IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 30, 2017, accepted January 31, 2018, date of publication February 6, 2018, date of current version April 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2802928

A Study on the Collusion Security of LUT-Based Client-Side Watermark Embedding

YUAN-GEN WANG[1], DONGQING XIE[1], AND BRIJ B. GUPTA[2]

[1]School of Computer Science, Guangzhou University, Guangzhou 510006, China
[2]National Institute of Technology, Kurukshetra 136119, India

Corresponding author: Dongqing Xie (dqxie@gzhu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672554 and Grant 61772007, in part by NSF of Guangdong Province under Grant 2014A030310112 and Grant 2015A030313602, in part by the Science and Technology Plan Project of Guangdong Province under Grant 2016B010124014, and in part by the Industry-University-Research Collaborative Innovation of Guangzhou City under Grant 201704020030 and Grant 201604016035.

ABSTRACT Recently, Celik *et al.* proposed a lookup-table (LUT)-based embedding mechanism for spread-spectrum watermarks, in which the content distribution server sends an encrypted content to the client, then the client uses his or her personalized decryption LUT to decrypt the received content, meanwhile embeds his or her personalized watermark into the content. They also provided a brief analysis on the security of the LUT-based embedding in terms of the collusion attack on watermarked contents. However, we find that the LUT-based embedding is vulnerable to not only the collusion attack on watermarked contents but the collusion attack on decryption LUTs as well, due to the fact all clients share the same long-term encryption LUT. In this paper, we present a theoretical analysis on the collusion security of the LUT-based embedding mechanism. The analysis shows that the collusion attack on decryption LUTs is more effective than the collusion attack on watermarked contents. Based on our analysis, the content distribution system proposed by Celik *et al.* can only be used for package sale, which limits its applications. In order to extend the applications, we suggest that the encryption and decryption LUTs of the LUT-based client-side embedding should be set as short-term keys instead of long-term keys. Finally, simulations are carried out to illustrate and validate our theoretical analysis.

INDEX TERMS Watermark, business model, security, lookup-table (LUT), copyright protection.

I. INTRODUCTION

Nowadays, the digital content producers face a great risk of copyright infringement due to the convenience of copying and distributing digital contents. Digital watermarking becomes the best technical way to protect digital copyright so far [1]–[3]. Among various embedding techniques, spread-spectrum (SS) embedding, which embeds the watermark message by adding a modulated pseudo-random sequence to the host signal, is considered as the most important embedding technique and has been the most widely used [4]–[10]. Besides some SS-based forensic watermarking schemes [7], [11]–[13] have been proposed to prevent or deter the copyright infringement by identifying which client leaks the unauthorized contents. There are also some watermarking protocols [14]–[25], which can not only prevent the copyright infringement, but can also protect the clients' rights that might be infringed by some untrusted content distribution servers.

In order to prevent clients from maliciously copying and distributing the digital contents in a mass-sale content distribution scenario, Celik *et al.* [7] is the first to propose the LUT-based client-side watermark embedding. That is the content distribution server sends an encrypted content to the client in a broadcasting way, then the client uses his or her personalized LUT to decrypt the received content and while at the same time embeds their personalized watermark into the content. This scheme solved the problem with both the bottleneck of Internet traffic of point-to-point transmission and severs' computational overload due to watermark embedding operation. Note that the personalized decryption LUT was considered by Celik *et al.* [7] as a long-term decryption key. In [7], Celik *et al.* have provided a theoretical analysis on the robustness and security of the LUT-based embedding. The analysis have shown that the LUT-based client-side embedding is not only efficient to detect watermarks but robust against Gaussian noises. Soon after, the great

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

attention has been payed on such the client-side embedding mechanism [17], [19], [20], [22]–[24]. In [17], Bianchi and Piva proposed a secure distribution scheme in which the personalized decryption keys contained the Buyer's fingerprint by means of existing asymmetric protocols, while did not use a trusted third party. Lin *et al.* proposed to apply the client-side embedding to both reversible data hiding [19] and vector quantization images [22]. These two works focus on the application of client-side embedding. Like [19], [22], Czaplewski [20] also paid attention to apply client-side embedding to color image with quaternion cipher method. Czaplewski and Rykaczewski [23] considered a new application scenario in which multicast distribution takes the place of broadcasting. Bianchi *et al.* [24] proposed to improve Celik *et al.* 's method [7] by increasing the anticollusion ability. However, all of these improved works [17], [19], [20], [22]–[24] including the original version [7] haven't considered the business model of the content distribution system. Actually the attacker can launch a collusion attack not only on the watermarked content but on the decryption LUTs in the business model employed by [7]. This results in a fatal destruction of the LUT-based client-side embedding system.

In this paper, we analyze the business model of the content distribution system based on the client-side embedding from a security viewpoint. We find that the collusion attack on the decryption LUT is more effective than the collusion attack on the watermarked content. This shows that the content distribution system proposed by both Celik *et al.* and the successors can only be used for package sale, which results in an important limitation of application of the client-side embedding technique. In order to extend the applications of the content distribution system that uses the LUT-based client-side embedding, we suggest to set the encryption and decryption LUTs of the LUT-based client-side embedding as short-term keys instead of long-term keys. In doing so, we present a rigorously theoretical analysis on the collusion security of the client-side watermark embedding to support the suggestion. Finally, a number of simulation results are provided to demonstrate the effectiveness of our analysis.

The rest of the paper is organized as follows. Section II briefly introduces the LUT-based client-side embedding. In Section III, from a security viewpoint, we provide an analysis on the business model of the content distribution system that uses the LUT-based client-side embedding. Section IV gives the simulation results, followed by the concluding remarks made in Section IV.

II. OVERVIEW OF THE LUT-BASED CLIENT-SIDE EMBEDDING

The LUT-based content distribution model was firstly proposed by Celik *et al.* [7]. As shown in Fig. 1, the server encrypts a digital content with the long-term key to obtain a common encrypted version, then broadcasts the common encrypted content to all the clients. The server generates a personalized watermark (fingerprint) for each client, then computes a decryption key by combining the encryption key and the personalized watermark. The authorized client needs to only purchase his or her personalized decryption key sent by the server in a point-to-point (P2P) communication way. Compared with the traditional content distribution model, the secure content distribution model proposed by Celik *et al.* can significantly reduce the computational burden of the server and the bandwidth requirement for networks.

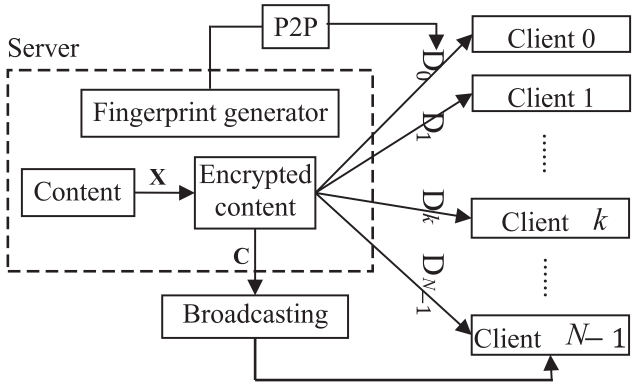

FIGURE 1. Illustration of the secure content distribution model proposed by Celik *et al.*

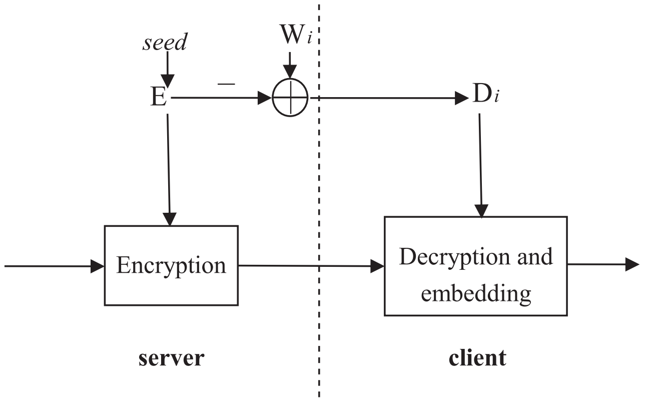

FIGURE 2. Illustration of encryption and joint decryption/watermarking.

The secure content distribution model proposed by Celik *et al.* can mainly be divided into three parts: key generation, encryption, and joint decryption/watermarking. As shown in Fig. 2, the common encrypted content is sent to all clients in broadcasting way. Each client decrypts the content with his or her received personalized decryption key, meanwhile his or her personalized watermark is mandatorily embedded into the content. In the following, we briefly introduce the three parts of the LUT-based client-side embedding, respectively.

A. KEY GENERATION

Given a content distribution system that uses the LUT-based client-side embedding, the server of the content distribution system first constructs an LUT $\mathbf{E}$ of size $L \times 1$, of which the entries are chosen independently and randomly according to a fixed probability distribution. Assume that there are N clients served by the content distribution system. For each client k, $k \in \{0, 1, \cdots, N-1\}$, the server generates a personalized watermark LUT $\mathbf{W}_k$ of size $L \times 1$. The entries of $\mathbf{W}_k$ are also chosen independently and randomly according to a fixed probability distribution. Then the server generates the personalized decryption LUT for client k by

$$\mathbf{D}_k = -\mathbf{E} + \mathbf{W}_k. \tag{1}$$

Finally, the server transmits the personalized decryption LUT $\mathbf{D}_k$ to client k securely. Note that, in the LUT-based embedding, $\mathbf{E}$ is set as the long-term encryption key and is common for all clients, thus $\mathbf{D}_k$ is the long-term decryption key, too.

B. ENCRYPTION

Let a real vector $\mathbf{x}$ of length M denote the original content to be distributed and watermarked. By adding a linear transformed LUT $\mathbf{E}$ into the original content $\mathbf{x}$, the server constructs an encrypted content by

$$\mathbf{c} = \mathbf{x} + \mathcal{T}(K)\mathbf{E}, \tag{2}$$

where K is the session key that should be different for each delivered content, and $\mathcal{T}(K)$ is a key-dependent binary matrix of size $M \times L$, in which each row contains only S ($S \ll L$) ones and the rest elements are all zeros. Note that S is a parameter which controls the security of the system.

C. JOINT DECRYPTION/WATERMARKING

Once client k, $k \in \{0, 1, \cdots, N-1\}$, receives the session K and the encrypted content $\mathbf{c}$, he or she first generates the key-dependent transform matrix $\mathcal{T}$ by K and then decrypts $\mathbf{c}$ by

$$\begin{aligned}\mathbf{y}_k &= \mathbf{c} + \mathcal{T}(K)\mathbf{D}_k \\ &= \mathbf{x} + \mathcal{T}\mathbf{E} + \mathcal{T}(-\mathbf{E} + \mathbf{W}_k) \\ &= \mathbf{x} + \mathcal{T}\mathbf{W}_k.\end{aligned} \tag{3}$$

According to Eq. (3), the personalized watermark $\mathbf{w}_k$ ($\mathbf{w}_k = \mathcal{T}\mathbf{W}_k$) is embedded into the original content $\mathbf{x}$ during the decryption of $\mathbf{c}$. Therefore, client k can just obtain the watermarked content $\mathbf{y}_k$, not the original content $\mathbf{x}$.

III. WHICH COMPONENTS OF THE WATERMARKED CONTENT CAN BE REALLY SOLD?

Let $\mathbf{y}_k$ denote the watermarked content obtained by client k, $k \in \{0, 1, \cdots, N-1\}$. In the content distribution system that uses the traditional watermarking techniques [11], [12], the watermarked content $\mathbf{y}_k$ is inseparable when $\mathbf{y}_k$ is being distributed to client k. Therefore, the content distribution server must sell the whole of the watermarked content $\mathbf{y}_k$ to client k. Whereas, in the content distribution system that uses the LUT-based watermarking of [7], the watermarked content $\mathbf{y}_k$, as described by Eq. (3), is made up of the encrypted content $\mathbf{c}$, the session key K, and the personalized decryption key $\mathbf{D}_k$. And the three components of $\mathbf{y}_k$ (i.e., $\mathbf{c}$, K, and $\mathbf{D}_k$, respectively) have to be distributed to client k separately. Then, let's consider which of the three components of $\mathbf{y}_k$ can be used for sale. Since the encrypted content $\mathbf{c}$ and the session key K are common to all clients and there are no personalized "watermarks" in both of them, it is unreasonable for the content distribution system to gain by selling $\mathbf{c}$ and K. Otherwise, once an adversary receives $\mathbf{c}$ and K, he or she can maliciously leak $\mathbf{c}$ and K to the public without being tracked. Therefore, from the viewpoint of security, the only thing that can be used for sale is the personalized decryption key $\mathbf{D}_k$. Next, we present an analysis on selling $\mathbf{D}_k$ in detail.

The personalized decryption key $\mathbf{D}_k$, $k \in \{0, 1, \cdots, N-1\}$, is set as a long-term key in [7], thus $\mathbf{D}_k$ could be used to decrypt a lot of different encrypted contents with the corresponding different session key K. Assume that there are R encrypted contents that $\mathbf{D}_k$ can decrypt, and denote the R contents as $\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{R-1}$, respectively. Note that R is a large number due to the fact that $\mathbf{D}_k$ is set as the long-term key. If a client (k) just wants to buy content $\mathbf{c}_i$, $i \in \{0, 1, \cdots, R-1\}$, then he or she has to buy $\mathbf{D}_k$, $k \in \{0, 1, \cdots, N-1\}$. This means that in order to buy one content the client in fact buys all of the R contents decrypted by $\mathbf{D}_k$ (note that the session key K is open). Thus, in the content distribution system that uses the LUT-based watermarking of [7], if $\mathbf{D}_k$ is set as a long-term key, then the business model of the content distribution system has to be a package sale, which disregards the consumers who just would like to buy a single digital content. Furthermore, two kinds of collusion attacks could be conducted on the LUT-based watermarking of [7], which are the collusion attacks on watermarked contents and on decrypted LUTs, respectively. In the following subsections, we give the details of the two kinds of collusion attacks[1] and some remarks based on the analysis, respectively.

A. COLLUSION ATTACK ON WATERMARKED CONTENTS

The collusion attack on watermarked contents is the most common kind of collusion attack, which constructs an attacked content by averaging the watermarked contents of the malicious clients involving in the collusion attack. Here, we assume that there are $\bar{N}$ malicious clients involving in the collusion attack. Let $\mathbf{y}_0, \mathbf{y}_1, \cdots, \mathbf{y}_{\bar{N}-1}$ denote the watermarked contents of the $\bar{N}$ malicious clients, respectively. And let $\mathbf{y}^A$ denote the average of the watermarked contents $\mathbf{y}_0, \mathbf{y}_1, \cdots, \mathbf{y}_{\bar{N}-1}$. Then, according to Eq. (3), it is obtained that

$$\begin{aligned}\mathbf{y}^A &= \frac{1}{\bar{N}} \sum_{k=0}^{\bar{N}-1} \mathbf{y}_k \\ &= \frac{1}{\bar{N}} \sum_{k=0}^{\bar{N}-1} (\mathbf{x} + \mathcal{T}\mathbf{W}_k) \\ &= \mathbf{x} + \frac{1}{\bar{N}} \mathcal{T} \sum_{k=0}^{\bar{N}-1} \mathbf{W}_k.\end{aligned} \tag{4}$$

[1] Collusion attack refers to a group of malicious clients gather their individual knowledge of watermarking system to obtain an attacked content in which none of their watermarks can be reliably detected [7], [26].

Eq. (4) shows that the attacked content $\mathbf{y}^A$ is identical to the original content added by the linear-transformed average watermark LUTs of the $\bar{N}$ malicious clients, which consists with the viewpoint of Celik *et al.* [7] that the averaging attack on watermarked contents is equivalent to an averaging attack on watermark LUTs. In the SS watermarking scenario, the entries of watermark LUT are often selected according to Gaussian distribution with zero mean [27], [28]. It is obvious that the attacked content $\mathbf{y}^A$ is much closer to the original content $\mathbf{x}$ than any of the watermarked contents $\mathbf{y}_0, \mathbf{y}_1, \cdots, \mathbf{y}_{\bar{N}-1}$. And each of the watermarks of the $\bar{N}$ malicious clients is difficult to be detected from the attacked content if the value of $\bar{N}$ is large enough.

B. COLLUSION ATTACK ON DECRYPTION LUTs

Since all of the clients share the same long-term encryption LUT $\mathbf{E}$, the LUT-based embedding is also vulnerable to the collusion attack on decryption LUTs. The $\bar{N}$ malicious clients involving in the collusion attack can first estimate the encryption LUT $\mathbf{E}$ by averaging their personalized decryption LUTs. Our analysis is as follows.

Let $\mathbf{D}_0, \mathbf{D}_1, \cdots, \mathbf{D}_{\bar{N}-1}$ denote the personalized decryption LUTs of the $\bar{N}$ malicious clients, respectively. And let $\bar{\mathbf{D}}$ denote the average of the decryption LUTs $\mathbf{D}_0, \mathbf{D}_1, \cdots, \mathbf{D}_{\bar{N}-1}$. According to Eq. (1), $\bar{\mathbf{D}}$ can be evaluated by follows

$$\begin{aligned}\bar{\mathbf{D}} &= \frac{1}{\bar{N}}\sum_{k=0}^{\bar{N}-1}\mathbf{D}_k \\ &= \frac{1}{\bar{N}}\sum_{k=0}^{\bar{N}-1}(-\mathbf{E}+\mathbf{W}_k) \\ &= -\mathbf{E}+\frac{1}{\bar{N}}\sum_{k=0}^{\bar{N}-1}\mathbf{W}_k.\end{aligned} \tag{5}$$

Note that the average LUT $\bar{\mathbf{D}}$ is identical to the negative encryption LUT $\mathbf{E}$ (i.e., $-\mathbf{E}$) added by the average watermark LUTs of the $\bar{N}$ malicious clients. And it is obvious that the average LUT $\bar{\mathbf{D}}$ is much closer to the negative encryption LUT $\mathbf{E}$ than any of the personalized decryption LUTs of the $\bar{N}$ malicious clients.

After obtaining the average LUT $\bar{\mathbf{D}}$, client k, who involves in the collusion attack, can replace his or her personalized decryption LUT $\mathbf{D}_k$ with the average LUT $\bar{\mathbf{D}}$, and then decrypt the encryption content $\mathbf{c}$ using the average LUT $\bar{\mathbf{D}}$ and the session K to construct an attacked content $\mathbf{y}_k^B$. According to Eqs. (2), (3), and (5), it is obtained that

$$\begin{aligned}\mathbf{y}_k^B &= \mathbf{c}+\mathcal{T}\bar{\mathbf{D}} \\ &= \mathbf{c}-\mathcal{T}\mathbf{E}+\frac{1}{\bar{N}}\mathcal{T}\sum_{k=0}^{\bar{N}-1}\mathbf{W}_k \\ &= \mathbf{x}+\frac{1}{\bar{N}}\mathcal{T}\sum_{k=0}^{\bar{N}-1}\mathbf{W}_k.\end{aligned} \tag{6}$$

Let $\mathbf{y}_0^B, \mathbf{y}_1^B, \ldots, \mathbf{y}_{\bar{N}-1}^B$ denote, respectively, the attacked contents constructed by the $\bar{N}$ malicious clients involving in the collusion attack on decryption LUTs. According to Eqs. (4) and (6), it is obvious that $\mathbf{y}^A = \mathbf{y}_0^B = \mathbf{y}_1^B = \ldots = \mathbf{y}_{\bar{N}-1}^B$, which shows that the collusion attack on decryption LUTs is the same as the collusion attack on watermarked contents. However, in contrast to the collusion attack on watermarked contents, the collusion attack on decryption LUTs can not only construct the attacked images, but also estimate the long-term encryption key (i.e., the encryption LUT $\mathbf{E}$).

C. REMARKS

It is obvious that the more the number of the contents decrypted by $\mathbf{D}_k$ is, the more loss will be caused by the collusion attacks on the LUT-based watermarking. Based on the above analysis, the personalized decryption key $\mathbf{D}_k$ and the corresponding encryption key $\mathbf{E}$ had better be set as short-term keys instead of long-term keys. Of cause, if $\mathbf{D}_k$ and $\mathbf{E}$ is set as short-term keys, the burden of the key management will inevitably increase. For the sake of understanding, we give the following two remarks.

- *Remark* 1: According to Eqs. (5) and (6), it is seen that the collusion attack on decryption LUTs can be performed even if only one of the malicious clients involving in the collusion attack possesses the encryption content $\mathbf{c}$ and the session K. Therefore, the other malicious clients need not to apply for the encryption content $\mathbf{c}$ and the session K again from the server. This cannot be done by the collusion attack on watermarked contents. If the application of the encryption content $\mathbf{c}$ and the session K costs money (we think that, in most cases, it is not free), the collusion attack on decryption LUTs will spend much less money than the attack on watermarked contents on performing an attack.
- *Remark* 2: Eq. (5) shows that if there are a large enough number of malicious clients who involve in the collusion attack on decryption LUTs, these malicious clients can obtain an average LUTs $\bar{\mathbf{D}}$ that is very close to the encryption key $\mathbf{E}$. Once the average LUT $\bar{\mathbf{D}}$ is leaked maliciously (for example, it is possible that the malicious clients sell the average LUT $\bar{\mathbf{D}}$ for profit). Then every client of the content distribution system could remove his or her personalized watermark by replacing his or her personalized decryption LUT with the average LUT $\bar{\mathbf{D}}$. In this case, the server of the content distribution system has to reset its long-term encryption key $\mathbf{E}$ and the personalized decryption LUTs, and then redistributes the personalized decryption LUTs to the clients. A long-term secret key which is reset frequently tends to become the short-term key.

IV. SIMULATION RESULTS

In this section, a number of simulations have been carried out to demonstrate the effectiveness of the proposed analysis. In our simulations, 10,000 host signals are generated for testing joint decryption/watermarking and collusion attack, and these host signals are normally independently and identically distributed (i.i.d.) with zero mean and variance $\sigma_{\mathbf{x}}^2$, i.e. for $\forall i \in [M]$, $\mathbf{x}(i) \sim \mathcal{N}(0, \sigma_{\mathbf{x}}^2)$. Simulation results provided in this paper are averaged on these 10,000 signals. Like the host signal, the watermark LUT and encryption LUT are also i.i.d. generated respectively by $\mathbf{W}_k(j) \sim \mathcal{N}(0, \sigma_{\mathbf{W}}^2)$ and $\mathbf{E}(j) \sim \mathcal{N}(0, \sigma_{\mathbf{E}}^2)$ for $\forall j \in [L]$ and $\forall k \in [N]$. The document-to-watermark ratio (DWR) is used to evaluate the watermarking strength, which is defined by

$$\mathrm{DWR}_{[\mathrm{dB}]} = 10 \log_{10} \left(\frac{\sigma_{\mathbf{x}}^2}{\sigma_{\mathbf{w}}^2} \right), \tag{7}$$

where $\sigma_{\mathbf{w}}^2$ denotes the power of watermark signal and $\sigma_{\mathbf{w}}^2 = S \cdot \sigma_{\mathbf{W}}^2$ in our setup. The normalized correlation ratio is used to evaluate the performance of collusion attacks, which is defined by

$$C(\mathbf{y}, \hat{\mathbf{y}}) = \frac{\mathbf{y}^T \hat{\mathbf{y}}}{\|\mathbf{y}\|_2 \|\hat{\mathbf{y}}\|_2}, \tag{8}$$

where $\|\cdot\|_2$, $\mathbf{y}$, and $\hat{\mathbf{y}}$ denote L_2-norm, the watermarked signal, and its collusively attacked version, respectively. The detailed setup is listed in Table I. These simulations consist of the following two parts.

TABLE 1. Parameter setup in the simulation.

Parameter	Value
Host signal	$\sigma_{\mathbf{x}}^2 = 1,\ M = 10^7$
Watermark LUT	$\sigma_{\mathbf{W}}^2 = 0.002,\ L = 10^5$
Encryption LUT	$\sigma_{\mathbf{E}}^2 = 0.2,\ L = 10^5$
Embedding strength	DWR=20 dB
Number of clients	$N = 10^8$
Number of conspirators	$\bar{N} = 20$
Number of encryptions	$S = 5$

A. COLLUSION ATTACK ON WATERMARKED CONTENTS

First, a simulation was carried out to show how the performance of collusion attack on watermarked contents varies when the number of malicious clients (conspirators) changes. The curves of correlation ratio are drawn in Fig. 3. We can see from Fig. 3 the correlation ratio between the watermark message $\mathbf{W}_k$ and the watermarked signal embedded with the same watermark message $\mathbf{W}_k$ is much greater than other two cases and remains unchanged as malicious clients $\bar{N}$ varies. This shows that the personalized fingerprint $\mathbf{W}_k$ can be accurately tracked. However, the correlation ratio between the watermark message $\mathbf{W}_j$ and the watermarked signal embedded with the another different watermark message $\mathbf{W}_k$ is always close to zero. This is because the two different watermark messages $\mathbf{W}_j$ and $\mathbf{W}_k$ $(k \neq j)$ are set to be orthogonal in our setup. This implies that the fingerprinting set in our simulation has a good distinguishable ability. This also means the fragility of fingerprinting is perfect in the case of free noise. Finally, we can see from Fig. 3 that the correlation ratio between a special watermark message $\mathbf{W}_k$ and the collusively attacked version $\hat{\mathbf{y}}$ decreases sharply as the malicious clients $\bar{N}$ increases and reduces to zero when $\bar{N}$ increases to approximately 20. This means that the detection of any client's fingerprint fails under the collusion attack, which is coincided with our analysis presented in Section III-A.

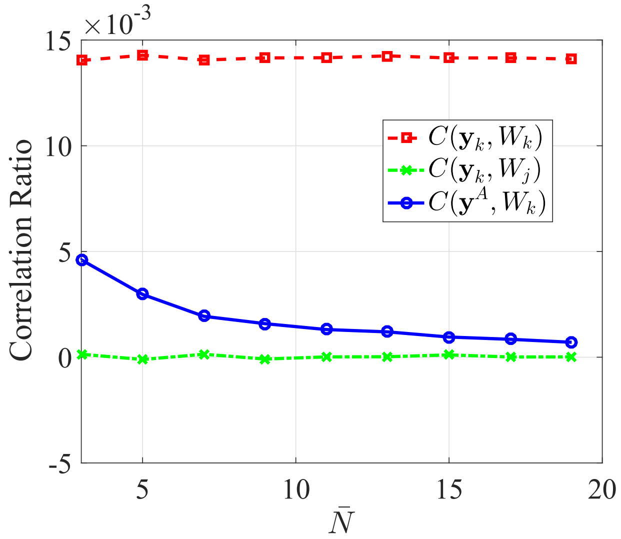

FIGURE 3. Comparison of various correlation ratios. Note that here for $\forall k, j \in [N], k \neq j$.

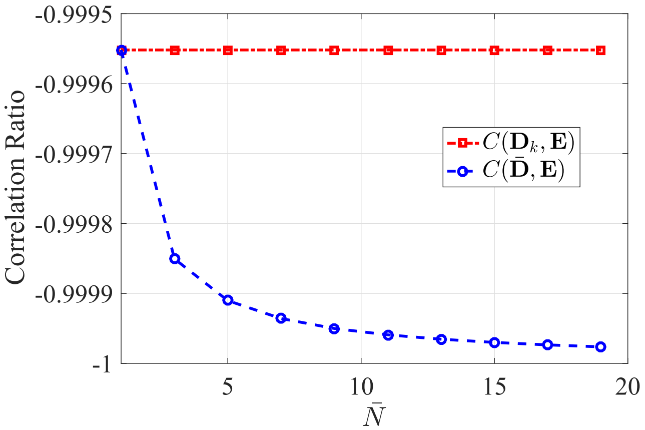

FIGURE 4. Illustration of the collusion attack on decryption LUT.

B. COLLUSION ATTACK ON DECRYPTION LUTs

Then, the performance of collusion attack on decryption LUTs is tested and compared with that of the collusion attack on watermarked contents. According to our analysis on the business model, the encryption key can be estimated by collecting several different decryption LUTs. The result is shown in Fig. 4. We can see from Fig. 4 that the correlation ratio between the encryption key and any decryption key $\mathbf{D}_k$ is independent of malicious clients $\bar{N}$ and keeps unchanged. However, the correlation ratio between the average LUT $\bar{\mathbf{D}}$

and the true encryption LUT $\mathbf{E}$ is close to -1 as malicious clients $\bar{N}$ increases. This implies that the estimate of encryption LUT $\mathbf{E}$ is considerably accurate. Note that the accurate estimate of encryption key is efficient enough to defeat the secure content distribution system proposed by Celik *et al*.

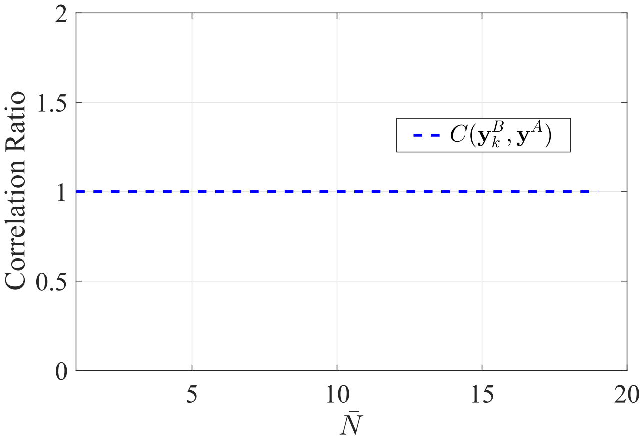

FIGURE 5. Illustration of the equivalency of collusion attacks on the watermarked content and the decryption LUTs.

In the following, we further show that the collusion attack on decryption LUTs is equivalent to the collusion attack on watermarked contents. According to Eq. (6), $\mathbf{y}_k^B$ is obtained using the average decryption LUT for joint decryption/watermarking. For $\forall k \in [N]$, the curve of correlation ratio between $\mathbf{y}^A$ and $\mathbf{y}_k^B$ is drawn in Fig. 5. It can be seen from Fig. 5 that the correlation ratio always equals 1 no matter what value the malicious clients $\bar{N}$ takes. This implies these two collusion attacks are totally equivalent, which is also consistent with our analysis presented in Section III-B.

V. CONCLUSION

Digital watermarking has been widely used to protect copyrights of digital contents. Recently, Celik *et al.* [7] proposed a LUT-based client-side embedding for preventing clients from maliciously copying and distributing digital contents in a mass-sale content distribution scenario. From a security viewpoint, this paper has provided an analysis on the business model of the secure content distribution system applying the LUT-based client-side embedding. We have found that the collusion attack on decryption LUTs is equivalent to the collusion attack on watermarked contents. Simulation results have shown the effectiveness of our analysis. Therefore, the content distribution system applying the LUT-based client-side embedding can only be used for package sale, which limits its applications. In order to extend the applications of the content distribution system that applies the LUT-based client-side embedding, we suggest to set the encryption and decryption LUTs of the LUT-based client-side embedding as short-term keys instead of long-term keys. However, how to efficiently manage the short-term keys in such special client-side watermark embedding system will be the direction of our future work.

REFERENCES

[1] M. Barni and F. Bartolini, "Data hiding for fighting piracy," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 28–39, Mar. 2004.

[2] Y.-G. Wang, G. Zhu, and J. Huang, "An improved sample projection approach for image watermarking," *Digit. Signal Process.*, vol. 24, no. 1, pp. 135–143, Jun. 2014.

[3] Y.-G. Wang and G. Zhu, "An improved AQIM watermarking method with minimum-distortion angle quantization and amplitude projection strategy," *Inf. Sci.*, vol. 316, pp. 40–53, Sep. 2015.

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[5] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 898–905, Apr. 2003.

[6] J. Zhong and S. Huang, "An enhanced multiplicative spread spectrum watermarking scheme," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 12, pp. 1491–1506, Dec. 2006.

[7] 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 Security*, vol. 3, no. 3, pp. 475–487, Sep. 2008.

[8] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev*, vol. 40, no. 3, pp. 278–286, May 2010.

[9] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[10] Y.-G. Wang, G. Zhu, and Y.-Q. Shi, "Transportation spherical watermarking," *IEEE Trans. Image Process.*, vol. 27, no. 4, pp. 2063–2077, Apr. 2018, doi: 10.1109/TIP.2018.2795745.

[11] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Trans. Image Process.*, vol. 8, no. 11, pp. 1534–1548, Nov. 1999.

[12] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1069–1087, Apr. 2003.

[13] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[14] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[15] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, and M. Maas, "A buyer–seller watermarking protocol based on secure embedding," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 783–786, Dec. 2008.

[16] 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 Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[17] T. Bianchi and A. Piva, "TTP-free asymmetric fingerprinting based on client side embedding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1557–1568, Oct. 2014.

[18] 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, Mar. 2013.

[19] C.-Y. Lin, P. Prangjarote, C.-H. Yeh, and H.-F. Ng, "Reversible joint fingerprinting and decryption based on side match vector quantization," *Signal Process.*, vol. 98, pp. 52–61, May 2014.

[20] B. Czaplewski, "Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher quaternion chaining," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 1–13, Oct. 2016.

[21] F. Frattolillo, "Watermarking protocols: An excursus to motivate a new approach," *Int. J. Inf. Secur.*, to be published, doi: 10.1007/s10207-017-0386-9.

[22] C.-Y. Lin, P. Prangjarote, L.-W. Kang, W.-L. Huang, and T.-H. Chen, "Joint fingerprinting and decryption with noise-resistant for vector quantization images," *Signal Process.*, vol. 92, no. 9, pp. 2159–2171, 2012.

[23] B. Czaplewski and R. Rykaczewski, "Matrix-based robust joint fingerprinting and decryption method for multicast distribution of multimedia," *Signal Process.*, vol. 111, pp. 150–164, Jun. 2015.

[24] T. Bianchi, A. Piva, and D. Shullani, "Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding," *EURASIP J. Inf. Secur.*, vol. 2015, Dec. 2015, Art. no. 6.

[25] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "Study of imposter attacks on novel fingerprint dynamics based verification system," *IEEE Access*, vol. 5, pp. 595–606, 2017.

[26] G. Doerr and J.-L. Dugelay, "Collusion issue in video watermarking," *Proc. SPIE*, vol. 5681, pp. 685–696, Mar. 2005.

[27] Y.-G. Wang, G. Zhu, S. Kwong, and Y.-Q. Shi, "A study on the security levels of spread-spectrum embedding schemes in the woa framework," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2017.2735989.2017.

[28] B. Mathon, F. Cayre, P. Bas, and B. Macq, "Optimal transport for secure spread-spectrum watermarking of still images," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1694–1705, Apr. 2014.

YUAN-GEN WANG received the B.S. degree in physics from Jiangxi Normal University, Nanchang, China, in 1999, and the M.E. and Ph.D. degrees in communication and information system from Sun Yat-sen University, Guangzhou, China, in 2006 and 2013, respectively. He was with the Zhongkai University of Agriculture and Engineering, Guangzhou, China, as a Lecturer, from 2006 to 2011, and as an Associate Professor, from 2011 to 2017. From 2015 to 2016, he was a Research Scholar with the New Jersey Institute of Technology, Newark, NJ, USA. He is currently an Associate Professor with Guangzhou University, Guangzhou, China. He has authored or co-authored over 10 papers in the SCI journals. His research interests include digital watermarking, forensics, and image processing.

DONGQING XIE received the Ph.D. degree in applied mathematics from Hunan University in 1999. He is currently a Professor and a Ph.D. supervisor with the School of Computer Science, Guangzhou University, China. His main research interests include algorithm cybersecurity and algorithm design. He has published over 80 research papers and four books at various venues. He has won around two dozen grants from different funding sources. He has served the professional communities in various roles, such as panel chairs and conference chairs. He is a member of China Computer Federation.

BRIJ B. GUPTA received the Ph.D. degree from the IIT Roorkee, India, in the area of information and cybersecurity. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada Award (10,000 dollars). He spent over six months in the University of Saskatchewan, Canada, to complete a portion of his research work. He was a Visiting Researcher with Yamaguchi University, Japan, in 2015, and with Guangzhou University, China, in 2016. He is currently an Assistant Professor with the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. He has published over 80 research papers (including two book and 14 chapters) in International Journals and Conferences of high repute including the IEEE, Elsevier, ACM, Springer, Wiley, and Inderscience. His research interest includes information security, cybersecurity, mobile/smartphone, cloud computing, web security, intrusion detection, computer networks, and phishing. He has visited several countries, i.e., Canada, Japan, China, Malaysia, and Hong-Kong to present his research work. His biography was selected and published in the 30th Edition of Marquis Whos Who in the World, 2012. He is serving as a Guest Editor of various Journals.