fingerprint $\mathbf{b}_k$ (the user does not transmit any information to the owner other than to request authorization), the embedded $\bar{\mathbf{G}}\mathbf{w}_k$ is also unknown to the owner. In this regard, the owner alone has no ability to frame the k -th user.

Afterwards, we consider the case where the owner **colludes** with the cloud, i.e., the owner aggregates the knowledge of the cloud to launch attacks.

Theorem 2. *Even if the owner colludes with the cloud, the knowledge he/she aggregates from the cloud still does not allow him to frame the users.*

Proof. We start by analyzing the situation where the owner attempts to passively attack with information gathered from the cloud. There are two ways for the owner to frame the k -th user, one is to embed the k -th user's fingerprint into any media content, which requires the knowledge of $\mathbf{b}_k$ or $\mathbf{D}_k$, and the other is to directly obtain $\mathbf{m}_k$. However, as **Theorem 1** shows, the cloud cannot obtain any plaintext information about the k -th user's personal fingerprint and D-LUT in both schemes. In fact, the cloud also cannot obtain any plaintext information about the watermarked content $\mathbf{m}^k$ of the k -th user, because in FairCMS-I, the joint decryption and fingerprinting process occurs locally to the user, and in FairCMS-II, the security of $E_{PK_{U_k}}^1(\mathbf{m}^k)$ is guaranteed by **Theorem 1**. Therefore, passive attacks cannot work even with the aggregated knowledge of the owner and the cloud.

We then proceed to analyze the situation of active attack. In fact, the owner cannot launch any effective active attacks (the cloud does not cooperate due to the assumption honest-but-curious), because the direct interaction between the owner and the user in both schemes is strictly limited (there is only one round in the authorization phase), and any other interaction request trying to obtain additional data will be deemed illegal by the user and abort the sharing process. $\square$

VII. EFFICIENCY ANALYSIS

In this section, we evaluate the efficiency of FairCMS-I and FairCMS-II and compare the results with the efficiency of user-side embedding AFP to demonstrate that these two schemes can be regarded as a secure outsourcing of AFP.

To make a fair comparison, we assume that the computational complexity of modular exponentiation, bilinear pairing and discrete logarithm are $O(\alpha)$, $O(\beta)$ and $O(\gamma)$, respectively. Moreover, we assume that the computational overhead caused by plain-field multiplication and addition operations is negligible compared to that of the encrypted domain. In addition, the data expansion rate resulting from PRE encryption is δ , i.e., for the media content $\mathbf{m}$ of size M , its ciphertext is of size $O(\delta M)$. We further assume that the number of the users is K . For ease of presentation, the additive homomorphic encryption employed in the user-side embedding AFP [10] is assumed to be the lifted-ElGamal encryption. The analyzed results are summarized in Table II, in which three cost cases including the computation cost, the communication cost, and the storage cost are considered.

The computation cost is analyzed first. For both FairCMS-I and FairCMS-II, the cost of **Parts 1** and **3** is unconcerned, as they are performed offline only before the media sharing trail begins and when a copyright dispute occurs, respectively. Conversely, **Part 2**, which requires online interaction among the owner, users and the cloud, is the main burden of the operational efficiency of media sharing protocol. In **Part 2** of FairCMS-I, the owner only costs $O(K\alpha)$ to produce re-encryption keys for all K users. The cloud needs to spend $O(K(T + 2L)\beta)$ to perform the re-encryption operations and spend $O(KTL\alpha)$ to calculate the D-LUTs in the ciphertext domain, where T is the length of the LUTs and L is the length of the users' fingerprints. The user needs to spend $O((L + 2)\alpha)$ to encrypt his/her fingerprint and calculate the re-encryption keys, and spend $O(T\alpha + T\gamma)$ to decrypt his/her personalized D-LUT. Similarly, in **Part 2** of FairCMS-II, the case of the owner's side is the same as that of FairCMS-I, so the computation cost is still $O(K\alpha)$. In FairCMS-II, the cloud's cost increases $O(KMT\alpha + KM\beta)$, and the cost to the user changes to $O((M + L + 2)\alpha + M\gamma)$, where M is the size of the required media content. This is because in FairCMS-II, the joint decryption and fingerprinting operation is outsourced to the cloud who carries out all computations in the ciphertext domain. In the client-side embedding AFP scheme, the owner is responsible for encrypting the E-LUT and computing the D-LUTs online for each user in the encryption domain, which costs $O(K(L + 1)T\alpha)$. The user needs to encrypt his/her own fingerprint and decrypt the encrypted D-LUTs, which costs $O((T + L)\alpha + T\gamma)$.

The communication cost is then analyzed. In FairCMS-I, the owner sends the LUT encrypted media content $\mathbf{c}$ to the cloud with a communication cost of $O(M)$. The user receives the public-key encrypted D-LUT and the LUT encrypted media content sent from the cloud, which costs $O(\delta T + M)$. We ignore the overhead of transmitting $\mathbf{B}^m$ because it can be generated locally on all parties by sharing the same session key SK_m . In FairCMS-II, the media content that the owner

TABLE II
EFFICIENCY ANALYSIS RESULTS

		FairCMS-I	FairCMS-II	AFP
		$O(K\alpha)$	$O(K\alpha)$	$O(K(L+1)T\alpha)$
Computational Cost	Owner	$O(K\alpha)$	$O(K\alpha)$	$O(K(L+1)T\alpha)$
	Cloud	$O(KTL\alpha + K(T+2L)\beta)$	$O(K(L+M)T\alpha + K(T+2L+M)\beta)$	$\circ^*$
	User	$O((T+L+2)\alpha + T\gamma)$	$O((M+L+2)\alpha + M\gamma)$	$O((T+L)\alpha + T\gamma)$
Communication Cost	Owner	$O(M+T(L+\delta)+K)$	$O(\delta M+T(L+\delta)+K)$	$O(K(\delta L+\delta T+M))$
	Cloud	$+$ *	$+$ *	$\circ^*$
	User	$O(\delta(T+L)+M+2)$	$O(\delta(M+L)+2)$	$O(\delta(L+T)+M)$
Storage Cost	Owner	$O(M)$	$O(M)$	$O(M(L+2)+K\delta L)$
	Cloud	$O(M(L+1)+K\delta L)$	$O(M(L+\delta)+K\delta L)$	$\circ^*$
	User	$\circ^*$	$\circ^*$	$\circ^*$

* ‘+’ means that the communication cost of the cloud is the sum of the communication costs of the owner and all K users. ‘ $\circ$ ’ means that the storage cost is zero.

deliver is encrypted with the public-key encryption, hence the communication cost is $O(\delta M)$. Similarly, the user receives the fingerprint embedded media content encrypted with public-key cryptography at a cost of $O(\delta M)$. In addition, the owner needs to transmit $\mathbf{G}$, $E_{PK_O}^2(\mathbf{E}(t))$ and the re-encryption keys in both schemes, which costs $O(T(L+\delta)+K)$. In the proposed two schemes, the user also needs to spend $O(\delta L+2)$ to send the encrypted fingerprint and the re-encryption keys. Note that the communication overhead of the cloud is the sum of the communication overheads of the owner and all K users, which we mark as “+” in Table II. Accordingly, in the AFP scheme, the communication costs of the owner and the user are $O(K(\delta L+\delta T+M))$ and $O(\delta(L+T)+M)$, respectively.

At last, the storage cost is analyzed. We consider only the storage cost of media contents and proof materials, including the original media content, the encrypted media content, the secret matrices, as well as the encrypted users’ fingerprints. In the user-side embedding AFP scheme, these materials and contents are all stored by the owner, which costs $O(M(L+2)+K\delta L)$. In the proposed schemes, the owner only costs $O(M)$ to store the original media content, by transferring the remaining storage requirements to the cloud. Correspondingly, in FairCMS-I and FairCMS-II, the cloud requires the storage overhead of $O(M(L+1)+K\delta L)$ and $O(M(L+\delta)+K\delta L)$ respectively. The reason for the difference in storage overhead lies in the different encryption forms of the stored encryption media content. The user does not participate in the management of the proof materials and the encrypted media content, thereby the storage overhead is zero, which is marked as “ $\circ$ ” in Table II.

The results in Table II confirms the two assertions we made earlier. For one thing, compared with the AFP scheme, it is easy to see from Table II that the owner-side computing, communication, and storage costs are reduced in both proposed schemes. In the AFP scheme, the cost of the owner increases linearly as the number of users K increases. However, in FairCMS-I and FairCMS-II, this linear-increase relationship is eliminated, i.e., the owner merely prepares an encryption key for the newly joined user. This is particularly important, as we mentioned in Section IV-B, because only in this way, the increase in the number of users will not overload the cost of the owner, which is a major problem faced in the AFP scheme. In other words, the owner can achieve significant

cost savings by renting the cloud’s resources, thereby enabling large-scale media sharing. Moreover, the larger the scale of media sharing, the more computing savings the owner can get, which fits exactly with the idea of computing outsourcing. Based on the above reasons, we conclude that both FairCMS-I and FairCMS-II can be regarded as the privacy-preserving outsourcing of user-side embedding AFP.

For another, since $M > T > L$ and $\delta > 1$, it is intuitive from Table II that in FairCMS-II, the cloud has increased in computing and storage costs compared to that of FairCMS-I. In fact, the cloud-side communication cost of also increases in FairCMS-II as the uniqueness of each media content copy used for distribution hinders the use of network-level bandwidth saving mechanisms such as multicasting and caching. This means that FairCMS-I is more efficient at the cost of lacking IND-CPA security. Therefore, the trade-off between security and efficiency is evident.

Finally, we analyze the necessary efforts required from the user to obtain the protected content. As can be seen from Table II, compared with the AFP scheme, the computational cost and communication cost of the user in FairCMS-I only increase constant terms $O(2\alpha)$ and $O(2)$ respectively, which is negligible. FairCMS-II has an increase in user-side overhead compared to FairCMS-I, because in FairCMS-II, the user transmits and decrypts the media content while in FairCMS-I, the user transmits and decrypts the D-LUTs. Nevertheless, this user-side efficiency level is substantially the same as the current mainstream media sharing schemes [3], [26], [28], [40], which all require users to decrypt the received encrypted media content with their own private key.

VIII. EXPERIMENT

In this section, we conduct simulation experiments to evaluate the performance of the two proposed schemes in terms of visual effect, perception quality, success tracing rate, and efficiency.

A. Parameter Setting

We use four gray scale images as the shared media content (excluding the experiments in Figs. 13(b), 14, and 15(b), as well as Table V), each with a resolution of 512×512 pixels. As shown in Fig. 7, the contents of the four images are Baboon,

Pirate, Lena, and Car, respectively. For each image, the vector $\mathbf{m}$ is obtained by performing 8×8 discrete cosine transform (DCT) on the image and arranging the DCT coefficients in zig-zag order. We set the variance σ_E^2 of a E-LUT as 10^6 , the length T of LUTs as 1000, the length L of fingerprints as 50, the parameter S as 4, and the number K of users as 200. Moreover, to support encryption algorithm and homomorphic operations, E-LUT, σ_W , and $\mathbf{m}$ is quantized via the fixed point representation manner [10]. Specifically, only the E-LUT and σ_W are quantized in the AFP scheme and FairCMS-I, and $\mathbf{m}$ is additionally quantized in FairCMS-II. In the experiments, the quantization is done with 15 bits for the magnitude part and 5 bits for the fractional part. The performance test of watermarking is implemented by Matlab, and the efficiency test of cryptography is implemented by JavaScript and Python. The experimental equipment is a desktop computer with an Intel Core i7 – 8700 processor and 16 GB of RAM.



Fig. 7. Four test images with a resolution of 512×512 pixels. The contents of (a)-(d) are Baboon, Pirate, Lena, and Car, respectively.

B. Visual Effect

We first observe the effect of single-value alteration encryption and fingerprint embedding from a visual point of view. We set the standard deviation σ_W of W-LUT as 0.3 and use Fig. 7(a) to simulate the AFP scheme. From this, we obtain the corresponding E-LUT-encrypted image and the fingerprint embedded image, as shown in Fig. 8. The peak signal-to-noise ratio (PSNR) of the encrypted picture is 5.751dB, and it can be seen from Fig. 8(a) that the single-value alteration encryption does not reveal any visible information of the original image. The PSNR of the decrypted and fingerprint embedded image is 50.952dB, and its difference to the original image is not visible for naked eyes. Therefore, with appropriate selection of system parameters, AFP does not cause perception quality concerns.

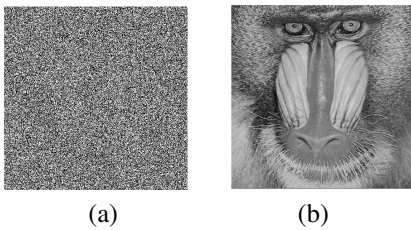


Fig. 8. The encrypted image (PSNR = 5.751dB) and fingerprint embedded image (PSNR = 50.952dB) corresponding to Fig. 7(a).

C. Perception Quality

Because the standard deviation σ_W of W-LUT determines the intensity of fingerprint embedding, it directly affects the

TABLE III
COMPARISON OF THE PSNR (IN DB) AGAINST DIFFERENT σ_W

Method	$\sigma_W=0.1$	$\sigma_W=0.12$	$\sigma_W=0.15$	$\sigma_W=0.2$	$\sigma_W=0.25$	$\sigma_W=0.3$
AFP/FairCMS-I	67.895	61.150	57.512	55.385	52.843	51.244
FairCMS-II	68.009	61.183	57.538	55.401	52.866	51.241

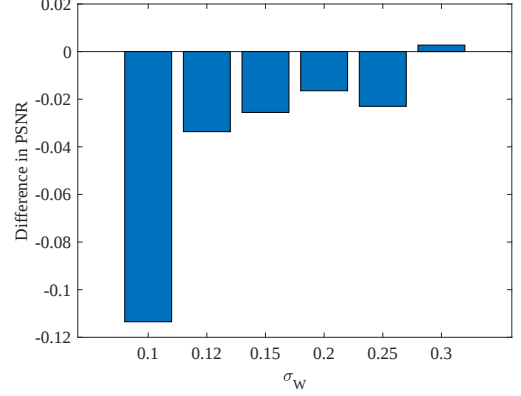


Fig. 9. The difference between AFP/FairCMS-I and FairCMS-II in PSNR.

perception quality of the embedded image. Here we fix other parameters, such as the quantization bits, and investigate the effect of different values of σ_W on the perception quality of the embedded image, which is again measured by the value of PSNR. In FairCMS-I, D-LUTs are computed in the ciphertext domain homomorphically, while the media encryption operation as well as the joint decryption and fingerprinting operation are completed in the plaintext domain, which is exactly the same as in the AFP scheme. As a result, the performance of FairCMS-I and the AFP scheme is theoretically consistent in terms of perception quality and traitor tracing. Table III shows the comparison results between AFP/FairCMS-I and FairCMS-II in terms of perception quality. The experimental results are averaged over four tests, each using the image in Fig. 7 in turn. As can be seen from Table III, the smaller σ_W is, the better the image perception quality. Fig. 9 visualizes the difference between AFP/FairCMS-I and FairCMS-II in PSNR. As shown in Fig. 9, the PSNR values of FairCMS-II are slightly better than that of AFP/FairCMS-I under most settings. Compared with Fig. 8, it can be concluded that all the listed PSNR values are high enough for usage in practical applications. Note that the watermark embedding here is not limited to working in the DCT domain. A suitable transform domain can be chosen according to the media type, such as the dual-tree complex wavelet transform domain for video [41] and the Fourier transform domain for audio [42], to maximize the perception quality of the media content.

D. Success Tracing Rate

With other parameters such as the number of quantization bits being fixed, the success rate of traitor tracing is dominated by fingerprint embedding strength and noise power. We assume that the additive noise $\mathbf{n}$ obeys a Gaussian distribution with variance σ_n^2 and mean 0. The matched filter decoder is selected for fingerprint detection since it has a fairly obvious

TABLE IV
COMPARISON OF THE SUCCESS TRACING RATE AGAINST DIFFERENT σ_n AND σ_W

Method	$\sigma_n=0.2$						$\sigma_n=0.5$					
	$\sigma_W=0.1$	$\sigma_W=0.12$	$\sigma_W=0.15$	$\sigma_W=0.2$	$\sigma_W=0.25$	$\sigma_W=0.3$	$\sigma_W=0.1$	$\sigma_W=0.12$	$\sigma_W=0.15$	$\sigma_W=0.2$	$\sigma_W=0.25$	$\sigma_W=0.3$
AFP/FairCMS-I	0.4888	0.6463	0.8775	0.9525	0.9775	0.9788	0.3275	0.6400	0.8488	0.9475	0.9775	0.9800
FairCMS-II	0.4613	0.6375	0.8675	0.9488	0.9838	0.9750	0.3213	0.6475	0.8525	0.9363	0.9638	0.9738

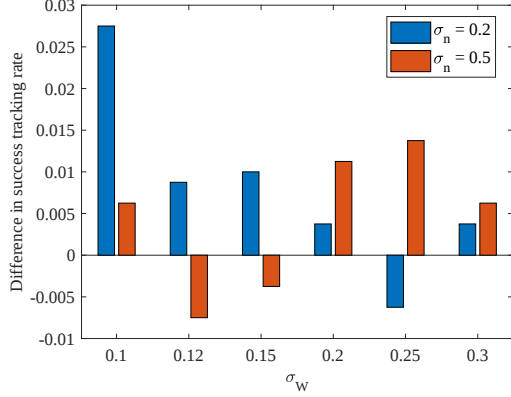


Fig. 10. The difference between AFP/FairCMS-I and FairCMS-II in success tracing rate.

suppression effect on Gaussian noise. Here we investigate the success rate of traitor tracing of AFP/FairCMS-I and FairCMS-II under different values of σ_W and σ_n . Table IV presents the average results of four tests as in the previous subsection. In each test, we consider copyright infringement of each user and track that user. If a user's fingerprint is extracted without any errors, it is counted as a successful trace, otherwise it is counted as a failed trace. The success tracing rate is recorded as the number of successful traces divided by the total number of traces. As presented in Table IV, the increase of σ_W and σ_n has a positive and negative effect on the successful tracing rate as a whole, respectively. Fig. 10 visualizes the difference between AFP/FairCMS-I and FairCMS-II in success tracing rate. As shown in Fig. 10, compared with AFP/FairCMS-I, the success tracing rate of FairCMS-II decreases slightly in most cases. Nevertheless, this does not bother as the decrease is basically less than 0.015.

E. Efficiency

First, to evaluate the efficiency of implementing privacy-protected access control, we test the time cost of each step in the lifted-ElGamal based PRE, and the results are presented in Figs. 11 and 12. In the experiment, we adopt the lookup table method [34] to solve the discrete logarithm problem. In this method, a hash table that records all (Z^m, m) pairs needs to be created first. In this way, m can be recovered from Z^m only by querying the hash table during decryption, and the time consumed by the querying operation is negligible. The main time overhead lies in the establishment of the hash table. Fig. 12 shows the time consumed in the establishment of the hash table when the plaintext is quantized by different bits. As can be seen from Fig. 12, when the plaintext is quantized to

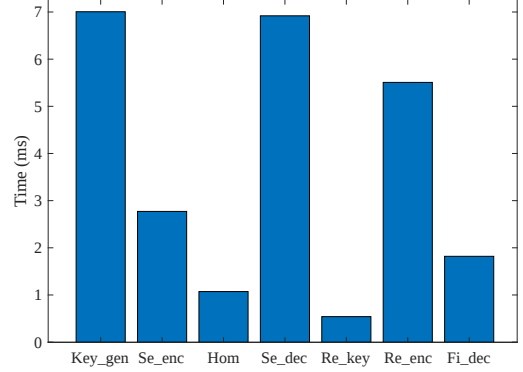


Fig. 11. The computation time taken to perform each algorithm. Key_gen, Se_enc, Hom, Se_dec, Re_key, Re_enc, and Fi_dec refer to the time consumed by key generation, second-level encryption, homomorphic operation, second-level decryption, generation of re-encryption key, re-encryption, and first-level decryption, respectively.

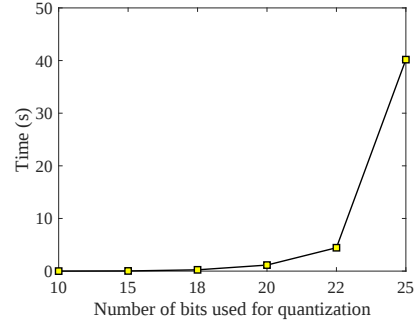


Fig. 12. The time taken to solve discrete logarithm using the lookup table method [34] when different bits are used to quantize the plaintext.

20 bits, the time cost is less than 2 seconds. Note that the hash table only needs to be created once no matter how much data needs to be encrypted and decrypted. As a result, solving the discrete logarithm problem has little effect on the efficiency of FairCMS-I and FairCMS-II. Fig. 11 shows the efficiency performance of other steps except solving discrete logarithm. As can be seen from Fig. 11, all the steps can be completed in milliseconds and the relatively more time-consuming steps are those that require calculating bilinear pairings, including key generation, second-level decryption, and re-encryption.

Second, we compare the cloud-side efficiency of FairCMS-I and FairCMS-II, and the results are presented in Fig. 13. As shown therein, the cloud-side efficiency of FairCMS-I is significantly higher than that of FairCMS-II, thus validating our analysis in Section VII. The main reason for the cloud-side efficiency gain of FairCMS-I lies in the use of lightweight single-value alteration method to encrypt the media content, as shown in Fig. 14. This is the key to ensuring that the system

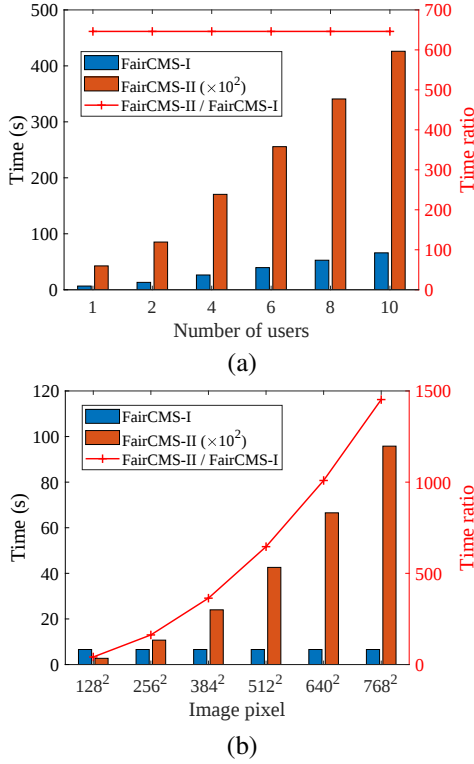


Fig. 13. The comparison of cloud-side computational efficiency between FairCMS-I and FairCMS-II. The bars and polyline correspond to the left and right Y-axes, respectively. The time consumed by FairCMS-II is 100 times the reading on the Y-axis. (a) Efficiency comparison under different number of users. (b) Efficiency comparison under different image pixels.

is efficient when the size of the media content being shared (e.g., video) is large. The time cost of encrypting a video using the single-value alteration method is depicted in Table V, and it is shown to be acceptably low. Therefore, we suggest that owners select FairCMS-I when the media content size is large and the security requirements is not excessively rigorous. In spite of this, there are no fixed thresholds for media content size and security requirements that can be used as a basis for recommendations regarding scheme selection.

Finally, we conduct a comparative experiment to evaluate the proposed schemes against their relevant existing counterparts, and the results are displayed in Fig. 15. For FairCMS-I and FairCMS-II, we measure the time overhead of Part 2 as it is executed once for each user. For the other schemes, we evaluate their primary sources of overhead, namely encryption, homomorphic operations, and re-encryption operations, which also require execution once for each user. The lifted-ElGamal scheme is utilized in the evaluation for uniform comparison. As shown in Fig. 15, for one thing, FairCMS-I and FairCMS-II allow the owner to achieve significant computational overhead savings relative to the original AFP scheme [10]. With FairCMS-I or FairCMS-II, the owner's computing overhead can be reduced to less than 0.2 seconds, even if the number of users reaches hundreds. For another, FairCMS-I exhibits significantly higher cloud-side efficiency compared with [3], [27], [28], and the cloud-side efficiency gain increases with the size of the media content. Thus, the comparison shown in Table I is validated.

TABLE V
THE TIME (IN SECOND) REQUIRED TO ENCRYPT A VIDEO WITH DIFFERENT FRAMES USING THE SINGLE-VALUE ALTERATION ENCRYPTION ADOPTED BY FAIRCMS-I

Number of frames	600	1200	1800	2400	3000	3600	4200	4800
Encryption	129	306	461	645	809	1012	1182	1406
Decryption	136	275	484	636	852	1066	1283	1455

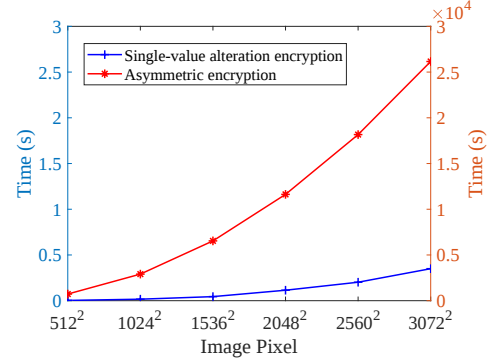


Fig. 14. Efficiency comparison between the single-value alteration encryption and the asymmetric encryption (i.e., the second-level encryption of the lifted-ElGamal based PRE). The blue and red lines correspond to the Y-axis on the left and right, respectively.

IX. CONCLUSION

This paper solves the three problems faced by cloud media sharing and proposes two schemes FairCMS-I and FairCMS-II. FairCMS-I gives a method to transfer the management of LUTs to the cloud, enabling the calculation of each user's D-LUT in the ciphertext domain and its subsequent distribution. However, utilizing the single-value alteration method for masking the original media content does not achieve the IND-CPA security. Then FairCMS-II offers an enhanced privacy solution by replacing the encryption method with the lifted-ElGamal based PRE scheme, albeit at the cost of increased cloud overhead. Notably, both FairCMS-I and FairCMS-II fulfill scalability and owner-side efficiency requirements. In summary, the two proposed schemes can facilitate the media sharing of owners, while simultaneously ensuring the joint protection of copyright and users' rights, ultimately promoting the sustainable growth of the media sharing industry.

REFERENCES

- [1] R. Hu and S. Xiang, "Cover-lossless robust image watermarking against geometric deformations," *IEEE Trans. Image Process.*, vol. 30, pp. 318–331, 2021.
- [2] Z. Wang, O. Byrnes, H. Wang, R. Sun, C. Ma, H. Chen, Q. Wu, and M. Xue, "Data hiding with deep learning: A survey unifying digital watermarking and steganography," *IEEE Trans. Comput. Soc. Syst.*, 2023, in press, doi:10.1109/TCSS.2023.3268950.
- [3] L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z. Shan, and K. Ren, "You can access but you cannot leak: Defending against illegal content redistribution in encrypted cloud media center," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 6, pp. 1218–1231, 2020.
- [4] X. Dong, W. Zhang, M. Shah, B. Wang, and N. Yu, "Watermarking-based secure plaintext image protocols for storage, show, deletion and retrieval in the cloud," *IEEE Trans. Services Comput.*, vol. 15, no. 3, pp. 1678–1692, 2022.

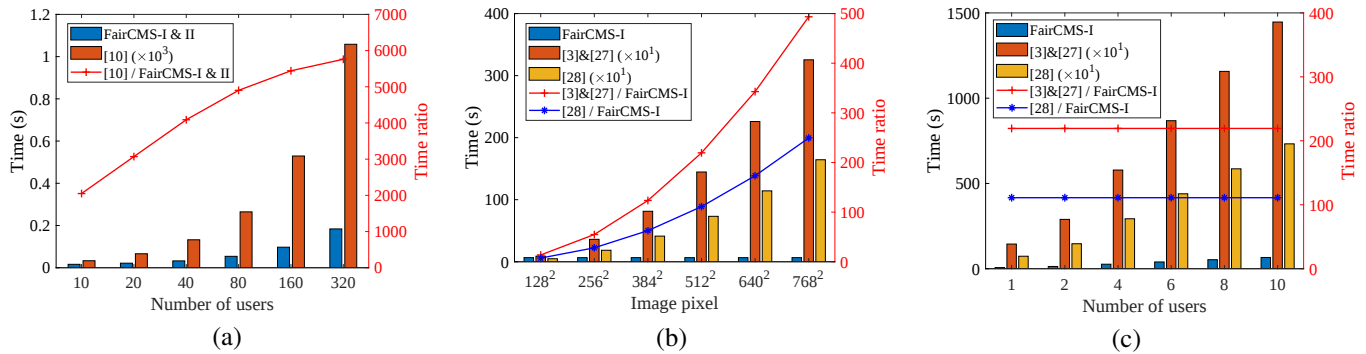


Fig. 15. Comparison of computational efficiency with existing works. The bars and polyline correspond to the left and right Y-axes, respectively. (a) Efficiency comparison with the AFP scheme [10] on the owner side. (b) Efficiency comparison with [3], [27], [28] on the cloud side under different image pixels. (c) Efficiency comparison with [3], [27], [28] on the cloud side under different number of users. The time consumed by [10] and [3], [27], [28] is 1,000 times and 10 times the reading on the Y-axis, respectively.

- [5] R. Bobba, O. Fatemeh, F. Khan, A. Khan, C. A. Gunter, H. Khurana, and M. Prabhakaran, "Attribute-based messaging: Access control and confidentiality," *ACM Trans. Inf. System Secur.*, vol. 13, no. 4, pp. 1–35, 2010.
- [6] W. Wei, S. Liu, W. Li, and D. Du, "Fractal intelligent privacy protection in online social network using attribute-based encryption schemes," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 736–747, 2018.
- [7] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud," in *Proc. 7th ACM Symp. Inf. Comput. Commun. Secur.*, pp. 87–88, 2012.
- [8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. System Secur.*, vol. 9, no. 1, pp. 1–30, 2006.
- [9] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," in *Proc. EUROCRYPT*, vol. 96, pp. 84–95, Springer, 1996.
- [10] T. Bianchi and A. Piva, "TTP-free asymmetric fingerprinting based on client side embedding," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1557–1568, 2014.
- [11] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, 2001.
- [12] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1618–1626, 2004.
- [13] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer-seller watermarking protocol," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, pp. 920–931, 2010.
- [14] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 87–96, 2013.
- [15] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Trans. Services Comput.*, 2016, in press, doi:10.1109/TSC.2016.2551238.
- [16] B. Yu, C. Zhang, and W. Li, "File matching based on secure authentication and proxy homomorphic re-encryption," in *Proc. 11th Int. Conf. Machine Learning Comput.*, pp. 472–476, ACM, 2019.
- [17] B. K. Samanthula, Y. Elmehdwi, G. Howser, and S. Madria, "A secure data sharing and query processing framework via federation of cloud computing," *Inf. Systems*, vol. 48, pp. 196–212, 2015.
- [18] C.-z. Gao, Q. Cheng, X. Li, and S.-b. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network," *Cluster Comput.*, vol. 22, no. 1, pp. 1655–1663, 2019.
- [19] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure sharing of partially homomorphic encrypted IOT data," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Systems*, pp. 1–14, ACM, 2017.
- [20] D. Derler, S. Ramacher, and D. Slamanig, "Homomorphic proxy re-authenticators and applications to verifiable multi-user data aggregation," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, pp. 124–142, Springer, 2017.
- [21] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Trans. Multimedia*, vol. 15, no. 4, pp. 778–788, 2013.
- [22] Y. Polyakov, K. Rohloff, G. Sahu, and V. Vaikuntanathan, "Fast proxy re-encryption for publish/subscribe systems," *ACM Trans. Privacy Secur.*, vol. 20, no. 4, pp. 1–31, 2017.
- [23] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1667–1680, 2014.
- [24] J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *J. Netw. Computer Appl.*, vol. 112, pp. 89–96, 2018.
- [25] G. S. Poh and K. M. Martin, "An efficient buyer-seller watermarking protocol based on Chameleon encryption," in *Proc. Int. Work. Digital Watermarking*, pp. 433–447, Springer, 2008.
- [26] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2594–2608, 2016.
- [27] T. Zheng, Y. Luo, T. Zhou, and Z. Cai, "Towards differential access control and privacy-preserving for secure media data sharing in the cloud," *Computers Secur.*, vol. 113, p. 102553, 2022.
- [28] F. Frattolillo, "A multiparty watermarking protocol for cloud environments," *J. Inf. Secur. Appl.*, vol. 47, pp. 246–257, 2019.
- [29] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–2119, 2014.
- [30] M. U. Celik, A. N. Lemma, S. Katzenbeisser, and M. van der Veen, "Lookup-table-based secure client-side embedding for spread-spectrum watermarks," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 3, pp. 475–487, 2008.
- [31] M. U. Celik, A. N. Lemma, S. Katzenbeisser, and M. van der Veen, "Secure embedding of spread spectrum watermarks using look-up-tables," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, vol. 2, pp. 153–156, 2007.
- [32] T. Marshall, "Coding of real-number sequences for error correction: A digital signal processing problem," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 2, pp. 381–392, 2003.
- [33] Z. Wang and G. B. Giannakis, "Complex-field coding for OFDM over fading wireless channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 707–720, 2003.
- [34] Y. Chen, B. Wang, H. Jiang, P. Duan, Y. Ping, and Z. Hong, "PEPFL: A framework for a practical and efficient privacy-preserving federated learning," *Digital Commun. Netw.*, 2022, in press, doi:10.1016/j.dcan.2022.05.019.
- [35] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.
- [36] D. Evans, Y. Huang, J. Katz, and L. Malka, "Efficient privacy-preserving biometric identification," in *Proc. Netw. Distri. System Secur. Symp. (NDSS)*, vol. 68, pp. 90–98, 2011.
- [37] X. Xiao, Y. Zhang, Y. Zhu, P. Hu, and X. Cao, "Fingerchain: Copyrighted multi-owner media sharing by introducing asymmetric fingerprinting into blockchain," *IEEE Trans. Netw. Serv. Manage.*, vol. 20, no. 3, pp. 2869–2885, 2023.
- [38] X. Xiao, X. Ye, Y. Zhang, W. Wen, and X. Zhang, "Preview-supported copyright image sharing," *J. Electronics & Inf. Technol.*, vol. 45, pp. 1–10, 2022.
- [39] T. Bianchi, A. Piva, and D. Shullani, "Anticollusion solutions for

asymmetric fingerprinting protocols based on client side embedding,” *EURASIP J. Inf. Secur.*, vol. 2015, no. 1, pp. 1–17, 2015.

- [40] F. Frattolillo, “A buyer-friendly and mediated watermarking protocol for web context,” *ACM Trans. Web*, vol. 10, no. 2, pp. 1–28, 2016.
- [41] W. Huan, S. Li, Z. Qian, and X. Zhang, “Exploring stable coefficients on joint sub-bands for robust video watermarking in dt cwt domain,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 4, pp. 1955–1965, 2021.
- [42] E. Salah, K. Amine, K. Redouane, and K. Fares, “A Fourier transform based audio watermarking algorithm,” *Appl. Acoustics*, vol. 172, p. 107652, 2021.



Xiangli Xiao received the B.E. degree from the College of Electronic and Information Engineering, Southwest University, Chongqing, China, in Jun. 2020. He is currently pursuing the Ph.D. degree in the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His current research interests include multimedia security, digital watermarking, blockchain, and cloud computing security.



Yushu Zhang (Senior Member, IEEE) received the B.S. degree from the School of Science, North University of China, Taiyuan, China, in 2010, and the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. He held various research positions with City University of Hong Kong, Southwest University, University of Macau, and Deakin University. He is currently a Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. He is

an Associate Editor of Information Sciences, Journal of King Saud University-Computer and Information Sciences, and Signal Processing. His research interests include multimedia security, blockchain, and artificial intelligence. He has co-authored more than 200 refereed journal articles and conference papers in these areas.



Leo Yu Zhang (Member, IEEE) received the Ph.D. degree from the City University of Hong Kong, Hong Kong, China, in 2016. He is currently a Senior Lecturer with the School of Information and Communication Technology, Griffith University, QLD, Australia. He used to be a faculty member at the School of Information Technology, Deakin University, from 2018 to 2023. He held various research positions with the City University of Hong Kong, the University of Macau, the University of Ferrara, and the University of Bologna. He is an

Associate Editor of IEEE Transactions on Dependable and Secure Computing. His current research focuses on trustworthy AI and applied cryptography, and he has published over 100 articles in refereed journals and conferences, such as TIFS, TDSC, Oakland, AsiaCCS, NeurIPS, CVPR, ICCV, IJCAI, AAAI, etc.



Zhongyun Hua (Senior Member, IEEE) received the B.S. degree from Chongqing University, Chongqing, China, in 2011, followed by the M.S. and Ph.D. degrees from the University of Macau, Macau, China, in 2013 and 2016, respectively. He is currently an Associate Professor with the School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, China. His works have appeared in prestigious venues such as IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Image Processing, IEEE Transactions on Signal Processing, and ACM Multimedia. He has been recognized as a ‘Highly Cited Researcher 2022’. His current research interests are focused on chaotic system, multimedia security, and secure cloud computing. He has published about seventy papers on the subject, receiving more than 5800 citations.



Zhe Liu (Senior Member, IEEE) received the B.S. and M.S. degrees from Shandong University, China, in 2008 and 2011, respectively, and the Ph.D. degree from the Laboratory of Algorithmics, Cryptology and Security, University of Luxembourg, Luxembourg, in 2015. He is currently a Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. He has co-authored over 100 peer-reviewed journal articles and conference papers.

His research interests include security, privacy, and cryptographic solutions for the Internet of Things. He has served as a program committee member for more than 50 international conferences. He was a recipient of the prestigious FNR Awards-Outstanding Ph.D. Thesis Award in 2016, the ACM CHINA SIGSAC Rising Star Award in 2017, as well as the DAMO Academy Young Fellow in 2019.



Jiwu Huang (Fellow, IEEE) received the B.S. degree from Xidian University, Xi’an, China, the M.S. degree from Tsinghua University, Beijing, China, and the Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, in 1982, 1987, and 1998, respectively. He is currently a Professor with the College of Electronics and Information Engineering, Shenzhen University, Shenzhen, China. His current research interests include multimedia forensics and security. He serves as a member of the IEEE CASS Multimedia Systems and

Applications Technical Committee and the IEEE SPS Information Forensics and Security Technical Committee. He is an Associate Editor for the IEEE Transactions on Information Forensics and Security, the LNCS Transactions on Data Hiding and Multimedia Security (Springer), and the EURASIP Journal on Information Security (Hindawi).