Hindawi
Security and Communication Networks
Volume 2021, Article ID 9864833, 15 pages
https://doi.org/10.1155/2021/9864833

Research Article

PRUDA: A Novel Measurement Attribute Set towards Robust Steganography in Social Networks

Liyan Zhu[1,2], **Jinwei Wang**[1,3], **Xiangyang Luo**[1,2], **Yi Zhang**[1,2], **Chunfang Yang**[1,2] **and Fenlin Liu**[1,2]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Henan, China*
[2]*P. L. A. Information Engineering University, Henan, China*
[3]*Nanjing University of Information Science and Technology, Jiangsu, China*

Correspondence should be addressed to Xiangyang Luo; luoxy_ieu@sina.com

Received 24 May 2021; Accepted 17 August 2021; Published 31 August 2021

Academic Editor: Debiao He

Cloud services have become an increasingly popular solution to provide different services to clients. More and more data are outsourced to the cloud for storage and computing. With this comes concern about the security of outsourced data. In recent years, homomorphic encryption, blockchain, steganography, and other technologies have been applied to the security and forensics of outsourced data. While encryption technologies such as homomorphic encryption and blockchain scramble data so that they cannot be understood, steganography hides the data so that they cannot be observed. Traditional steganography assumes that the environment is lossless. Robust steganography is grounded in traditional steganography and is proposed based on a real lossy social network environment. Thus, researchers, who study robust steganography, believe that the measurement should follow traditional steganography. However, the application scenario of robust steganography breaks through the traditional default lossless environment premise. It brings about changes in the focus of steganography algorithms. Simultaneously, the existing steganography methods miss the evaluation of applicability and ease of use. In this paper, "default parameters" are observed by comparing the process of robust image steganography with traditional image steganography. The idea of "perfecting default parameters" is proposed. Based on this, the attribute set of measuring robust image steganography is presented. We call it PRUDA (Payload, Robustness, ease of Use, antiDetection, and Applicability). PRUDA perfects default parameters observed in the process of traditional steganography algorithms. Statistics on image processing attacks in mobile social apps and analyses on existing algorithms have verified that PRUDA is reasonable and can better measure a robust steganography method in practical application scenarios.

1. Introduction

With the proliferation of mobile terminals and the astonishing expansion of the mobile Internet, Internet of things, and cloud computing, more and more data are outsourced to cloud storage systems because once the data are shared with untrusted servers, there are potential risks that the data might be modified or replicated by unauthorized servers. Users worry that when they outsource their data to untrusted parties, they lose control of the outsourced data, and the ownership of the data is not well guaranteed. Thus, users are reluctant to share their data in these network environments with other entities they do not trust because of privacy concerns. To address this issue, many schemes have been proposed to protect outsourced data security. Homomorphic encryption [1, 2], blockchain [3, 4], and steganography [5, 6] are effective methods that have been popular in recent years. When using homomorphic encryption and blockchain to encrypt and verify the outsourced data, the carrier transmitted over the channel and stored in the cloud are garbled media. The garbled media is easy to attract the attention of attackers. Steganography embeds private data into normal media, and the carrier transmitted over the channel and stored in the

cloud is everyday media. It not only hides the content of data but also hides its existence. Thus, the data are doubly insured.

The photos and pictures of blowout growth [7] shared on social applications, post bars, and open websites provide natural carriers for steganography. For the sake of speed or other bandwidth considerations, images are often processed unexpectedly (such as scaled or compressed) in the cloud environment. The traditional image steganography method cannot function effectively in this lossy environment. Based on this, robust image steganography is introduced [8]. Traditional steganography methods usually focus on designing proper distortion functions. The aim is to improve antistatistical detection performance by keeping the modifications concentrated on complicated texture areas adaptively [9, 10], or the pixels' modification directions met expectation [11]. Robust image steganography [12–17] has inherited a lot from traditional image steganography. For example, the measurement attributes. New problems arise due to the different application backgrounds of robust image steganography.

Figure 1 shows the application scenarios of traditional steganography and robust steganography. A stego image is transmitted in a lossless environment in traditional steganography (Figure 1(a)) while it is transmitted in an open lossy environment in robust steganography (Figure 1(b)). Measurement attributes are born in traditional steganography (the blue dashed tail arrow) and used to evaluate all steganography methods (the regular blue arrows). The application background of robust steganography, lossy environment (e.g., Wechat1 and Facebook2), is not reflected (the hollow green arrow) in the measurement attributes. As one robust steganography method after another was proposed, the contradiction between the measurement attributes and the robust steganography is gradually exposed.

The existing robust image steganography methods can be divided into methods combing with watermarking algorithm and methods digging environment features (or called channel features which refer to lossy operations in transmission or the cloud) according to the algorithm's idea. The former obtained the wanted robustness while introducing the unwanted low embedding rate and poor antidetection performance such as DCRAS [8], GMAS [16], and MREAS-P_J [17]. Some researchers tried to dig channel features and simulated channel attacks to keep attacks that images suffered when transmitting are predictable such as designing a transport channel matching [12], adjusting cover images according to the received image [13], constructing an autoencoder [14], and utilizing a simulated repetitive compression network [15]. These methods always had good antidetection performance and a higher embedding rate. However, they generally had relatively strict restrictions on channels. Otherwise, the robustness would be reduced.

All these methods consider reducing the message extraction error rates while maintaining [15] (sometimes sacrificing [17]) the antistatistical detection ability. Antistatistical detection ability is one of the essential attributes to measuring traditional steganography. It means that the measurement attributes are beginning to diverge. For traditional steganography, two key attributes of the measurement are message embedding capacity (payload) and antistatistical detection ability [18]. There are also eyes on embedding efficiency [19], color frequency test [20], and dual statistics attacks [21]. The validity of antistatistical detection abilities has been challenged because of the impact of network behaviors [22].

With profound research in robust image steganography, some questions arose. Is there any disadvantage to measuring robust image steganography using them directly? Are they suitable for the application background of a lossy environment? When evaluating a robust steganography method using the traditional measurement attributes directly, the usage of measurement attributes has been altered to some extent. These nonuniform settings hamper comparisons between methods. It means traditional measurement attributes begin to limit robust steganography methods. Besides, because the existing measurement attributes do not consider the lossy environment's application background, the evaluation of a method is incomprehensive. These indicate that the existing measurement attributes cannot accurately evaluate robust image steganography.

Based on the above considerations, we try to look for suitable measurement attributes for robust image steganography. We first compare the transmission process of robust image steganography and traditional steganography. The "default parameter" is observed, and the concept of "perfecting default parameter" is naturally introduced. The attribute set PRUDA (Payload, Robustness, ease of Use, antiDetection, and Applicability) is presented based on this. The main contributions are as follows:

(i) The concept of "perfecting default parameter" is proposed. It provides a direction for the attribute set perfection and may offer inspiration to other related measurements' improvement.

(ii) Contrasting the pursuits and application background of robust image steganography with the existing measurement attributes, the attribute set PRUDA is proposed. It may measure robust image steganography comprehensively and may push this field closer to the practical application faster.

(iii) A large number of statistics on processed images and open lossy channel attacks are given. They verify the rationality of PRUDA and can be used as the application basis of the relevant research on robust image steganography.

The rest of this paper is organized as follows: in Section 2, we introduce the concept of "perfecting default parameters." Then, logically and smoothly, by perfecting the "default parameters" of traditional steganography, a new measurement attribute set, "PRUDA," is proposed and elaborated in Section 3. Next, the rationality of PRUDA is verified in Section 4. Finally, the paper is discussed and concluded in Section 5.

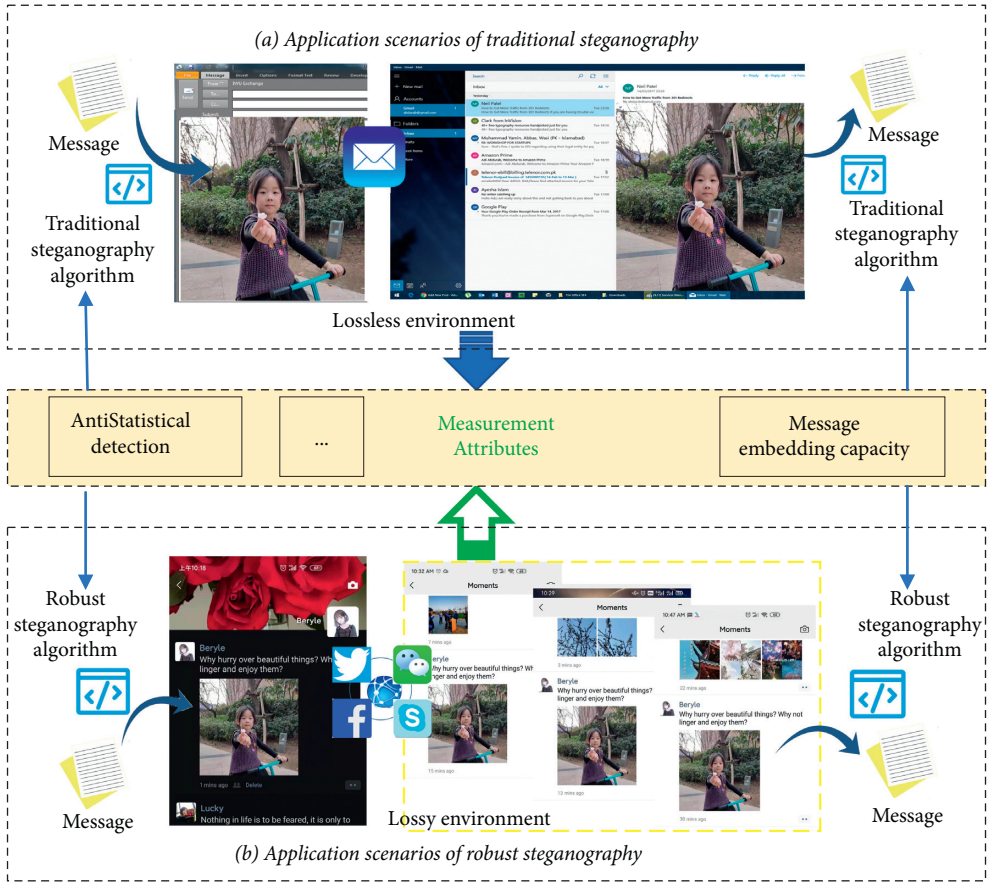

Figure 1: Comparison between application scenarios of (a) traditional steganography and (b) robust steganography.

2. The Concept of "Perfecting Default Parameters"

Figure 2 shows the comparison between the transmission process of traditional image steganography (Figure 2(a)) and robust image steganography (Figure 2(b)). The upper left box is the legend. As shown in Figure 2(a), the cover image can be any image for traditional image steganography. The sender embeds the secret messages of a given payload into a cover image and generates a stego image. The stego image is transmitted through a lossless channel [23]. The receiver extracts the secret message from the received stego image. In this process, the steganalyzer distinguishes the cover and stego image by statistical detection.

As shown in Figure 2(b), to ensure that the secret message can be extracted from a stego image transmitted through the public lossy channel, more operations are added in the transmission process of robust image steganography. Thus, this process is more complicated than that of traditional steganography. The cover image is no longer an arbitrary original image but maybe the image with specific features or the preprocessed image. The sender embeds the secret message of a given payload into a prefiltered or preprocessed cover image. Many algorithms encode the secret message first before embedding to reduce the message extraction error rate. Thus, the actual message embedding rate may be lower than that of the desired. The encoded message is always embedded into the prefiltered or preprocessed cover image, and the stego image is generated. When the stego image is transmitted through a public lossy channel, it may be subjected to scaling and compression attacks. After the stego image is received, the corresponding extraction steps are performed. In this process, the steganalyzer still distinguishes the cover and stego image by statistical detection. Nevertheless, it is worth a reminder that the cover image here is always not the original image but the prefiltered or preprocessed image.

The cover image, message extraction error rate, and environment are not considered when studying traditional steganography. We name them "default parameters." Specifically speaking, the traditional steganography algorithm can use any cover image to embed messages. The message extraction error rate is zero. The environment is lossless, and the stego image is unchanged before and after transmission. The only consideration in the whole process is to reduce the possibility of detecting the stego image and extract messages correctly. Therefore, it is reasonable to take antistatistical detection ability and message extraction error rate as the attributes of the measurement of traditional steganography.

To ensure robustness and improve antidetection performance, "default parameters" have changed a lot in robust image steganography. The cover image may not be arbitrary, but the prefiltered or preprocessed image. It directly affects the message embedding rate, which is computed based on

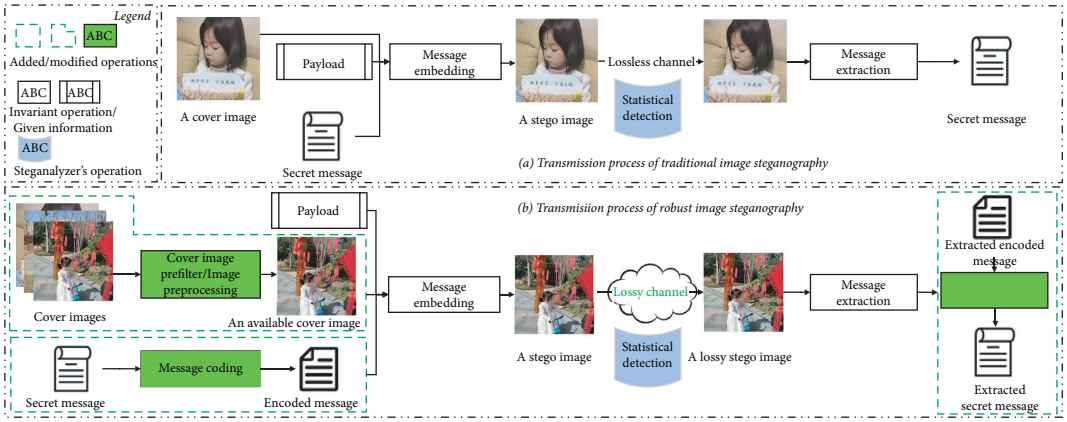

Figure 2: Comparison between transmission process of (a) traditional and (b) robust image steganography.

the cover image. Messages are no longer embedded directly but are first encoded using various codes. The environment is a public and lossy channel with its own transmission rules. Images and behaviors that do not obey these rules would be easily detected [24]. Stego images suffer attacks during transmission. After transmission, their image sizes and file sizes are uncertain. It is challenging to ensure the stego image's consistency of the sender and the receiver, so is the message extraction accuracy rate.

This is the complex environment faced by robust image steganography, in which "default parameters" are no longer default. Researchers try to enhance robustness considering the lossy environment. However, when evaluating the method, they directly use the measurement attributes of traditional steganography. This paper focuses on this neglected point and argues that it is time to perfect default parameters. "Perfecting default parameters" means to perfect those parameters that are no longer default to the measurement to take the actual application background (the lossy environment/channel) into account. We believe this can help robust image steganography towards practical applications.

3. PRUDA

Reasonable measurement attributes are essential to promote the research of robust image steganography. In this section, a five-sphere measurement attribute set, PRUDA, is put forward. As shown in Figure 3, PRUDA considers five perspectives. Payload is the message embedding rate of an image transmitted through the lossy channel. Considering the lossy channel's effect, the definition is extended by perfecting the definition: message embedding rate in the traditional steganography method. Robustness refers to the resistance of a stego image to attacks from the lossy channel. The definition is extended considering the feature and fault-tolerant retransmission mechanism of lossy channels. AntiDetection is defined as the unidentifiability and indistinguishability of images. The definition is updated considering the actual application background of robust steganography. Ease of Use means the difficulty of using the method, or rather, the difficulty of obtaining cover images. Applicability refers to the degree to which the channel is constrained by the method. Ease of Use and Applicability are two novel attributes proposed by perfecting two default parameters: cover image and environment in the traditional steganography method.

The attribute set PRUDA perfects the explicit and implicit (default) measurement attributes of traditional steganography. It not only inherits the measurement attributes of traditional steganography but also considers the actual application scenarios of robust image steganography. Thus, it can measure the robust image steganography method more accurately.

3.1. Payload. Payload is defined as the message embedding rate $p = n/n_I$ in traditional steganography, where n is the number of embedded messages, n_I is the number of pixels (spatial domain), or the nonzero AC coefficients (frequency domain) in an image. The "image" in the definitions refers to the sender's cover image and is represented by I.

I has undergone a great change in robust image steganography. Unlike traditional steganography methods [25, 26], which uniformly define I as any cover image, I is defined differently in various robust steganography methods. For example, in Yu et al.'s method [16], I is defined as a precompressed image, while in Zhang et al.'s method [27], I is defined as a scaled image.

Like I, n has changed a lot too. Unlike traditional steganography, where n represents there are n messages embedded, robust steganography methods have embedded far fewer messages than n. The reason for this is that in robust steganography methods, messages are often encoded first before embedded, such as RS (Reed–Solomon) [16], CRC (Cyclic Redundancy Check) [28], and BCH (Bose–Chaudhuri–Hocquenghem) [12]. That is, n is the encoded message. Thus, the effective message embedding rate p is lower than expected to some extent.

This inconsistency hampers the comparison of methods and is not conducive to the development of this field. Therefore, Payload needs to be unified, and it is redefined as

$$p = \frac{(n - n_{\text{em}})}{n_{RI}}, \tag{1}$$

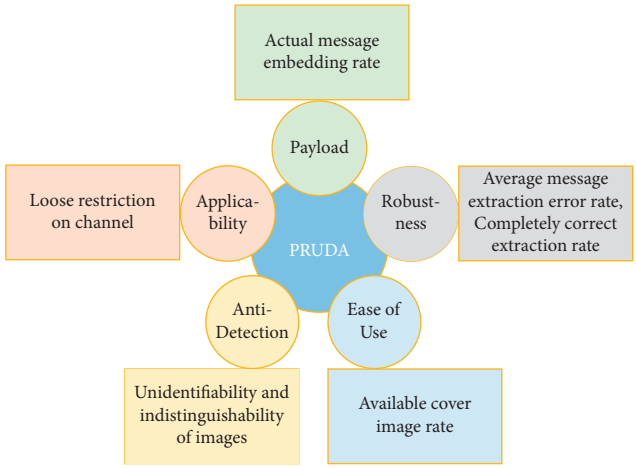

Figure 3: Five-sphere measurement set PRUDA.

where n_{em} and n_{RI} represent the number of embedded error correction code and the number of pixels (or nonzero AC coefficients) of "the open-processed image" RI, respectively. RI refers to the image performed simple, reasonable processing that most users would do, such as scaling an image to the received image's image size, precompressing an image once. p represents the percentage of embedded messages in RI. $(n - n_{em})$ represents the number of effective embedded messages.

This definition considers the inconsistency of payload calculation caused by the inconsistency of message encoding and cover image in robust image steganography, thus avoiding the differential use of message embedding rate and building a comparison bridge between different methods.

3.2. Robustness. Robustness refers to the resistance of a stego image to attacks from a lossy channel. Reflected in measurement attributes, it is the integrity of the messages extracted from the image attacked. For robust image steganography, the unit transmitted in the public lossy channel is the image. The unit of the sender embedding messages and that the receiver extracting messages is the image too. Considering the fault-tolerant retransmission mechanism in practical applications (if a fragment of messages fails to be extracted, the sender is requested to resend), the message complete extraction rate of the image is challenged. In other words, in the practical application, if N images are sent, and messages embedded in Nr images can be extracted entirely, then messages in $N - Nr$ images need to be resent. If messages embedded in each image cannot be fully extracted, even if the average message extraction error rate is low, the sender still needs to resend all the images.

The average message extraction error rate is one of the default parameters of traditional steganography and is 0. For existing robust image steganography methods, the average message extraction error rate of 0 comes with many constraints. Otherwise, the rate is far from zero. The message extraction utterly is the ultimate goal of robust image steganography. Considering the fault-tolerant retransmission mechanism in practical applications, assigning two meanings to robustness to measure the method's effectiveness is more practical. (1) The current average message extraction error rate $R_e = n_e/n$, where n_e is the number of message bits mistakenly extracted from every image, and n is the total number of embedded messages in the image. (2) The completely correct extraction rate $R_r = N_r/N$, where N_r is the number of stego images that can extract the completely correct message, and N is the total number of stego images. Giving robustness with these two meanings considers the extraction accuracy of each image and the overall average extraction error rate.

3.3. Ease of Use. For a user, the ease of use of a method has nothing to do with the method's complexity but with the difficulty of using it. The internal implementation is encapsulated when the product is released, and interactions with users depend on input and output parameters.

For the traditional steganography method, the input is generally a cover image, messages transmitted, and a shared key to the sender. The output is the stego image obtained by embedding messages into the cover image, transmitted through the lossy channel. As shown in

$$s \longleftarrow \mathrm{Emb}(c, k, m), \tag{2}$$

c, m, k, s, and $\mathrm{Emb}(\bullet)$ represent the cover image, secret message, shared key, stego image, and the embedding operation, respectively. $\leftarrow$ represents that after embedding operation, the stego image s is generated.

To the receiver, the input is the stego image transmitted through the lossy channel and a shared key. The output is the message extracted from the image. As shown in

$$m \longleftarrow \mathrm{Ext}(s, k), \tag{3}$$

$\mathrm{Ext}(\bullet)$ represents the extraction operation. $\leftarrow$ represents that after extraction operation, the transmitted secret message m is extracted.

We do not need to focus too much on k and m, but we have to think about c. In traditional steganography, there is generally no special requirement for c. In other words, for a traditional steganography method, c is one of the default parameters, and any image can be used as a cover; thus, the method is easy to use.

However, robust image steganography is not the case. To improve robustness or maintain antistatistical detection ability, preprocessing [12] or prefiltering [17] of cover images has gradually become one step of some steganography methods. The step limits the suitable cover images and increases the selection difficulty of cover images. It means that the cover image is no longer any image but images with particular characteristics. That is the reason why we think ease of use should be one of the attributes of measurement.

"Ease of Use" can be defined as how easy to obtain the method's cover image. As shown in

$$p_u = \frac{N_u}{N}, \tag{4}$$

N_u is the number of images available in the database. p_u is the ratio of the number of available images to the total number of images. Suppose the method is greatly affected by the "selection of cover image," and the "selection of cover image" is difficult to a certain extent. In that case, the method's usability will decline sharply, and we think that the reliability and guideline of the experimental results of the method may relatively be reduced.

3.4. AntiDetection. Steganography analysis is regarded as having promoted steganography's progress [18]. Statistical detection is an essential means of steganography analysis. Antistatistical detection ability is one of the critical evaluation attributes of steganography. However, with further development, the rationality of antistatistical detection ability has been questioned [22]. In robust image steganography, we need to pay extra attention to it.

With the advent of the mobile phone era, thousands of images are transmitted at any moment on the network, converging into an image ocean. Such an image ocean provides a natural hiding environment for stego images. In such an environment, as long as the stego image is like other images and does not attract attackers' attention, it is secure. This new security, known as behavioral security, has attracted the attention of scholars [24]. This section considers the antidetection ability from the images' perspective on robust image steganography's actual application background. It includes two aspects: (1) the image itself is unrecognizable, such as the image's size is not suspect; (2) the image is indistinguishable in the image ocean.

3.4.1. The Image Is Unrecognizable. To reduce the channel's monitor's attention, the stego image transmitted through the channel should be unrecognizable. That is, it should look similar to other images on the channel. As shown in

$$w_s \sim w_I, \tag{5}$$

w_s and s_I represent the identifiable feature of the stego image and the image transmitted on the channel, respectively. $\sim$ represents that they are approximate.

Take the most identifiable feature of images: size as an example. For a lossy channel with compression and scaling attacks, to ensure robustness, suppose smaller images are selected for transmission to avoid compression and scaling, for instance, memo, as shown in Figure 4. Memes are generally small and will not be scaled or compressed. Thus, they seem to be the right choice as robust covers. However, memes are not suitable for hiding messages, because (1) for the same messages, compared with typical size images, more emojis images are needed due to their small sizes, which is easy to attract the attention of the monitor; (2) frequently sending memes on moments where people are sharing photos is abnormal behavior [24]; and (3) memes are generally traceable; that is, their original versions are easy to locate. Besides, memes are generally of a single tone, and messages hidden in them are more likely to be extracted than those hidden in other normal photos. Therefore, memes that seem very appropriate from a robust point of view are not suitable for robust steganography. Normal photos may be more suitable.

3.4.2. The Image Is Indistinguishable. With the increasingly powerful camera apps on mobile phones, unprocessed images are rare. Unlike traditional steganography, which assumes that all images are unprocessed, nowadays, images processed are ubiquitous on social software, forums, and photo contests. When stego images mingle with kinds of images processed, the effect of a method's antistatistical detection ability is greatly weakened (Section 4.3.2). Thus, in the robust image steganography's practical application environment, it is more meaningful to consider the indistinguishability between a stego image and other images processed. As shown in

$$s \sim c^* \in \{c^* \mid c^* \text{ is processed}\}, \tag{6}$$

s and c^* represent the stego image and the processed image, respectively. $\sim$ represents that they are approximate.

Therefore, giving antidetection these two new meanings takes into account the unrecognizable of the image itself and considers the indistinguishability of the image in the general environment. It is more suitable for the practical application background of robust image steganography.

3.5. Applicability. Applicability refers to the degree to which the channel is constrained by a method. Robust image steganography studies how to extract messages correctly from the image transmitted through a lossy channel. It means the attacks that robust image steganography addressed should be those contained or possibly contained in the "open lossy environment," rather than the "imagined" ones.

At present, the robust steganography method is difficult to apply to free and open lossy channels. Focusing on the characteristics that fit, reality is a shortcut to promote research into practice. As shown in

$$f_s \sim f_c \in \{f_c \mid f_c \text{ is the channel's attack parameter}\}, \tag{7}$$

f_s and f_c represent the applicable condition of a steganography method and the real channel's attack parameter, respectively. $\sim$ represents that they are approximate.

To make the stego image resistant to an open lossy channel, in robust steganography, the constraints on the scaling/compression/other channel's attack parameters should be reasonable; it should be set within the actual factor range than be set as an imagined value. Take the most common image scaling and compression as examples.

3.5.1. Scaling Attack. Assume that the premise of a method is to know the size of the receiver's image. According to the investigation of some lossy channels, the received image's size can be determined. The channel's scaling factor remains constant for a long time. Thus, this premise is practical.

Suppose a method applies to upsampling with a scaling factor of more than five but not upsampling with a scaling

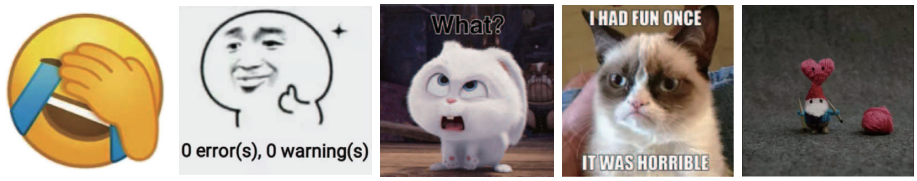

Figure 4: Examples of memes.

factor less than two and downsampling. According to surveys of real lossy channels, images are almost all downsampled on the channel. Hence, this hypothesis is impractical, and this study makes little sense in robust image steganography (however, it may be significant in other fields).

3.5.2. Compression Attack. Assume a method applies to a fixed quality factor, and when the quality factor changes a little, the method works poorly. According to surveys of real lossy channels, it is not easy to obtain the channel's accurate quality factor. Thus, this restriction may be a little harsh.

Suppose a method is useful for the quality factor within the range of a quality factor. According to the investigation of the actual lossy channel, the channel's compression factor range can be estimated, so this method's condition is reasonable.

There may be other types of attacks on the channel, and the actual attack types and attack parameters need to be fully considered in the research. Taking applicability as a measurement attribute can put the research of robust steganography to practical applications.

3.6. Observations on Five Attributes. Five attributes measure a robust steganography method from five dimensions. Different methods have different emphases and concerns, leading to different measurement dimensions.

With observations on the current development history of robust steganography, scholars' attention on attributes is affected and limited by the development of this research field. Therefore, it may be challenging to obtain a perfect method. Consideration of "lossy channel" is added in robust steganography. Thus, scholars paid more attention to Robustness in the early days, even at the expense of antiDetection and Payload [8]. Robustness had more to do with observing that attacks (such as the compression attack) were on a channel. The researchers constructed a number of attack experiments in laboratories based on the attacks they observed. That is said, research at that time [15] was "totally based on a laboratory environment." With further development, the robust steganography field has gradually gone from the "laboratory" to the "real environment." Applicability began to appear in experimental verification in some papers [16]. During this process, due to the impact of "lossy environment," the two measurement attributes of traditional steganography, Payload and antiDetection, were sacrificed to some extent [17]. At present, robust steganography is still in its infancy. Restricted to the stage, a mature robust steganography application (product) has not been released yet. Thus, Ease of Use has not been considered so far.

The above observations indicate that PRUDA's five attributes are the alchemy of quenching a robust steganography method that can only be used in a laboratory environment into one that can be used in an actual lossy environment. In essence, none of the five attributes is more important than the other. However, some attributes need to be paid special attention to at a particular development stage to facilitate a method's breakthrough. Thus, some attributes are considered to be more important than others at a specific stage of development. By perfecting attributes one by one, the robust steganography method is gradually improved, and finally, to realize the original intention of robust steganography research: achieving covert communication in an actual lossy environment.

4. Verification

In this section, we first discuss and show the not unified status quo of the existing methods. Then, the rationality and practicality of PRUDA are verified through actual statistics. Finally, since Robustness and Ease of Use are apparent, the discussion emphasizes the three attributes that may be questioned: Payload, antiDetection, and Applicability.

4.1. Verification of PRUDA's Necessity. We first gather statistics on the robust steganography methods' nonuniform measurement attributes to verify that it is necessary to perfect the existing measurement attributes. Then, an existing method is evaluated from five attributes to verify the necessity of PURDA.

4.1.1. Necessity of Perfecting Measurement Attributes. Some existing methods are analyzed from five aspects in this section, as shown in Table 1. The first column is the attack type that the second column's method can resist; the third column represents the payload used in the method, where (BCH/RS) is the algorithm used for message encoding. The fourth column shows robustness measurements used in the method (the average message extraction error rate R_e or the completely correct extraction rate R_r). The fifth column explicates what kind of images can be used as the method's cover images; the method's antistatistical detection performance is demonstrated in the sixth column. Performance calculation parameters are as follows: payload is 0.1bpp/bpnC/bpnAC (except for the method in [29, 30]). SPAM (Subtractive Pixel Adjacency Matrix) [32] feature is extracted from spatial domain images, and DCTR (Discrete

Table 1: Nonuniform measurement attributes of existing methods.

Attack type	Method	Payload	Robustness	Ease of Use	AntiDetection	Applicability
Scaling	Method in [27]	0.1–0.5bpp of scaled image	R_e	Any image	0.4936	Known scaling factor and scaling type is the nearest-neighbor interpolation
	Method in [29]	96bit	R_e, R_r	Any image	0.2082	Scaling factor greater than 0.5
	Method in [30]	128bit	R_e, R_r	Any image	0.3395	Scaling factor greater than 0.5
Compression	Method in [15]	0.1–0.15bpnC of original image	R_e	Repeatedly compressed image	0.405	No restriction
	JCRISBE [12]	0.05–0.3bpnAC of original image (BCH)	R_e	Repeatedly compressed image that meets certain requirements	0.43	Known accurate channel compression factor
	Method in [13]	0.1–0.5bpnAC of compressed image	R_e	Any image	0.42	Known accurate channel compression factor
	GMAS [16]	0.05–0.15bpnAC of precompressed image (RS)	R_e	The precompressed image	0.025	Known approximate channel compression range
	Method in [14]	0.05–0.35bpnAC of original image (BCH)	R_e	Any image	0.42	No restriction
	DCRAS [8]	0.01–0.1bpnAC of precompressed image (RS)	R_e, R_r	The precompressed image	0.055	Known approximate channel compression range
	Method in [31]	0.01–0.1bpnAC of precompressed image (RS)	R_e	The precompressed image	0.0227	Known approximate channel compression range
Multiple attacks	MREAS-P_J [17]	0.01–0.1bpnAC of precompressed image (RS)	R_e	The image that conforms to certain laws	Close to zero	Known approximate channel compression range

Cosine Transform Residual) [33] feature is extracted from frequency domain images. The seventh column gives the requirement of the method for the applicable channel.

Table 1 shows the nonuniform status of the existing methods. For example, for Payload, a fixed amount of embedded messages are used in [29, 30]'s method; in studies [12, 14, 15], an original image is the basis for calculating payload; in other papers, a scaled image or precompressed image is the basis. For Ease of Use, "any image" [13, 27] means the method is used easily; "precompressed image" [8, 16] means that the method needs to preprocess the cover image, which increases the difficulty for the use of the method; "repeatedly compressed image that meets certain requirements" [12] and "the image that conforms to certain laws" [17] mean that the method becomes more difficult to use. For antiDetection, when payload = 0.1, only [27]'s method maintains the antistatistical detection ability of traditional classical steganography (such as J-UNIWARD [34]) (data > 0.45); these data of other methods decrease significantly, even close to 0 [17]. Moreover, cover features extracted in these papers are based on preprocessed images rather than original ones. For Applicability, "no restriction" [14, 15] means that there is no requirement for the channel, while most methods require accurate channel details [12, 13, 27] or an approximate parameter range [8, 16, 17, 31]. All these show that nowadays when evaluating a method, it uses custom but not unified attributes. It hampers comparisons between methods. Thus, direct applying the traditional measurement attributes to robust steganography is not reasonable to some extent. Therefore, it is necessary to perfect the measurement attributes of robust steganography, determined by its practical application background.

4.1.2. Necessity of PURDA. We take the method in the paper [12] as an example to analyze the five attributes of PRUDA. We chose it because there are experiments on practical applications, and we think this is consistent with our idea to some extent. Our idea is trying to perfect the measurement attributes and make them more suitable for robust image steganography under the lossy channel. Thus, the robust steganography method is promoted to be closer to practice.

Two robust image steganography methods based on TCM (Transport Channel Matching), namely, JCRIS and JCRISBE, are introduced in the paper [12]. The notations used below follow those in that paper. The image size of the received image, Q.Size, and the channel compression factor, Q.qf , need to know. The TCM algorithm is used to compress images repeatedly. We denote the number of compressions as t_{TCM}. The JCRIS algorithm compresses the stego image repeatedly. This process is performed up to ϕ times. The JCRISBE algorithm encodes messages repeatedly. This process is performed up to t times.

10,000 images from the Bossbase-1.01 database are used to verify JCRISBE. Q.qf = 75, and attack quality factor QFc = 65, 72, 75, 78, 85. Payload = 0.01–0.1 bpnzAC.

(1) *Payload*. Two algorithms used 0.05–0.3 bpnzAC of the multiple compressed images as payload. For JCRIS, the cover image is compressed $\phi \times t_{\mathrm{TCM}}$ times, which means that the cover image has a small file size. For JCRISBE, the messages are encoded by BCH before embedded into the compressed image, which means there are many error correction codes in the embedded messages. The actual message embedding rate falls short of the 0.05–0.3 bpnzAC of the original cover image in both cases. Table 2 gives the actual embedding rate of our verification experiment ("all" means the results for all the QFc are the same). Obviously, the actual embedding rate is lower than the defined payload.

(2) *Robustness*. Two algorithms considered the message extraction error rate R_e. We verified R_e and R_r, and the results are shown in Table 2.

(3) *Ease of Use*. When the payload = 0.1 bpnzAC and the distortion function is J-UNIWARD, the available image in the Bossbase-1.01 database was about 55% and 99% for JCRIS and JCRISBE. It means that not all images can be used as cover images for these methods. The number of failed images we verified that cannot be as cover images is higher than that in the paper [12] (Table 2).

(4) *AntiDetection*. For JCRIS, the number of compression of the cover image is $\phi \times t_{\mathrm{TCM}}$, which means that the cover image's file size is relatively small and may be recognizable. The security of JCRIS was not evaluated in the paper [12]. For JCRISBE, in the statistical performance test, cover features are extracted from the TCM output compressed images and once-compressed images. Images used for extracting stego features are generated by embedding messages into these two kinds of images. When evaluating antistatistical detection performance, unlike the traditional steganography, images used for extracting cover features are no longer the original images but maybe processed images. The processing may differ in different methods, which brings obstacles to the security comparison between different methods.

(5) *Applicability*. This method requires a known received image size Q.Size and a known accurate channel compression factor Q.qf. Q.Size is predictable, which is verified in the next section. Q.qf may not be so easy to obtain. To verify the method's effectiveness when the channel's (attack) quality factor QFc is somewhat different from Q.qf, we did some experiments (Table 2). It shows that the method needs a Q.qf that equals QFc. Otherwise, the method is out of work.

4.2. Verification of Definition on Payload and Application. To verify the Payload's definition, we should verify whether the sender can predict the receiver's image size (scaling factor) and file size (compression factor). To verify the Application's definition, we should study if it is feasible to make some constraints on the channel, whether we can have harsh constraints. Our verification process is as follows.

We shot with the top seven mobile phones and three camera apps on 1,000 scenes. A total of $(13 + 10 + 12 + 10 + 11 + 11 + 9)$ resolution types $\times$ 1,000 scenes = 76,000 photos are captured, shared and compressed, separately. For space consideration, only the data of four mobile phones under one scene are listed here. Mobile phone brands came from Zhongguancun Online3 and listed in the first column of Table 3. Test phones were randomly selected from our laboratory classmates (the model and resolution are listed in the second column of Table 3). Three camera apps were selected combining Zhongguancun Online's recommendation4 and laboratory classmates' preferences (three camera apps are listed in the third column of Table 3). We used Huawei as PhoneA and others as PhoneB. When Huawei was used as PhoneB, Oppo was used as PhoneA temporarily.

We did the following test using PhoneA and PhoneB:

(i) Shoot with three camera apps using PhoneB, and captured images are called the Original Photo. Its two properties, image size and file size, are denoted as ImageSize_OP and FileSize_OP, respectively.

(ii) Post original photos in WeChat Moment using PhoneB.

(iii) Download photos from PhoneB's Moment in WeChat using PhoneA, and call them Moment Photo. Its two properties, image size and file size, are denoted as ImageSize_MP and FileSize_MP, respectively.

(iv) Resize the original photo's image size to ImageSize_MP, which is renamed ImageSize_CP. Then, perform JPEG compression to make the compressed photo as consistent as possible with FileSize_MP. The quality factor used is 98, and the compressed photo's file size is denoted as FileSize_CP.

The reason for choosing the compression quality factor 98 is that the FileSize_CP is the closest to FileSize_MP when the quality factor is 98 after our repeated tests. When the quality factor is slightly changed, the difference between FileSize_CP and FileSize_MP is greater than that of 98. The unit of FileSize_X (X is OP, MP, or CP) is in KB.

The comparison between ImageSize_OP and ImageSize_MP in Table 3 shows when the image size of the original image is greater than the resolution of the receiver's phone, the image will be scaled while preserving the ratio of the height-to-width. Otherwise, the image stays the same (the bold data). It indicates that the sender can predict the image size of the received image for a certain receiver. It has been used as a premise for existing robust steganography methods. Many methods resisting compression [12, 13, 16] are proposed on the presumption of resizing the cover image to the receiver's image size. The comparison between FileSize_MP and FileSize_CP in Table 3 shows that the FileSize_CP may be larger or smaller than FileSize_MP. It indicates that the original image can be compressed to an

Table 2: Verification on JCRISBE.

Value type	Q.qf	QFc	Payload (bpnzAC)									
			0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.10
R_e	75	65	0.5002	0.5007	0.5001	0.5001	0.4997	0.4999	0.5001	0.5002	0.5001	0.4998
		72	0.5003	0.5004	0.5003	0.4997	0.4998	0.5002	0.5002	0.4999	0.5001	0.5001
		75	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
		78	0.5001	0.4996	0.5006	0.4993	0.5001	0.4997	0.5000	0.5001	0.5000	0.4998
		85	0.5004	0.4995	0.5001	0.4998	0.5007	0.5000	0.5001	0.5002	0.5000	0.5001
R_r	75	65	0	0	0	0	0	0	0	0	0	0
		72	0	0	0	0	0	0	0	0	0	0
		75	1	1	1	1	1	1	1	1	1	1
		78	0	0	0	0	0	0	0	0	0	0
		85	0	0	0	0	0	0	0	0	0	0
Actual embedding rate	75	all	0.0085	0.0135	0.0199	0.0266	0.0332	0.0400	0.0467	0.0535	0.0604	0.0671
The number of failed images	75	all	678	4975	4294	3858	3490	3216	2996	2773	2602	2442

Table 3: Open channel transmission statistics on photos taken on the same scene with different camera apps on different phones.

Brand	Phone detail	Camera type	Original photo		Moment photo		Compressed photo	
			ImageSize_OP	FileSize_OP	ImageSize_MP	FileSize_MP	ImageSize_CP	FileSize_CP
Huawei	BLA-AL00 2160×1080	Built-in camera	3840×5120	3149	1080×1440	606	1080×1440	599
			2976×3968	1891	1080×1440	595	1080×1440	587
			2976×2976	1423	1080×1080	460	1080×1080	442
			2448×3264	1272	1080×1440	555	1080×1440	556
		BeautyCam App	**1984×3968**	1208	**1984×3968**	2890	**1984×3968**	1879
			1632×3264	819	**1632×3264**	1951	**1632×3264**	1256
			960×1920	981	**960×1920**	668	**960×1920**	651
			1080×1920	1103	**1080×1920**	773	**1080×1920**	731
			1080×1440	855	**1080×1440**	655	**1080×1440**	574
			1080×1080	647	**1080×1080**	485	**1080×1080**	434
		B126 App	**1080×1920**	911	**1080×1920**	674	**1080×1920**	572
			1080×1440	739	**1080×1440**	590	**1080×1440**	477
			1080×1080	588	**1080×1080**	477	**1080×1080**	385
Oppo	R15x 2340×1080	Built-in camera	3456×4608	3649	1080×1440	669	1080×1440	633
			3456×3456	2673	1080×1080	499	1080×1080	448
			2126×4608	2265	**2126×4608**	3122	**2126×4608**	2626
		BeautyCam App	**918×1920**	994	**918×1920**	719	**918×1920**	678
			1080×1920	1146	**1080×1920**	832	**1080×1920**	777
			1080×1440	912	**1080×1440**	684	**1080×1440**	622
			1080×1080	682	**1080×1080**	517	**1080×1080**	467
		B126 App	**1080×1920**	1436	**1080×1920**	952	**1080×1920**	1034
			1080×1440	1126	**1080×1440**	762	**1080×1440**	817
			1080×1080	814	**1080×1080**	544	**1080×1080**	590
Sumsung	SM-N9200 2560×1440	Built-in camera	5312×2988	3806	1080×1920	610	1080×1920	665
			3984×2988	2794	1080×1440	529	1080×1440	512
			2976×2976	2083	1080×1080	399	1080×1080	388
			3264×2448	1165	1080×1440	519	1080×1440	513
			3264×1836	1009	1080×1920	599	1080×1920	636
			2048×1152	461	1080×1920	600	1080×1920	623
		BeautyCam App	**1080×1920**	1210	**1080×1920**	756	**1080×1920**	810
			1080×1440	850	**1080×1440**	567	**1080×1440**	562
			1080×1080	650	**1080×1080**	428	**1080×1080**	429
		B126 App	**720×1280**	529	**720×1280**	348	**720×1280**	350
			768×1024	467	**768×1024**	327	**768×1024**	313
			768×768	360	**768×768**	249	**768×768**	242

Table 3: Continued.

Brand	Phone detail	Camera type	Original photo		Moment photo		Compressed photo	
			ImageSize_OP	FileSize_OP	ImageSize_MP	FileSize_MP	ImageSize_CP	FileSize_CP
IPhone	XR 1792 × 828	Built-in camera	4032 × 3024	3931	1080 × 1440	554	1080 × 1440	489
			3024 × 3024	3448	1080 × 1080	465	1080 × 1080	429
		BeautyCam App	1774 × 3840	7468	1080 × 2338	937	1080 × 2338	1090
			2160 × 3840	7955	1080 × 1920	748	1080 × 1920	778
			2880 × 3840	11590	1080 × 1440	687	1080 × 1440	636
			2160 × 2160	5241	1080 × 1080	564	1080 × 1080	510
		B126 App	**486 × 1052**	220	**486 × 1052**	253	**486 × 1052**	250
			720 × 1280	426	**720 × 1280**	490	**720 × 1280**	495
			828 × 1104	373	**828 × 1104**	458	**828 × 1104**	428
			828 × 828	298	**828 × 828**	358	**828 × 828**	336

image the file size of which is approximately equal to but not the exact size. Therefore, a proposed method can constrain the channel, but it must be a mild constraint rather than a harsh one.

4.3. Verification of Definition on AntiDetection. We have given the antiDetection two meanings. The image is unrecognizable, such as the image's size is not suspect; the image is indistinguishable in the image ocean. The first meaning is given because we want to keep the image noteless. The second meaning is given because we find the role of the existing statistical detection in open lossy channels (the application background of robust image steganography) is reduced. This section verifies the antiDetection's definition from two aspects: image composition in public lossy channels and the role of statistical detection in open lossy channels.

4.3.1. Image Composition in Open Lossy Channels. The social platform is an important application background of robust image steganography. We focus on the proportion of processed images on the social platform. From a common user's perspective, there are two types of images on social platforms: those captured by the user and those downloaded from other sources. Among downloaded images, there are also two types: captured photos and produced images. Thus, there are two types of images on social platforms: photos taken and images produced. The latter are processed images undoubtedly. Here, we focus on the former: besides the platform's processing such as compression and scaling, how many images are processed when sharing? To this end, we developed the following questionnaire (six questions (Q1–Q6) and corresponding options (O1–O6)):

Questionnaire on Camera and Photo Processing

Q1: the degree of concern with the camera app when buying a phone.

O1: 5 scores. (1 means not concerned at all; 5 means extremely concerned.)

Q2: your greatest concern in a camera application.

O2: A, resolution; B, number of cameras; C, camera functions (such as various image operations); D, others.

Q3: the proportion of processed images to all posted images.

O3: 5 scores. (1 means never processed at all, and 5 means every image is processed.)

Q4: the most commonly used operation.

O4: A, beautify/filter/blur; B, enhance (contrast, brightness, sharpen, etc.); C, adding (stickers, doodles, watermarks, etc.); D, others.

Q5: your age.

O5: A, 1–17; B, 18–25; C, 26–40; D, 40–55; E, over 55.

Q6: your gender.

O6: A, male; B, female.

A total of 1,917 questionnaires were collected. 641 participants were female, and the rest were male; 76.98% were 18–25 years old, and 15.24% were 26–55 years old. The statistical results are shown in Figure 5.

The blue bars in Figure 5 show all the returned questionnaires' statistical results. Figures 5(a)–5(d) are corresponding to questions 1–4 in the questionnaire, respectively. It can be seen that when buying a phone, 60.69% of people pay attention to the camera app (≥3); of the concerns about camera applications, half focus on resolution, and nearly 40% focus on image processing. Nearly half of the participants always processed their photos before posting on social platforms (≥3). In image processing, nearly half prefer beauty/filter/blur processing, 23% prefer enhancement processing, and 24% like to add extra doodles to their photos.

In our cognition, females prefer cameras and image processing more than males. To avoid inaccurate statistical results caused by gender, we chose 641 males as the comparison to ensure the ratio of males to females is 1 : 1. Among them, 75.02% were 18–25 years old, and 16.89% were 26–55 years old. The statistical results are shown in the red bars in Figure 5. It shows that on social networks, males and females showed similar preferences for image processing.

The statistical results show that nearly half of the photos transmitted through the open lossy channel (the application background of robust image steganography) have been processed. This means that the processed images transmitted through open lossy channels account for far more than half.

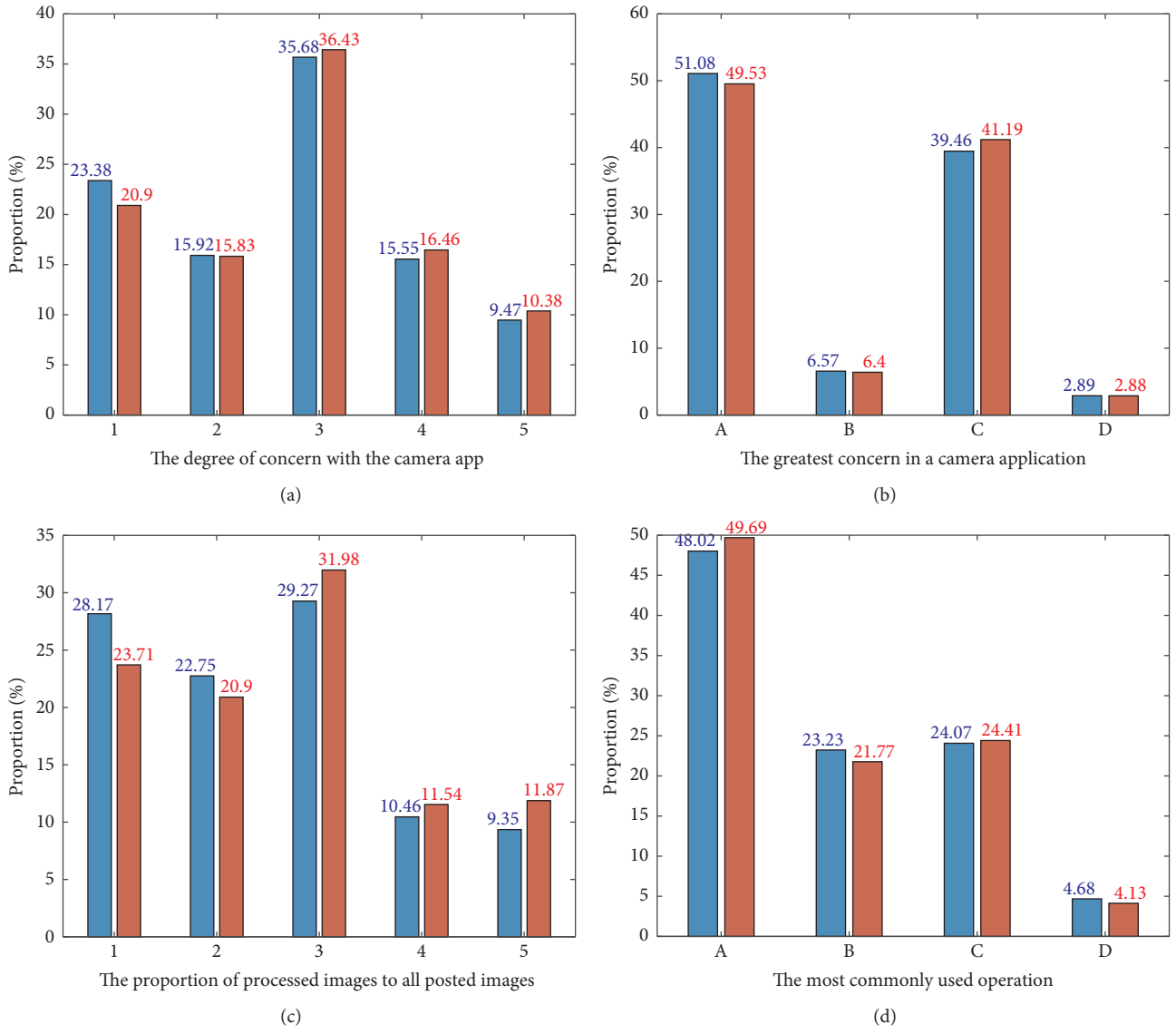

Figure 5: Statistical results of the questionnaire.

4.3.2. The Role of Statistical Detection in Open Lossy Channels. To study the role of statistical detection in open lossy channels, we verified the antistatistical detection performance in variously processed images. 10,000 gray images from the Bossbase-1.01 database and 886 color images from the UCID database were utilized. JPEG compression is first performed to generate JPEG images. The quality factor is 75 for Bossbase-1.01 database and 85 for the UCID database. Five operations, including mean filtering, gaussian filtering, contrast adjustment, image sharpening, and edge enhancement, were performed. Stego images are generated utilizing "J-UNIWARD + STC (Syndrome-Trellis Codes)." Payload = 0.1–0.3 bpnzAC. DCTR feature was utilized to extract features of cover and stego images. We randomly selected 1/2 for classifier training in each group and the remaining 1/2 for testing to get the average detection error rate E_{OOB}.

Table 4 is the experimental results of antistatistical detection. The first column refers to the types of cover images included in the experiment. The abbreviations are in parentheses. The corresponding stego images are generated by embedding messages in these cover images with different embedding rates. For example, "Contrast + Edge + Sharpen" means that the cover images contain these three types of images, each accounting for 1/3. The stego images are generated by embedding messages into these cover images. The second to the fourth column and the fifth to the seventh column are the detection error rates of two image databases under three different embedding rates of 0.1–0.3 bpnzAC.

Table 4 shows that images with edge enhancement or sharpening are suitable as cover images and have good antistatistical detection performance. In contrast, images with mean filtering and Gaussian filtering are the opposite. When cover images contain multiple types of images, the

Table 4: The effect of the statistical detection techniques in processed images.

Image type	E_{OOB} of different databases under different payloads					
	Bossbase-1.01			UCID		
	0.1	0.2	0.3	0.1	0.2	0.3
Original image (Original)	0.4266	0.3203	0.2143	0.4825	0.4419	0.3795
Mean filtering (Mean)	0.2845	0.1136	0.0339	0.3954	0.2494	0.1267
Gaussian filtering (Guassian)	0.4038	0.2721	0.1532	0.4578	0.3769	0.2828
Contrast adjustment (Contrast)	0.4385	0.3553	0.2771	0.4904	0.4589	0.4153
Edge enhancement (Edge)	0.4866	0.4605	0.4224	0.4951	0.4808	0.4529
Image sharpening (Sharpen)	0.493	0.4751	0.4443	0.4957	0.4921	0.4728
Original + Mean	0.3786	0.2428	0.1447	0.449	0.3564	0.2788
Original + Guassian	0.4234	0.3141	0.2133	0.4748	0.42	0.3533
Original + Contrast	0.4539	0.3838	0.3036	0.4931	0.4679	0.4256
Original + Edge	0.4646	0.4146	0.3555	0.4963	0.4771	0.4482
Original + Sharpen	0.4731	0.4283	0.3792	0.495	0.479	0.4579
Mean + Guassian	0.3706	0.2253	0.1213	0.4297	0.3271	0.2335
Contrast + Edge + Sharpen	0.4866	0.4551	0.4169	0.5016	0.4887	0.466
Original + Contrast + Edge + Sharpen	0.475	0.4357	0.3879	0.4962	0.4924	0.4591
Original + Mean + Guassian + Contrast + Edge + Sharpen	0.4519	0.3884	0.3252	0.4868	0.4514	0.4107

antistatistical detection performance is an approximate average value of that of them. It means that when an image is in an ocean composed of various types of images, the antistatistical detection performance increases, and the role of statistical detection may be weakened. The practical application environment of robust image steganography is open lossy channels, and there are plenty of processed images in open lossy channels. Considering this, it may be more meaningful to assign the antidetection as the indistinguishability between the stego images and other processed images.

5. Discussion and Conclusion

With the development and maturity of technologies, cloud services provide more and more convenience for people. This convenience comes with security issues. For privacy or data ownership reasons, users do not want the outsourced data to be seen by third parties or performed unexpected operations. For this reason, the outsourced data are often encrypted or hidden in other carriers. The recently popular used cryptographic technique is homomorphism encryption. In addition, the blockchain has been widely used to verify the integrity of outsourcing data in recent years. These methods encrypt the outsourced data into garbled code to hide the contents. However, garbled code can be a noticeable feature that catches an attacker's eyes. Steganography, masking the content of outsourced data and its existence simultaneously, is also effective schemes used to maintain the security of outsourced data in recent years. Because the cloud is an open lossy environment, which is different from the lossless hypothesis of traditional steganography, robust steganography came into being. The open lossy environment diverts the algorithm's focus and leads that the existing measurement attributes inherited from traditional steganography are no longer suitable for robust image steganography.

Affected by the lossy environment, many default parameters in traditional image steganography are no longer default in robust image steganography. Considering this, "perfecting the default parameters" is proposed. A measurement attribute set that is suitable for robust image steganography is proposed considering practical application background. We call it PRUDA. PRUDA perfects the default parameters of traditional steganography. It improves the existing measurement attributes from five perspectives of Payload, Robustness, Ease of Use, antiDetection, and Applicability. The rationality of measurement needs to be tested by practice. After all, it is a truth universally acknowledged that genuine knowledge comes from practice. For this reason, this paper verified PRUDA utilizing a large number of practice experiments. First, the existing robust image steganography methods are presented and discussed from five aspects, which shows some deficiencies in experimental verification's uniformity, and perfecting the existing measurement is needed. Then, the scaling and compression experiments are done on WeChat, one of China's most popular social media. Top 7 mobile phone brands and three camera apps are used. Results show that the definition of Payload and Application is reasonable. Finally, the questionnaire of photo processing and antistatistical detection performance of processed images shows that the definition of antiDetection is reasonable. Therefore, the rationality of PRUDA is verified.

Parts of the attributes in PRUDA have been used in the measurement of existing robust steganography methods. However, limited by the traditional measurement attributes, the robust steganography method is evaluated as incomprehensive and inconsistent. In this paper, the attribute set PRUDA unifies measurement attributes, hoping to break down the measurement barriers between methods. Worthy of note, this paper does not intend to challenge the existing measurement standard. It is valuable for traditional steganography methods. Nor does this paper intend to challenge any existing robust image steganography approach. They

have strongly promoted steganography field development. Our goal is to show the observation that the existing measurement standard is restricting the robust image steganography to some extent. This paper only draws the hook out. Further improvement on measurement is likely possible to promote robust image steganography closer to reality faster by doing the next work. (1) The definition of antiDetection and Applicability needs to be more specific and more operable. (2) Simple and effective methods to judge the unidentifiability of stego images and processed images are to be proposed.

Data Availability

The proposed scheme data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (no. U1736214, U1804263, and 62172435), the National Science Foundation for Young Scientists of China (no. 62002387), and Zhongyuan Science and Technology Innovation Leading Talent Project of China (no. 214200510019).

References

[1] P. Yang, X. Gui, J. An, and F. Tian, "An efficient secret key homomorphic encryption used in image processing service," *Security and Communication Networks*, vol. 2017, Article ID 7695751, 11 pages, 2017.

[2] Y. Liu, Y. Luo, Y. Zhu, Y. Liu, and X. Li, "Secure multi-label data classification in cloud by additionally homomorphic encryption," *Information Sciences*, vol. 468, pp. 89–102, 2018.

[3] N. Jia, S. Fu, and M. Xu, "Privacy-preserving blockchain-based nonlinear SVM classifier training for social networks," *Security and Communication Networks*, vol. 2020, Article ID 8872853, 10 pages, 2020.

[4] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: a panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[5] M. Sajjad, K. Muhammad, S. W. Baik et al., "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3519–3536, 2017.

[6] T. Xiang, J. Hu, and J. Sun, "Outsourcing chaotic selective image encryption to the cloud with steganography," *Digital Signal Processing*, vol. 43, pp. 28–37, 2015.

[7] M. Meeker, "Internet trends 2019," in *Proceedings of the Code 2019*, Francisco, CA, USA, June 2019.

[8] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A framework of adaptive steganography resisting jpeg compression and detection," *Security and Communication Networks*, vol. 9, no. 15, pp. 2957–2971, 2016.

[9] B. Li, M. Wang, J. Huang, and X. Li, "A new cost functions for spatial image steganography," in *Proceedings of IEEE International Conference on Image Processing*, pp. 4206–4210, Paris, France, October 2014.

[10] L. Xin, G. Chen, and J. Yin, "Content-adaptive steganalysis for color images," *Security and Communication Networks*, vol. 9, no. 18, pp. 5756–5763, 2017.

[11] T. Denemark and J. Fridrich, "Model based steganography with precover," *Electronic Imaging*, vol. 7, no. 1, pp. 56–66, 2017.

[12] Z. Zhao, Q. Guan, H. Zhang, and X. Zhao, "Improving the robustness of adaptive steganographic algorithms based on transport channel matching," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1843–1856, 2018.

[13] J. Tao, S. Li, X. Zhang, and Z. Wang, "Towards robust image steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 594–600, 2018.

[14] W. Lu, J. Zhang, X. Zhao, W. Zhang, and J. Huang, "Secure robust jpeg steganography based on autoencoder with adaptive," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, pp. 1–14, 2020.

[15] F. Li, K. Wu, C. Qin, and J. Lei, "Anti-compression jpeg steganography over repetitive compression networks," *Signal Processing*, vol. 170, Article ID 107454, 2020.

[16] X. Yu, K. Chen, Y. Wang, W. Li, W. Zhang, and N. Yu, "Robust adaptive steganography based on generalized dither modulation and expanded embedding domain," *Signal Processing*, vol. 168, Article ID 107343, 2020.

[17] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Multiple robustness enhancements for image adaptive steganography in lossy channels," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2750–2764, 2020.

[18] J. Fridrich, *Steganography in Digital media: Principles, Algorithms, and Applications*, Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[19] J. Fridrich, P. Lisonk, and D. Soukal, "On steganographic embedding efficiency," in *Proceedings of the 8th International Workshop on Information Hiding*, pp. 282–296, Alexandria, VA, USA, July 2006.

[20] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proceedings of the 3rd International Workshop on Information Hiding*, pp. 61–76, Dresden, Germany, September 1999.

[21] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of lsb steganography in color and grayscale images," in *Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges*, pp. 27–30, Ottawa, Canada, October 2001.

[22] S. Baluja, "Hiding images in plain sight: deep steganography," in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 2066–2076, Long Beach, CA, USA, December 2017.

[23] G. J. Simmons, "The prisoners problem and the subliminal channel," *Advances in Cryptology*, pp. 51–67, Springer, Berlin, Germany, 1983.

[24] Z. Yang, Y. Hu, Y. Huang, and Y. Zhang, "Behavioral security in covert communication systems," in *Proceedings of International Workshop on Digital Watermarking*, pp. 377–392, Xiamen, China, October 2019.

[25] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proceedings of IEEE*

Workshop on Information Forensic and Security, pp. 234–239, Tenerife, Spain, December 2012.

[26] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2015.

[27] Y. Zhang, X. Luo, J. Wang, C. Yang, and F. Liu, "A robust image steganography method resistant to scaling and detection," *Journal of Internet Technology*, vol. 19, no. 2, pp. 607–618, 2018.

[28] Y. Zhang, X. Luo, X. Zhu, Z. Li, and A. G. Bors, "Enhancing reliability and efficiency for real-time robust adaptive steganography using cyclic redundancy check codes," *Journal of Real-Time Image Processing*, vol. 17, no. 1, pp. 115–123, 2020.

[29] Y. Zhang, D. Ye, J. Gan, Z. Li, and Q. Cheng, "Image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection," *Computers, Materials & Continua*, vol. 56, no. 1, pp. 151–167, 2018.

[30] Y. Zhang, X. Luo, Y. Guo, C. Qin, and F. Liu, "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection," *IEEE Access*, vol. 7, Article ID 24282, 2019.

[31] Z. Bao, X. Luo, Y. Zhang, C. Yang, and F. Liu, "A robust image steganography on resisting jpeg compression with no side information," *IETE Technical Review*, vol. 35, no. 1, pp. 4–13, 2018.

[32] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215–224, 2010.

[33] V. Holub and J. Fridrich, "Low-complexity features for JPEG steganalysis using u," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219–228, 2015.

[34] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–13, 2014.