IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 24, 2019, accepted March 14, 2019, date of publication April 2, 2019, date of current version May 3, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2908924

Privacy-Preserving Reversible Information Hiding Based on Arithmetic of Quadratic Residues

CHING-CHUN CHANG[1], CHANG-TSUN LI[2], AND KAIMENG CHEN[3]
[1]Department of Computer Science, University of Warwick, Coventry CV4 7AL, U.K.
[2]School of Information Technology, Deakin University, Geelong, VIC 3216, Australia
[3]Computer Engineering College, Jimei University, Xiamen, 361021, China

Corresponding author: Kaimeng Chen (chenkaimeng@jmu.edu.cn)

This work was supported in part by the Marie Skłodowska-Curie actions of the EU Horizon 2020 Programme through the project entitled "Computer Vision Enabled Multimedia Forensics and People Identification" (Acronym: IDENTITY) under Project 690907, and in part by the National Science Foundation of Fujian Province of China under Grant 2017J05104.

ABSTRACT The phenomenal advances of cloud computing technology have given rise to the research area of privacy-preserving signal processing, which aims to preserve information privacy even when the signals are processed in an insecure environment. Privacy-preserving information hiding is a multidisciplinary study that has opened up a great deal of intriguing real-life applications, such as data exfiltration prevention, data origin authentication, and electronic data management. Information hiding is a practice of embedding intended messages into carrier signals through imperceptible alterations. In view of some content-sensitive scenarios, however, the ability to preserve perfect copies of signals is of crucial importance, for instance, considering the inadequate robustness of recent artificial intelligence-aided automated systems against noise perturbations. Reversibility of information hiding systems is a valuable property that permits recovery of original carrier signals if desired. In this paper, we propose a novel privacy-preserving reversible information hiding scheme inspired by the mathematical concept of quadratic residues. A quadratic residue has four (not necessarily distinct) square roots, which enables payloads to be encoded in a dynamic fashion. Furthermore, a predictive model based upon the projection theorem is devised to assist carrier signal recovery. The experimental results showed significant improvements over the state-of-the-art methods with regard to capacity, fidelity, and reversibility.

INDEX TERMS Cloud computing, data privacy, information hiding, number theory, symmetric ciphers.

I. INTRODUCTION

The past decades have witnessed the worldwide popularisation of social networks and the phenomenal prevalence of public cloud services [1]. The seemingly unlimited storage space and computational capacity offered by the clouds have opened up opportunities for numerous practical applications and have appealed to individuals and businesses to entrust an increasing amount of data to the environments out of the control of the data owner. The legality and morality of the use of such personal data by third parties came into question. In many current privacy policies, the sharing of personal information with law enforcement agencies without a warrant is permitted. As a more serious concern, there are non-negligible risks of intentional or unintentional data leakage to untrustworthy third parties [2]–[4].

Privacy-preserving signal processing is an emergent discipline, born as a possible solution addressing privacy concerns in cloud computing [5]–[7]. The aim is to allow the processing of data and in the meanwhile preserve information privacy even when it is exposed in untrusted environments. The realisation of this aim is often achieved through cooperation with cryptographic schemes, particularly the *homomorphic encryption* schemes which allow computations to be performed in the encrypted domain [8]–[15]. Accordingly, this research area is also referred to as *signal processing in the encrypted domain* in most cases. Although privacy-preserving signal processing is built upon deep theoretical grounds of cryptography, the research outcomes from the applied aspects are abundant. Its applications include not only the protection of multimedia contents in cloud

The associate editor coordinating the review of this manuscript and approving it for publication was Irene Amerini.

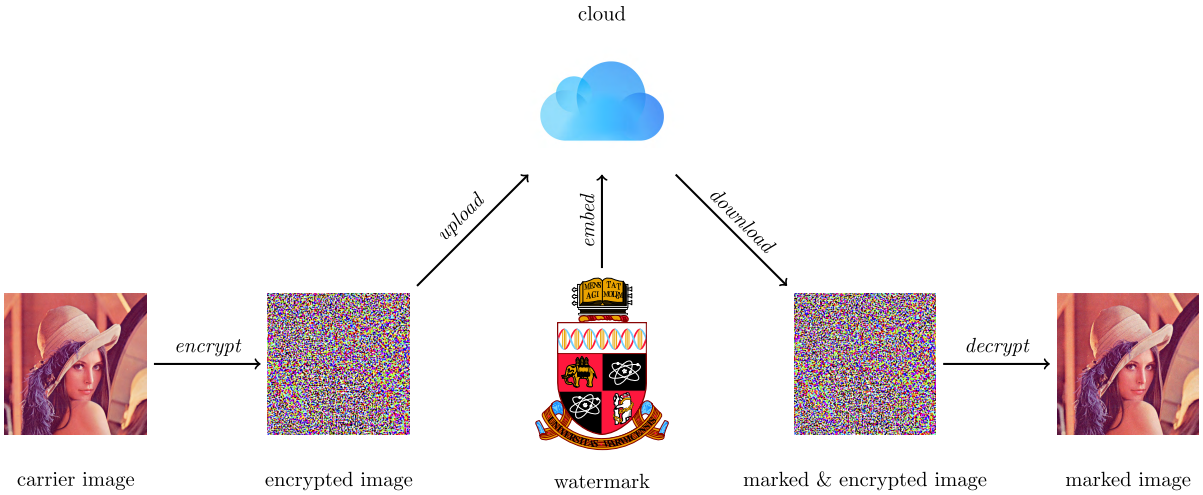


FIGURE 1. Privacy-preserving information hiding via cloud computing.

computing systems but also the safety of privacy-sensitive information such as biometric data in access control systems, criminal databases in forensic investigation systems, medical records in Internet-of-Things (IoT) healthcare systems, and video footages in surveillance security systems.

Privacy-preserving information hiding is regarded as one of the most promising and intriguing subdisciplines of privacy-preserving signal processing. It is also a multidisciplinary study combining cryptography, steganography, watermarking, signal processing, statistical analysis, *etc*. It deals with the problem of hiding information into encrypted carrier data and can be applied to fulfil many real-life requests such as data exfiltration prevention, data origin authentication, and electronic data management. It can also be of a substitution strategy when an information hiding algorithm is registered as a proprietary property and thus the access to the algorithm can only be made through authorised third parties. An overview of privacy-preserving information hiding via cloud computing is illustrated in Fig. 1.

Information hiding is a general term encompassing a wide range of research problems including steganography and watermarking. In general, information hiding is defined as the practice of imperceptibly altering a carrier signal to embed a message. The challenge of information hiding in the encrypted domain is a rather difficult one for the reason that when being protected by encryption, the carrier signals become unable to be observed and analysed. As a result of this, the exploitation of *data redundancy* becomes unfeasible, which prohibits conventional methods of information hiding from being deployed. In addition to this, if a cryptosystem is perfectly secure, it is theoretically not possible to foresee how the change in the encrypted domain would result in the change to carrier signals. The true consequences will only be known after decryption; in other words, whether the impact of information hiding is perceptible or not becomes hardly manageable. The main issues concerning privacy-preserving information hiding can be summarised as follows:

- *Cryptographic algorithms:* The choice of cryptographic algorithms forms the basis of a privacy-preserving information hiding schemes. On the one hand, modern public-key cryptosystems, particularly those possess homomorphic properties, are powerful in terms of the ability to perform mathematical operations in the encrypted domain, and malleable in terms of the feasibility to transform a ciphertext into another ciphertext which decrypts to the same plaintext, and secure due to the inherent advantage of circumventing the risks of key exchange. On the other hand, traditional symmetric-key ciphers are comparatively easier to implement since they are usually of low computational complexity and do not have the drawbacks commonly seen in homomorphic cryptosystems such as ciphertext expansion.
- *Data structures:* The data structure in which carrier signals are organised, managed, and stored needs to be taken into account. It is often that cryptographic algorithms cannot be directly applied to multimedia data since many of those algorithms were originally proposed to deal with large integers while practical implementations for multimedia data were not considered or standardised. There are a variety of ways and options to format multimedia data structures for the purposes of encryption and operations that follow. Some structures may, for instance, partition carrier signals into successive blocks based upon the spatial or temporal positions, and some may divide signals according to semantic significance. Some arrangements may involve the padding of additional bits for security purposes or for accommodating privacy-preserving information hiding schemes.
- *Information hiding schemes:* The designs of privacy-preserving information hiding schemes are application-oriented and can be characterised by various features and qualities. Some of the schemes allow the extraction of messages in the encrypted domain and yet the messages

will be lost as the content is decrypted. This type of schemes may be employed to manage the encrypted files stored online or to monitor the transfer and exportation of encrypted documents. Some of the schemes preserve the embedded information so that the protection furnished by information hiding lasts even after decryption. This type of schemes can be used to outsource the task of information hiding to authorised third parties, in the sense that the returned result is equivalent to that produced from a conventional information hiding algorithm. It is also possible to design schemes with a mixture of properties.

- *Content-adaptive predictors:* The decoding process of some privacy-preserving information hiding schemes involves the use of content-adaptive predictors, especially in the schemes that requires the original carrier signals. The precision of content-adaptive predictors could have a crucial effect on the ability and quality of recovery. The designs of predictors are often based upon sophisticated theories and advanced techniques of statistics and signal processing.

In this paper, we present a novel privacy-preserving reversible information hiding scheme to operate encrypted data based upon the theory of quadratic residue [16]. The proposed scheme adopts secure *stream cipher* to encipher the carrier image and utilises the *one-to-many relationship* between a quadratic residue and its square roots to encode payloads in a dynamic fashion. A content-adaptive predictive model derived from the projection theorem is devised to assist the recovery of carrier signals to a perfect state. The design of cryptographic and watermarking algorithms follows *Shannon's maxim*: 'the enemy knows the system' [17]; in other words, all the detailed construction of algorithms ought to be publicly known and only the keys for decrypting the carrier signal and decoding the watermark remain secret. Experimental results showed significant improvements over the state-of-the-art schemes with respect to three principle factors: capacity, fidelity, and reversibility.

The remainder of this paper is organised as follows. Section II introduces the research background of reversible information hiding with interesting insight into real-world applications. Section III aims to provide a constructive literature review of the developments and advancements in privacy-preserving reversible information hiding. Section IV discusses foundational elements of the proposed scheme. Section V presents detailed constructions of the proposed scheme. Section VI evaluates the scheme performance in comparison with the state-of-the-art algorithms in regard to capacity, fidelity, and reversibility. Section VII concludes our study and outlines the directions for future research.

II. REVERSIBLE INFORMATION HIDING

In forensic science, one of the most critical issues would be the authentication of digital evidence against illegitimate manipulations [18]. *Digital signature* schemes serve as one of the most effective solutions towards message authentication [19]. Typically, a digital signature is the encryption of a *hash value*, or a digest of a file, in a sense that:

- It cannot be forged as long as the private key (for encryption) remains secure.
- It is verifiable as long as the public key (for decryption) is available.

In 1993, Friedman proposed a trustworthy digital camera that contains a microprocessor for generating digital signatures when photos are taken [20]. The private key only known to the camera manufacturer is programmed into the microprocessor, whereas the public key is stored as image files' metadata and also engraved on the camera body. To verify the image file in question, the verification software decrypts the stored signature with the public key to obtain the hash value, and compares it with the hash value produced from the image in question. The verification is passed if both values match; otherwise, the image fails to be authenticated and is judged as tampered.

This construction, however, requires additional storage space for signatures and furthermore has risks of data loss and mismanagement during storage, transmission, or format transformation. Although watermarking can be considered as a potential solution addressing the problem of mislaying digital signatures as well as other auxiliary information, the modifications by the act of watermarking itself may violate the initial objective of integrity protection. In some cases, these non-malicious modifications and imperceptible distortions could be admissible and tolerable. In some sensitive scenarios, however, such alterations would be strictly forbidden, especially in the cases such as military reconnaissance or medical diagnosis. It might be argued that the noise introduced is too faint to be a possible cause of misinterpretation of medical images in a malpractice suit. Yet, this argument may not be persuasive in a courtroom.

Another critical concern is accompanied by the recent development of artificial intelligence aided automated systems, such as autonomous vehicle systems and autonomous diagnostic systems. It is evident that many current deep neural networks would not able to sustain some *adversarial perturbations* in a sense that some imperceptible noise would chance to or intend to mislead the model in a wrong or even chosen direction, as a demonstration shown in Fig. 2 provided by Goodfellow *et al.* [21]. It is also of a practical possibility that a few distorted samples of data collected and used in the training process would poison and eventually compromise the whole model. Hence, we conclude that the ability to preserve *perfect copies* of original images is not only an academic pursuit but also of great significance in real-life applications.

In order to fulfil the requirement of preserving the original carrier signals, the notion of *reversible information hiding* was introduced and has continued to advance over the last two decades [22]. Reversible information hiding is a special class of information hiding techniques that permits the restoration of original carrier signals once the embedded messages are extracted. To the best of our knowledge, the very

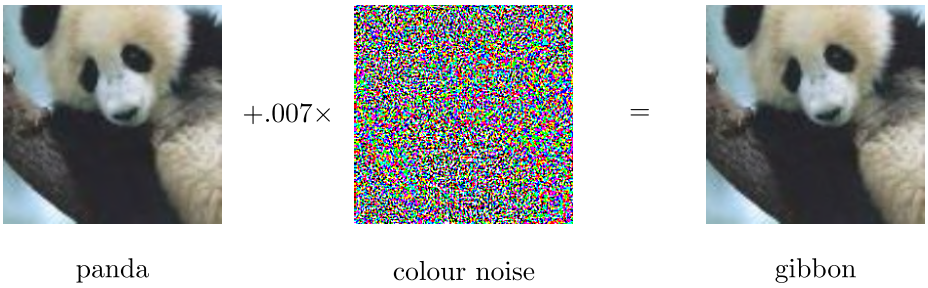


FIGURE 2. A demonstration of adversarial perturbations. By adding an imperceptible colour noise to an image 'panda', GoogLeNet mistakenly categorised it as a 'gibbon' with 99.3% confidence.

first reversible information hiding algorithm was invented by Barton and issued as a US patent in 1997 [23]. The invention relates to an information hiding method and apparatus for verifying whether the digital data has been modified from its intended form and allowed restoration of data to its original state if desired. Relevant literature suggested that reversible information hiding schemes are favourable for many authentication applications, and thus we would argue that reversible information hiding is more associated with watermarking, instead of steganography, from the application aspect [24]–[29]. Accordingly, we may also refer to reversible information hiding as *reversible watermarking* and message payloads as *watermarks*.

III. LITERATURE REVIEW

The rapid advancement of cloud computing technology has intrigued researchers to explore the possibility of outsourcing the task of reversible watermarking to cloud service providers without compromising the privacy of carrier signals. We have witnessed a dramatic growth in the research of privacy-preserving reversible watermarking over the past few years and a majority of works focused on a particular types of carrier signals, namely digital images. In the rest of this section, we review some of the most representative works in this research area.

A. SYMMETRIC-KEY CRYPTOSYSTEMS

One of the very first reversible information hiding scheme for encrypted images can be traced back to the work by Puech *et al.* who proposed to use block ciphers to encrypt images and embed one bit of information into a block of 4×4 pixels by substituting a significant bit of a selected carrier pixel with the intended bit of payloads [30]. Since encoding was realised through *bit replacement*, the watermark can be decoded directly in the ciphertext domain. Removing the distortion caused by watermark encoding is equivalent to unraveling whether the bit of the selected pixel is originally a zero or an one. This issue was resolved by analysing the *local standard deviation* of the decrypted image block in the two possible cases. As follow-up studies, this idea was refined by an adaptive local entropy analysis [31] and a most significant bit (MSB) predictor [32]. This research line, however, has an inherent weakness in the fidelity of marked images due to alterations of significant bits of pixels.

One of the most oft-cited works is Zhang's method, which exploits the three least significant bits (LSB) of a block of encrypted pixels to encode one bit of information and recovers the original pixels by a *fluctuation function* that captures spatial correlations in natural images [33]. This design paradigm effectively resolved the issue of low fidelity owing to the fact that only some imperceptible signals are distorted. It method was improved by many follow-up studies including:

- A *side-match* mechanism that involves recovered blocks in the smoothness estimation process [34].
- An evaluation function for estimating pixel distributions of a given block through analysing the *absolute mean difference* of a given pixel and its adjacent pixels [35].
- A support vector machine (SVM) which handles the problem of image recovery as a *binary classification problem* [36].
- An *elaborate selection* of changeable pixels, instead of altering a whole block of pixels, in order to enhance the visual quality of marked images and a content-based adaptive judging function in light of the fact that pixel fluctuations are minimal along the *isophote direction* [37].
- A *double-round embedding* approach based upon cyclic-shifting and data-swapping for encoding more information [38].

This class of schemes encodes messages mostly through *bit flipping* and therefore the message decoding process was accompanied by the image recovery process in the plaintext domain. In view of this, these schemes are often referred to as *joint schemes*. Message detection in the plaintext domain might, however, limit some potential applications such as encrypted data management that utilises the embedded annotations to supervise and administrate the storage and transfer of encrypted files, and even to protect files against cybersecurity breaches.

In contrast to the class of joint schemes, the notion of *separable schemes* emphasises the separability of message extraction process and signal recovery process. In response to this required property, Zhang proposed to compress encrypted images and append additional messages to the vacated space [39]. The possibility of compressing encrypted data was investigated by Johnson *et al.* ahead of the invention

of privacy-preserving reversible information hiding [40], and has undergone profound development over years [41]–[45]. Some improvements were made over this pioneering compression-based scheme, including:

- A *distributed source coding* technique using low-density parity-check (LDPC) code for approaching an optimal compression rate [46].
- A *three-round embedding* strategy for increasing the embedding rate and a *progressive recovery* mechanism that exploits previously recovered pixels in the future round of recovery [47].
- An extension to deal with encrypted *JPEG bitstreams* [48].

Instead of establishing separability upon distributed source coding techniques, Chang and Li proposed a *lexicographic permutation* approach that encodes a dynamic number of bits by permuting the encrypted symbols into a particular pattern in accordance to the given set of bits and permits the bits to be decodable in the ciphertext domain [49]. In general, joint schemes mostly realise the encoding function by bit flipping, whereas separable schemes often construct the encoding function by bit replacement. This conceptual framework was pointed out in [50] and refined in [51].

In literature, the above schemes are often referred to as the class of *vacating room after encryption* (VRAE) in contrast to that of *reserving room before encryption* (RRBE), which is characterised by some *compulsory preprocessing* steps contributing to a comparatively enormous payload capacity. Ma *et al.* utilised *self-embedding* approach to embed some insignificant bits of a part of the image into another part of the image in a reversible manner so that the reserved space can be used to carry additional information even after encryption [52]. The improvements in this line of research mainly focused on more efficient representations of images, including:

- A *sparse coding* technique that encodes images into sparse representations via a pre-trained *K-means singular value decomposition* (K-SVD) based dictionary so that the original images can be reconstructed in presence of the sparse codes and residuals [53].
- An *extended run length code* that efficiently compresses the most significant bit (MSB) plane [54].

However, this class of schemes would have rather restricted range of applications taking into account the fact that an individual may have too limited computational resource to execute preprocessing algorithms in the first place. In other words, it may constitute a violation of the chief purpose of accessing cloud computing services, in spite of the fact that it could be of good value in some other circumstances and applications.

B. ASYMMETRIC-KEY CRYPTOSYSTEMS

Schemes based upon public-key cryptography involve relatively high computational complexity and often induce non-negligible *ciphertext expansion* problem. It is especially the case when attempting to operate the encryption process pixel by pixel [55]–[58], due to the fact that public-key cryptography usually involves modular arithmetic with large numbers and thus it would not be efficient to project a small pixel space onto a large ciphertext space. To some extent, schemes adopting ill-constructed encryption procedures would be of limited practical value considering that the expanded file size would be far greater than the payload size in most cases, excluding the standard and inevitable expansion inheres in the given cryptosystem. Furthermore, this class of schemes usually cannot produce a marked plaintext since the payloads are generally embedded into the *expanded space* offered by encryption, which evaporates along with decryption. In other words, an intended watermark will be filtered out after decipherment and thus from that point onwards the carrier data will no longer be under the protection of the watermark. Despite the fact that schemes of this type could fit in with some other potential applications, they would not be applicable when the aim is simply to outsource the task of watermarking to a cloud service provider with expectation of receiving a marked content.

Reserving room before encryption (RRBE) paradigm has been adopted by schemes compatible with asymmetric-key cryptosystems and has been realised by

- A pre-computation of *reversible integer transform* and a pre-recording of overflow/underflow locations enabling the *different expansion* techniques to be operated in the encrypted domain [59].
- A pre-shrinking of image histogram to reconcile the statistical distribution of carrier signals with the subsequent *histogram-shifting* encoding in the encrypted domain [60].
- A *self-embedding* technique to reserve space and an encoding technique based upon *mirroring ciphertext group* strategy to prevent over-saturation of pixels in the plaintext domain [61].

Vacating room after encryption (VRAE) paradigm is a preferable solution towards privacy-preserving reversible information hiding in view of the fact that it can not only encipher a bit-stream of sufficient length, instead a single element of signals, in each session of encryption, but also manage carrier signals without any specific pre-processing. To the best of our knowledge, one of the first studies following this research direction is the work by Chang *et al.* who studied encoding mechanisms for different types of *partially homomorphic cryptosystems* (multiplicative homomorphisms and additive homomorphisms), and developed online and offline predictive models based upon *total variation denoising* and *Bayesian inference*, respectively, in order to suit various operational requirements [62].

IV. FOUNDATIONS OF THE PROPOSED SCHEME

In this section, we present the fundamental mechanisms that form the building blocks of our proposed privacy-preserving

reversible watermarking scheme. We begin by introducing the watermark encoding and decoding mechanisms based upon the Rabin cryptosystem and demonstrate them with a simple example. Then, we discuss the content-adaptive prediction mechanism for assisting image recovery.

A. ENCODING AND DECODING MECHANISMS

Let us start with the encoding and decoding mechanisms based upon Rabin cryptosystem [63]. The goal is to embed information into an encrypted carrier image. We use stream cipher to encrypt an image and exploit properties of the Rabin cryptosystem to encode the watermark into the encrypted image. We refer to the information to be embedded per round of operation as a *watermark symbol* denoted by w and a random variable of the enciphered carrier image as a *cipher symbol* denoted by c. Note that a cipher symbol is not a pixel. Instead, it is an integer convert from certain bits of a group of selected pixels. We shall see the construction of cipher symbols later.

Let p and q be two distinct prime numbers and $n = pq$ be a modulus. The encryption and decryption functions of Rabin cryptosystem are defined as

$$\text{Encryption} : a \equiv c^2 \pmod{n}, \tag{1}$$

and

$$\text{Decryption} : \{\rho_0, \rho_1, \rho_2, \rho_3\} \equiv \sqrt{a} \pmod{n}, \tag{2}$$

where c is an input plaintext, a is an output ciphertext, and ρ_i, $0 \leq i \leq 3$ is a possible deciphered result. It can be observed that the decipherment of Rabin cryptosystem is unusual is a sense that it produces four possible answers, though it is not necessary that they are all distinct numbers. In number theory, a is called a *quadratic residue* modulo n and ρ_i is one of its *square roots*. Note that any square root can be encrypted into the same quadratic residue. In addition to this, the chosen prime numbers p and q are required for efficiently calculating the square roots. For more mathematical details, please refer to Appendix.

The watermark encoding process is carried out as follows. To begin with, we apply Rabin cryptosystem to encrypt c into a and subsequently decrypt a into a set of four possible numbers, $\{\rho_0, \rho_1, \rho_2, \rho_3\}$, in which the numbers are assumed to have been sorted in ascending order, that is, $\rho_0 \leq \rho_1 \leq \rho_2 \leq \rho_3$. Then, we embed w by replacing c with ρ_w resulting $c' = \rho_w$. Consider that at a certain time an authorised party wants to extract w for some intended purposes. With the presence of watermarking key, c' is processed with an encryption and immediately followed by a decryption that yields $\{\rho_0, \rho_1, \rho_2, \rho_3\}$. Finally, the watermark w is determined by matching c' with ρ_w. It is worth pointing out that the number of bits that can be carried may vary in each round of watermarking operation. There are three different cases to be taken into consideration:

1) If there are four distinct values in the set of square roots, two bits of information can be embedded.
2) If there are two distinct values in the set of square roots, one bits of information can be embedded.
3) If there are only one distinct value in the set of square roots, no information can be embedded at all.

In summary, the number of bits able to be carried is equal to $\log_2 \eta$, where η denotes the number of distinct square roots of a given quadratic residue. Due to the fact that the encryption and decryption functions of Rabin cryptosystem are used in conjunction throughout our scheme, we refer to this conjoint operation as *Rabin transform* for simplicity of notation.

Example : An example of how to encode and decode the watermark is demonstrated as follows. Consider a 7-bit carrier cipher symbol

$$c = (0100100)_2 = 36.$$

By applying Rabin transform, the resultant square roots in ascending order are

$$\{\rho_0 = 8, \rho_1 = 36, \rho_2 = 41, \rho_3 = 69\}.$$

Given that c yields 4 distinct square roots, we can embed 2 bits of information into c. Suppose that the intended watermark symbol is

$$w = (10)_2 = 2.$$

To encode the information, we substitute c with ρ_2, resulting

$$c' = 41.$$

To decode the information, we compute the Rabin transform of c' and sort the yielded square roots in ascending order. Finally, by matching c' to ρ_2, we determine $w = 2$.

B. PREDICTION MECHANISM

A marked cipher symbol can be recovered into four candidate symbols, although they are not necessarily all distinct numbers. These candidate symbols would then result in four sets of possible values of the original pixels, which will be discussed in a subsequent section. The issue to be addressed at the moment is to distinguish which set of pixels amongst some given sets is more likely to be the original set. It can be realised through developing a *predictive model* that is capable of estimating pixels at certain locations by pixels at other locations. By perceiving an image as a *Markov random field*, a predictive model can generate a *denoised image* in a sense that some contaminated pixels are purified by their neighbouring correlated pixels.

Let us divide pixels of an image into a group of changeable pixels and a group of unchangeable pixels in such a fashion that each changeable pixel is encircled by four unchangeable pixels located at its north, south, east and west, as illustrated in Fig. 3. The changeable pixels are those used for carrying the payloads and the unchangeable pixels are those used for assisting image recovery. We adopt an efficient but also effective predictive model:

$$\widetilde{u} = \sum_i \psi_i \cdot u_i$$

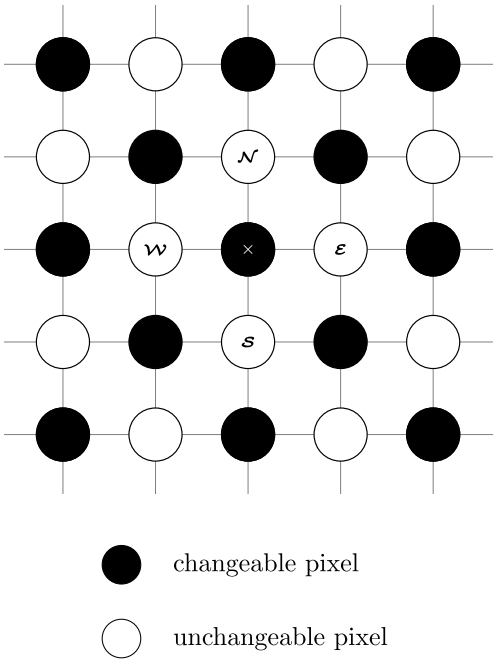


FIGURE 3. Sets of changeable and unchangeable pixels.

$$= \psi_{\mathcal{N}} \cdot u_{\mathcal{N}} + \psi_{\mathcal{S}} \cdot u_{\mathcal{S}} + \psi_{\mathcal{E}} \cdot u_{\mathcal{E}} + \psi_{\mathcal{W}} \cdot u_{\mathcal{W}}, \quad (3)$$

where $\widetilde{u}$ is an estimated pixel, u_i is an uncontaminated pixel, and ψ_i is a weight of the predictive model. The remaining issue is to compute proper weights that lead to an accurate prediction.

Let $\vec{u}$ denote a column vector of n changeable pixels such that

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}, \quad (4)$$

and $\vec{u}_i$ denote a column vector of n unchangeable pixels at corresponding locations, for example,

$$\vec{u}_{\mathcal{N}} = \begin{bmatrix} u_{\mathcal{N},1} \\ u_{\mathcal{N},2} \\ \vdots \\ u_{\mathcal{N},n} \end{bmatrix}. \quad (5)$$

An optimal predictive model would be that minimises the L^2 norm:

$$\left\| \vec{u} - \sum_i \psi_i \cdot \vec{u}_i \right\|_2. \quad (6)$$

According to Hilbert projection theorem, minimising this norm is equivalent to finding a set of weights such that $\vec{v} = \vec{u} - \sum \psi_i \vec{u}_i$ is orthogonal to $\vec{u}_{\mathcal{N}}$, $\vec{u}_{\mathcal{S}}$, $\vec{u}_{\mathcal{E}}$, and $\vec{u}_{\mathcal{W}}$, respectively. In other words, for a given vector $\vec{u}_{\mathcal{N}}$, we have

$$\vec{u}_{\mathcal{N}}^{\mathsf{T}} \cdot \vec{v} = 0, \quad (7)$$

and

$$\vec{u}_{\mathcal{N}}^{\mathsf{T}} \cdot \vec{u} = \vec{u}_{\mathcal{N}}^{\mathsf{T}} \cdot \sum \psi_i \vec{u}_i. \quad (8)$$

Let us express the above equation as

$$\begin{bmatrix} u_{\mathcal{N},1} \\ u_{\mathcal{N},2} \\ \vdots \\ u_{\mathcal{N},n} \end{bmatrix}^{\mathsf{T}} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} u_{\mathcal{N},1} \\ u_{\mathcal{N},2} \\ \vdots \\ u_{\mathcal{N},n} \end{bmatrix}^{\mathsf{T}} \mathbf{A}_{n\times 4} \begin{bmatrix} \psi_{\mathcal{N}} \\ \psi_{\mathcal{S}} \\ \psi_{\mathcal{E}} \\ \psi_{\mathcal{W}} \end{bmatrix}, \quad (9)$$

where

$$\mathbf{A} = \begin{bmatrix} u_{\mathcal{N},1} & u_{\mathcal{S},1} & u_{\mathcal{E},1} & u_{\mathcal{W},1} \\ u_{\mathcal{N},2} & u_{\mathcal{S},2} & u_{\mathcal{E},2} & u_{\mathcal{W},2} \\ \vdots & \vdots & \vdots & \vdots \\ u_{\mathcal{N},n} & u_{\mathcal{S},n} & u_{\mathcal{E},n} & u_{\mathcal{W},n} \end{bmatrix}. \quad (10)$$

By deriving the orthogonality for other three vectors $\vec{u}_{\mathcal{S}}$, $\vec{u}_{\mathcal{E}}$, and $\vec{u}_{\mathcal{W}}$ in a similar manner, we have

$$\mathbf{A}^{\mathsf{T}}\vec{u} = \mathbf{A}^{\mathsf{T}}\mathbf{A}\vec{\psi}, \quad (11)$$

where

$$\vec{\psi} = \begin{bmatrix} \psi_{\mathcal{N}} \\ \psi_{\mathcal{S}} \\ \psi_{\mathcal{E}} \\ \psi_{\mathcal{W}} \end{bmatrix}. \quad (12)$$

Finally, the weights are given by

$$\vec{\psi} = (\mathbf{A}^{\mathsf{T}}\mathbf{A})^{-1}\mathbf{A}^{\mathsf{T}}\vec{u}. \quad (13)$$

V. CONSTRUCTIONS OF THE PROPOSED SCHEME

In this section, we present detailed procedures based upon the mechanisms discussed previously. The aims and tasks of three parties involved (*i.e.* data owner, cloud server, and end user) are discussed respectively.

A. DATA OWNER

Let $\mathbf{m} = \{m_1, m_2, \ldots, m_N\}$ denote an one-dimensional row vector converted from a carrier image such that each element of $\mathbf{m}$ is a pixel. The data owner carries out the encryption procedures as follow:

Step 1: Learn the weight variables $\psi = \{\psi_{\mathcal{N}}, \psi_{\mathcal{S}}, \psi_{\mathcal{E}}, \psi_{\mathcal{W}}\}$ for the predictive model from the given image. The weights are recorded by using 64 bits and may be further compressed into fewer bits.

Step 2: Encrypt each pixel m_i by a stream cipher such that each bit of the pixel is combined with a pseudo-random bit of the keystream via exclusive-or operation. In other words, an enciphered bit is generated by

$$E(\mathfrak{m}_i^k) = \mathfrak{m}_i^k \oplus \mathfrak{r}_i^k, \quad (14)$$

where $\mathfrak{m}_i^k$ denotes the k^{th} bit of the pixel m_i and $\mathfrak{r}_i^k$ denotes a pseudo-random bit defined likewise. In a similar fashion, the cryptographic key is denoted by $\mathbf{r} = \{r_1, r_2, \ldots, r_N\}$ and the enciphered image is denoted by $E(\mathbf{m}) = \{E(m_1), E(m_2), \ldots, E(m_N)\}$.

Step 3: Encrypt the weights via an arbitrary cipher, resulting $E(\psi)$, and if the watermark is provided by the data owner instead of the cloud server, compress and encrypt also the watermark $E(\mathbf{w})$. Depending on different applications, the watermark could be the data owner's intended message such as authentication codes or cloud server's auxiliary information such as data annotation.

Step 4: Send the set of encrypted files $\{E(\mathbf{m}), E(\psi), E(\mathbf{w})\}$ to the cloud server for the subsequent task of watermarking.

B. CLOUD SERVER

Let p and q be two distinct prime numbers chosen by the cloud server and $n = pq$ is the modulus. The cloud server chooses two distinct prime numbers for activating the Rabin transform mechanism, and carries out the message encoding procedures as follows:

Step 1: Sample ℓ changeable encrypted pixels randomly and group them together, yielding $\lambda N/\ell$ groups of pixels in total, where λ denotes the proportion, or the ratio, of changeable pixels. In other words, the total number of groups is equal to the number of changeable pixels divided by the number of pixels sampled each round and thus is represented by $\lambda N/\ell$. The random sampling is initiated by a random seed, which serves as the *watermarking key*. In other words, the embedded information can only be extracted with the presence of this key; otherwise, an unauthorised party can only employ *brute force attack* to find out the sampling patterns.

Step 2: Extract the t^{th} bit from each pixel in a group to form a cipher symbol in a sense that a symbol is a decimal integer converted from ℓ bits. There are $\lambda N/\ell$ cipher symbols in total, and yet by considering the modular arithmetic involved in Rabin transform, the number of changeable symbols should be represented more precisely by

$$N' = \lambda N/\ell - \epsilon, \tag{15}$$

where ϵ denotes the number of symbols whose value exceeds the modulus $n = pq$. Let us denote the changeable cipher symbol used in the current round of watermarking operation by c.

Step 3: Convert $E(\psi)$ and $E(\mathbf{w})$ into N' watermark symbols in a sense that each watermark symbol w is composed of four, two, or zero bit(s) of information adjusted dynamically according to the capacity of corresponding carrier symbol c. The encoding mechanism is realised by Rabin transform as described previously and produces a marked cipher symbol c'. A collection of all marked cipher symbols is converted in an inverse manner to construct the marked and encrypted image denoted by $E(\mathbf{m}')$.

Step 4: Send the marked and encrypted image to the intended end user, who could be the data owner if the initial purpose is to outsource the task to the cloud server, or could be the cloud server if the aim is to utilise the annotations to manage encrypted files stored in the cloud and to prevent unauthorised file exportation. It is also possible that the end user is another authorised party with permission to access the image file as well as the watermark information.

It is worth noting that 2^{ℓ} must not be greater than the modulus n since we use ℓ bits to form a cipher symbol and feed it into the functions involving modular arithmetic. In practice, we determine ℓ first and then choose proper prime numbers p and q to yield proper modulus n. In addition to this, the parameter ℓ governs the balance between the capacity and reversibility. On the one hand, if a cipher symbol is composed of more pixels, the total number of cipher symbols for carrying message payloads decreases and thus a lower capacity. On the other hand, involving more pixels in the construction of a symbol would reduce the probability of sampling a series of unpredictable pixels. Also note that the parameter t governs the fidelity and is also in charge of the reversibility. Depending on the application in hand, we may choose a smaller value for t if the visual quality of watermarked image is of more concern; otherwise, a larger value for t may be chosen to enhance the probability of recovering the watermarked image to a perfect copy.

C. END USER

There are three different levels of accessibility to be taken into consideration depending on the types of keys available to the end user. Let us demonstrate how the end user can react in three different scenarios:

1) The end user has granted the key $\mathbf{r}$ for decipherment and thus is able to obtain a meaningful marked image denoted by $\mathbf{m}'$.
2) The end user has acquired the watermarking key, namely the locations of pixels in each round of sampling. Hence, by applying the decoding mechanism, the embedded messages $E(\psi)$ and $E(\mathbf{w})$ can be extracted. We further assume that the end user is authorised to decrypt and decompress them into meaningful information.
3) The end user has gained access to both cryptographic and watermarking keys. The aim is not only to obtain the marked image and embedded information, but also to recover the original image. The task of image recovery can be realised with aid of the previously discussed prediction mechanism. We start by inputing the weights ψ and marked image $\mathbf{m}'$ into the predictive model, which outputs a denoised image $\widetilde{\mathbf{m}}$. We take a copy of the marked and encrypted image $E(\mathbf{m}')$ and find out $\lambda N/\ell$ groups of changeable pixels via the known sampling patterns. For a group of ℓ cipher pixels, we convert their t^{th} bits into a cipher symbol c' and apply Rabin transform to generate four corresponding

FIGURE 4. Standard 8-bit test images of size 512 × 512.

square roots, which are not necessarily all distinct. We replace ℓ bits of each square root with the t^{th} bits of the very group of ℓ pixels respectively, resulting four modified groups of pixels. Then, we decipher them into four groups of plain pixels. Finally, we compare these four candidate groups of pixels with the group of corresponding pixels of the denoised image. The group of pixels that gives the smallest L^1 norm is determined as that of recovered pixels. The recovery procedures are performed iteratively until all the groups of pixels have been properly processed.

It is worth noting that the reversibility, namely the ability to recover a perfect copy of a carrier image, is content-dependent and is also affected by the configurations of parameters ℓ and t. As aforementioned, these parameters play a pivot role in balancing a three-way trade-off between capacity, fidelity, and reversibility. We will examine their impacts in more detail through the following experiments.

VI. EXPERIMENTS

In this section, we examine the scheme performance with respect to capacity, fidelity, and reversibility. We measure the capacity by the number of bits carried and fidelity by peak signal-to-noise ratio (PSNR). Algorithms are evaluated on standard grayscale test images of size 512×512 widely used across literature, as shown in Fig. 4. Images generated from different steps of process are illustrated in Fig 5. This demonstration begins with an original carrier image, whose semantics are later obfuscated by a stream cipher. After that, 4096 bits of information are embedded into it resulting in a marked and encrypted image, which is then decrypted into a meaningful marked image with fidelity of about 33.64 (dB). In the end of this demonstration, the original image is restored. The parameter configurations are $\ell = 8$ and $t = 6$, indicating that each carrier symbol is formed by the 6^{th} bits of 8 changeable pixels. Our scheme performance is evaluated and compared with the prior art including the schemes by Zhang [33], and Liao and Shu [35], and Dragoi *et al.* [51].

TABLE 1. Maximum payload capacity.

	Payload (bits)
Proposed ($\ell = 6, p = 3, q = 19$)	31219
Proposed ($\ell = 7, p = 3, q = 31$)	22099
Proposed ($\ell = 8, p = 11, q = 23$)	29998
Proposed ($\ell = 9, p = 11, q = 43$)	25331
Dragoi *et al.* ($\ell = 6$)	32512
Dragoi *et al.* ($\ell = 7$)	27867
Dragoi *et al.* ($\ell = 8$)	24384
Dragoi *et al.* ($\ell = 9$)	21675
Zhang	16384
Liao and Shu	16384

TABLE 2. Average prediction error.

	$\psi_{\mathcal{N}}$	$\psi_{\mathcal{S}}$	$\psi_{\mathcal{E}}$	$\psi_{\mathcal{W}}$	Error
Airplance	0.2474	0.2191	0.2786	0.2564	2.84
Lena	0.4046	0.4075	0.0935	0.0954	3.07
Pappers	0.2574	0.2860	0.2461	0.2125	4.03
Zelda	0.4770	0.4760	0.0240	0.0237	2.20

A. MAXIMUM PAYLOAD CAPACITY

The test results of the watermarking capacity with different configurations of parameters (p, q, and ℓ) are presented in Table 1. It is shown that the proposed scheme achieves a larger capacity than [33] and [35] in most cases, and outperforms [51] when the length of symbols (in bits) increases to $\ell \geq 8$. In general, the capacity would decrease as the number of changeable symbols diminishes, namely as ℓ increases. Nonetheless, an interesting observation can be made on the case in which $\ell = 7$. It can be observed that despite a steady linear trend from $\ell = 6$ to $\ell = 9$, there is a sudden downturn when $\ell = 7$. The underlying reason is mainly the infeasible selection of p and q. According to our scheme design, the choice of p and q must satisfy that $pq \leq 2^{\ell} - 1$ and a symbol is changeable only if its value in $[0, 2^{\ell} - 1]$ is smaller than the modulus $n = pq$. A large gap between n and $2^{\ell} - 1$ would lead to a great number of unchangeable symbols and hence it is desirable to choose a pair of p and q such that pq is as close to $2^{\ell} - 1$ as possible. However, in the case when $l = 7$, we are not able to find a pair of proper prime numbers that keeps the gap small enough and thus an abrupt drop in terms of the capacity is observed.

B. CAPACITY-FIDELITY CURVE

The test results of the capacity-fidelity (rate-distortion) curves are shown in Fig. 6 to Fig. 9. Let the pixels specified by coordinates i and j be denoted by $u_{i,j}$ and its marked version by $u'_{i,j}$. The fidelity of a marked image is measured by

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}}, \tag{16}$$

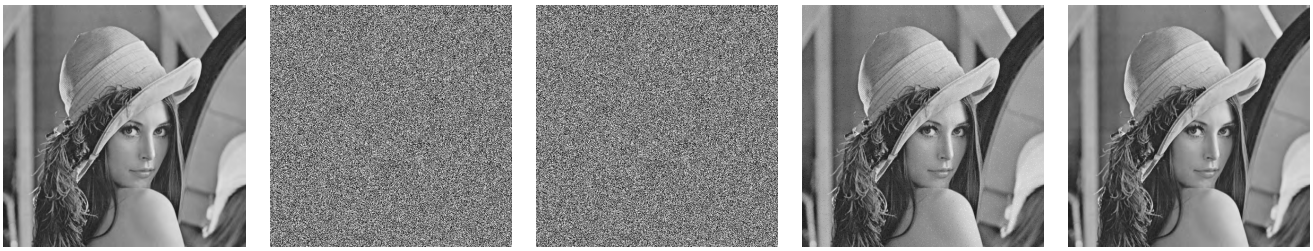
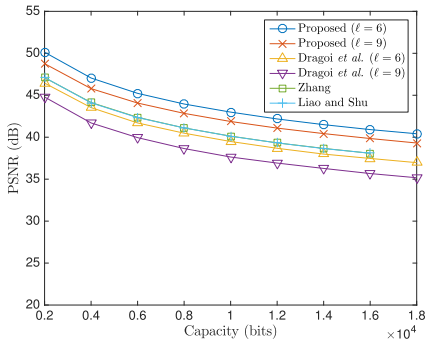


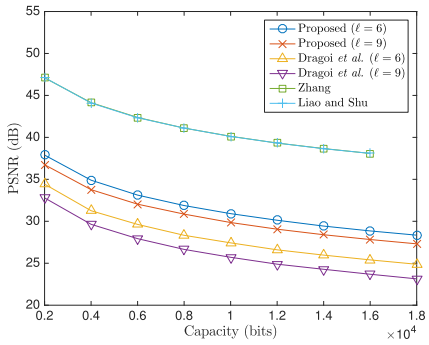
FIGURE 5. Images generated from different steps of process.

TABLE 3. Recovery rates for each bit plane.

	1^{st}	2^{nd}	3^{rd}	4^{th}	5^{th}	6^{th}	7^{th}	8^{th}
Airplance	60.86%	60.57%	75.94%	88.73%	95.42%	98.95%	99.97%	100.00%
Lena	56.78%	56.67%	69.21%	85.72%	95.81%	99.34%	99.98%	100.00%
Pappers	55.14%	55.26%	64.52%	79.26%	93.25%	98.68%	99.87%	100.00%
Zelda	57.50%	57.56%	71.26%	89.92%	99.24%	99.99%	100.00%	100.00%

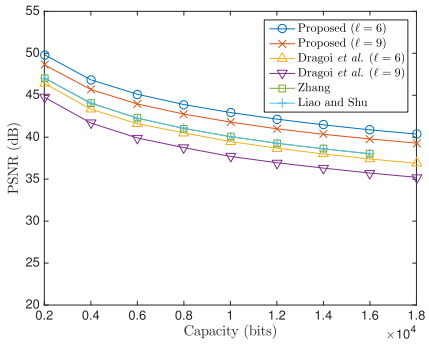


Airplane ($t = 4$)

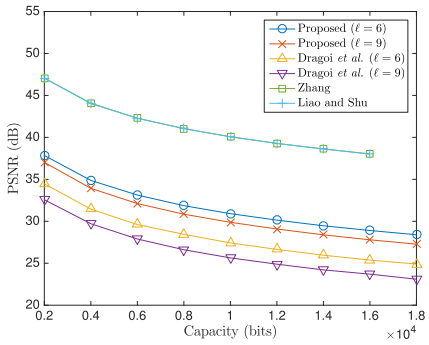


Airplane ($t = 6$)

FIGURE 6. Capacity-fidelity curve (Airplane).



Lena ($t = 4$)



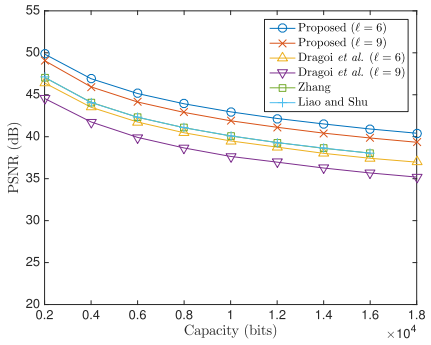
Lena ($t = 6$)

FIGURE 7. Capacity-fidelity curve (Lena).

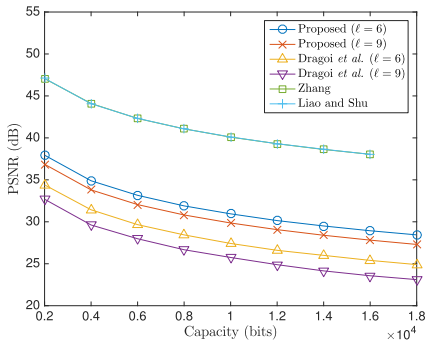
where the mean squared error (MSE) is calculated by

$$\text{MSE} = \frac{\sum_{i=1}^{512}\sum_{j=1}^{512}(u_{i,j} - u'_{i,j})^2}{512 \times 512}. \tag{17}$$

It can be seen that a superior rate-distortion performance over the prior art is achieved when the 4^{th} bit plane is set as the *watermarking channel*, namely when $t = 4$. It can also be observed that a striking decline in performance occurs when $t = 6$, causing the proposed scheme and [51] to be inferior to [33] and [35]. The changes in the 6^{th} bit plane cause severe distortions in visual quality of marked images. Nevertheless, choosing a more significant bit plane as the watermarking channel would enhance the reversibility, namely the probability to recover a perfect copy. Overall, our scheme achieves high fidelity due to the fact that the watermarking process does not necessarily alter all the bits of changeable symbols, and attains high capacity by embedding two bits into each

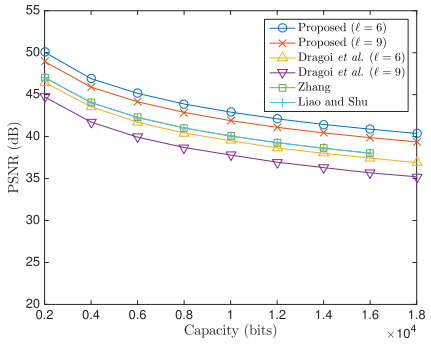


Peppers ($t = 4$)

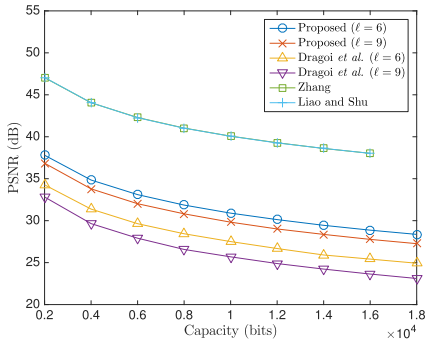


Peppers ($t = 6$)

FIGURE 8. Capacity-fidelity curve (Peppers).



Zelda ($t = 4$)



Zelda ($t = 6$)

FIGURE 9. Capacity-fidelity curve (Zelda).

changeable symbol for the most part. Hence, under the same fidelity constraint, the proposed scheme reaches a higher embedding rate, and *vice versa*.

TABLE 4. Reversibility (Airplane).

Airplane (4096 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	58.10	0.00
Proposed ($\ell = 9, t = 4$)	0.00	59.90	0.00
Proposed ($\ell = 6, t = 6$)	0.06	64.79	0.00
Proposed ($\ell = 9, t = 6$)	0.67	68.51	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	59.47	50.67
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	64.05	12.16
Dragoi *et al.* ($\ell = 6, t = 6$)	0.92	64.43	1.00
Dragoi *et al.* ($\ell = 9, t = 6$)	1.00	∞	0.00
Zhang	0.00	51.07	170.86
Liao and Shu	0.00	60.18	16.46

Airplane (8192 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	55.11	0.00
Proposed ($\ell = 9, t = 4$)	0.00	56.86	0.00
Proposed ($\ell = 6, t = 6$)	0.00	62.37	0.00
Proposed ($\ell = 9, t = 6$)	0.40	68.31	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	56.36	102.86
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	60.20	28.74
Dragoi *et al.* ($\ell = 6, t = 6$)	0.90	64.14	1.10
Dragoi *et al.* ($\ell = 9, t = 6$)	0.88	62.40	1.09
Zhang	0.00	47.15	1174.80
Liao and Shu	0.00	56.82	130.75

Airplane (16384 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	52.06	0.00
Proposed ($\ell = 9, t = 4$)	0.00	53.75	0.00
Proposed ($\ell = 6, t = 6$)	0.00	58.82	0.00
Proposed ($\ell = 9, t = 6$)	0.18	66.60	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	52.15	270.65
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	54.84	97.39
Dragoi *et al.* ($\ell = 6, t = 6$)	0.00	55.97	7.48
Dragoi *et al.* ($\ell = 9, t = 6$)	0.35	60.87	1.69
Zhang	0.00	43.17	3061.40
Liao and Shu	0.00	53.89	258.96

C. REVERSIBILITY

The reversibility refers to the ability to recover the altered pixels. In the previous section, we assumed that the number of changeable pixels is λN, where N is the total number of pixels of a carrier image and λ is the ratio of selected changeable pixels. A more precise value for the number of changeable pixels is calculated by

$$\left\lceil \frac{H-2}{2} \right\rceil \times \left\lceil \frac{W-2}{2} \right\rceil + \left\lfloor \frac{H-2}{2} \right\rfloor \times \left\lfloor \frac{W-2}{2} \right\rfloor, \quad (18)$$

where H and W denotes the height and width of an image. Hence, there are in total 130050 changeable pixels for an image of size 512×512.

The reversibility strongly depends on the accuracy of a given predictive model. Table 2 presents the weight parameters of the applied predictive model as well as its average prediction error, as calculated by

$$\text{Error} = \frac{\sum_{i=1}^{130050} |u_i - \tilde{u}_i|}{130050}, \quad (19)$$

where u_i denotes the true value of a changeable pixel and $\tilde{u}_i$ denotes its estimated value. Overall, the predictive model is content-adaptive with low prediction error in average. Table 3 shows the rates of correct recovery of altered bits by purely considering the *pairwise distances*. The aim is to test and analyse to what extent the predictive model is capable of

TABLE 5. Reversibility (Lena).

Lena (4096 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	57.47	0.00
Proposed ($\ell = 9, t = 4$)	0.00	58.75	0.00
Proposed ($\ell = 6, t = 6$)	0.64	67.91	0.00
Proposed ($\ell = 9, t = 6$)	0.92	69.26	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	58.34	65.37
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	62.35	17.67
Dragoi *et al.* ($\ell = 6, t = 6$)	0.98	64.43	1.00
Dragoi *et al.* ($\ell = 9, t = 6$)	1.00	∞	0.00
Zhang	0.00	54.13	55.30
Liao and Shu	00.0	60.21	12.00

Lena (8192 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	54.47	0.00
Proposed ($\ell = 9, t = 4$)	0.00	55.83	0.00
Proposed ($\ell = 6, t = 6$)	0.05	65.85	0.00
Proposed ($\ell = 9, t = 6$)	0.69	68.85	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	55.28	132.05
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	58.74	39.98
Dragoi *et al.* ($\ell = 6, t = 6$)	0.97	64.43	1.00
Dragoi *et al.* ($\ell = 9, t = 6$)	0.89	62.67	1.00
Zhang	0.00	46.58	1232.30
Liao and Shu	0.99	55.47	161.53

Lena (16384 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	51.46	0.00
Proposed ($\ell = 9, t = 4$)	0.00	58.81	0.00
Proposed ($\ell = 6, t = 6$)	0.00	62.54	0.00
Proposed ($\ell = 9, t = 6$)	0.51	68.65	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	51.54	311.81
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	54.44	106.84
Dragoi *et al.* ($\ell = 6, t = 6$)	0.00	56.28	7.06
Dragoi *et al.* ($\ell = 9, t = 6$)	0.23	60.69	1.80
Zhang	0.00	43.50	2502.00
Liao and Shu	0.00	52.56	315.26

TABLE 6. Reversibility (Peppers).

Peppers (4096 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	54.40	0.00
Proposed ($\ell = 9, t = 4$)	0.00	58.75	0.00
Proposed ($\ell = 6, t = 6$)	0.00	62.81	0.00
Proposed ($\ell = 9, t = 6$)	0.41	67.65	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	56.69	95.50
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	59.82	31.31
Dragoi *et al.* ($\ell = 6, t = 6$)	0.93	64.23	1.07
Dragoi *et al.* ($\ell = 9, t = 6$)	1.00	∞	0.00
Zhang	0.00	52.02	93.40
Liao and Shu	0.00	56.01	35.90

Peppers (8192 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	51.34	0.00
Proposed ($\ell = 9, t = 4$)	0.00	51.77	0.00
Proposed ($\ell = 6, t = 6$)	0.00	59.25	0.00
Proposed ($\ell = 9, t = 6$)	0.26	65.62	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	53.61	193.58
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	56.04	74.16
Dragoi *et al.* ($\ell = 6, t = 6$)	0.87	64.19	1.08
Dragoi *et al.* ($\ell = 9, t = 6$)	0.75	62.25	1.14
Zhang	0.00	45.21	1645.5
Liao and Shu	0.00	52.82	282.05

Peppers (16384 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	48.35	0.00
Proposed ($\ell = 9, t = 4$)	0.00	48.77	0.00
Proposed ($\ell = 6, t = 6$)	0.00	56.07	0.00
Proposed ($\ell = 9, t = 6$)	0.04	64.07	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	49.35	515.57
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	50.94	238.70
Dragoi *et al.* ($\ell = 6, t = 6$)	0.00	52.39	16.51
Dragoi *et al.* ($\ell = 9, t = 6$)	0.04	57.72	3.52
Zhang	0.00	41.96	3443.70
Liao and Shu	0.00	50.01	537.5

assisting the recovery of flipped bits, from the least significant (1^{st}) bit plane to the most significant (8^{th}) bit plane. Let u_i be an original pixel, $\bar{u}_i$ be its altered counterpart with the t^{th} bit being flipped, and $\tilde{u}_i$ be its estimated value generated from the predictive model. Suppose that we have no knowledge about which value, u_i or $\bar{u}_i$, is the original one and decide to recover the pixel as the one closer to $\tilde{u}_i$. Hence, the rate of correct recovery is computed by

$$\text{Rate} = \frac{\sum_{i=1}^{130050} \tau_i}{130050}, \tag{20}$$

where

$$\tau_i = \begin{cases} 1, & \text{if } |u_i - \tilde{u}_i| \leq |\bar{u}_i - \tilde{u}_i|, \\ 0, & \text{otherwise.} \end{cases} \tag{21}$$

As anticipated, it is much easier to recover the bits from a significant bit plane than an insignificant bit plane. Note that this recovery rate does not represent the real recovery rate because in the proposed recovery process we calculate the *accumulated distances* for a group of pixels that together form a symbol, instead of considering individually one pixel after another.

Tables 4 to 7 show the average reversibility performance from 500 trails of experiments with different payload settings (4096, 8192, and 16384 bits). In each trail, we generate a random payload and assign a new watermarking key for randomly selecting ℓ changeable pixels to form a symbol. The reversibility is measured by the probability of perfect recovery and the average PSNR of recovered images. In spite of the fact that the watermark extraction process and carrier recovery process are independent in the proposed scheme, it is not the case for the prior art. In the prior art, failing to recover the carrier image causes a mistaken watermark decoding. Thus, we also include the number of incorrect bits being extracted as one of the measurements. It can be observed that the selected t^{th} bit plane plays a pivotal role in the reversibility. It is scarcely possible to restore a perfect copy when embedding payloads into an insignificant bit plane ($t = 4$) and it is more likely to achieve a perfect recovery when a more significant bit plane is used to carry the payloads ($t = 6$). Apart from this, the number of pixels forming a symbol also has substantial impact on carrier signal recovery. By comparing the cases of $\ell = 6$ and $\ell = 9$, it can be seen that the reversibility is significantly higher when more pixels are grouped together to form a symbol. For [33] and [35], a perfect recovery is barely possible. For [51], a superior reversibility can be achieved under small payload setting (4096 to 8192 bits). Nevertheless, the proposed scheme is in general of higher reversibility when large payloads are applied (16384 bits). Furthermore, the proposed scheme is able to extract the watermark bits without any errors.

TABLE 7. Reversibility (Zelda).

Zelda (4096 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	63.10	0.00
Proposed ($\ell = 9, t = 4$)	0.00	66.17	0.00
Proposed ($\ell = 6, t = 6$)	0.96	69.20	0.00
Proposed ($\ell = 9, t = 6$)	1.00	∞	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	61.35	32.91
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	66.92	6.61
Dragoi *et al.* ($\ell = 6, t = 6$)	1.00	∞	0.00
Dragoi *et al.* ($\ell = 9, t = 6$)	1.00	∞	0.00
Zhang	0.00	60.80	12.46
Liao and Shu	0.00	67.89	3.00

Zelda (8192 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	60.10	0.00
Proposed ($\ell = 9, t = 4$)	0.00	63.18	0.00
Proposed ($\ell = 6, t = 6$)	0.93	70.06	0.00
Proposed ($\ell = 9, t = 6$)	1.00	∞	0
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	58.35	65.41
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	63.13	14.82
Dragoi *et al.* ($\ell = 6, t = 6$)	1.00	∞	0.00
Dragoi *et al.* ($\ell = 9, t = 6$)	0.92	62.48	1.06
Zhang	0.00	46.80	1122.00
Liao and Shu	0.00	56.74	122.62

Zelda (16384 bits)

	Pr	PSNR	Bits
Proposed ($\ell = 6, t = 4$)	0.00	57.10	0.00
Proposed ($\ell = 9, t = 4$)	0.00	60.01	0.00
Proposed ($\ell = 6, t = 6$)	0.92	70.71	0.00
Proposed ($\ell = 9, t = 6$)	0.99	70.20	0.00
Dragoi *et al.* ($\ell = 6, t = 4$)	0.00	54.68	151.57
Dragoi *et al.* ($\ell = 9, t = 4$)	0.00	59.05	37.31
Dragoi *et al.* ($\ell = 6, t = 6$)	0.01	57.05	5.97
Dragoi *et al.* ($\ell = 9, t = 6$)	0.40	61.32	1.50
Zhang	0.00	44.03	2142.30
Liao and Shu	0.00	53.90	233.25

VII. CONCLUSIONS

In this paper, we proposed a novel privacy-preserving reversible information hiding scheme for embedding watermarks into encrypted images in cloud computing environments and other potential real-world applications. We adopt secure and efficient stream cipher for image encryption and utilise the arithmetic of quadratic residues for watermark embedding. In addition to this, a content-adaptive predictive model based upon the projection theorem is devised to fulfil the requirement of recovering the original copy. Experimental results show that in most cases the proposed scheme outperforms the prior art in terms of capacity, fidelity and reversibility. From our perspective, privacy-preserving reversible information hiding will have many more successful real-world applications in the near future because it has evolved the classical information hiding to address security and privacy issues in many new technologies and its reversibility would be a desirable feature for many artificial intelligence aided automated systems in which the available perfect copies are of great significance to the system performance.

APPENDIX

In this appendix, we give a brief introduction to quadratic residues and how to find their square roots [64]. An integer a is called a quadratic residue modulo n if and only if there exists an integer x such that

$$x^2 \equiv a \pmod{n}. \tag{22}$$

Otherwise, a is called a quadratic nonresidue modulo n. According to Euler's criterion, if an integer a is relatively prime to an odd prime p, then a is a quadratic residue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{23}$$

and a quadratic nonresidue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{24}$$

This can be expressed concisely by the Legendre symbol:

$$\frac{a}{p} \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{25}$$

The Jacobi symbol generalises the Legendre symbol by considering an odd positive integer modulus n which is not necessary an odd prime. Suppose that n has the prime factorisation $n = p_1 \times p_2 \times \cdots \times p_k$.

Then the Jacobi symbol is defined as

$$\frac{a}{n} = \frac{a}{p_1} \times \frac{a}{p_2} \times \cdots \times \frac{a}{p_k}. \tag{26}$$

If a is a quadratic residue modulo n, then $(a|n) = 1$. However, the converse does not hold. In other words, a is not necessary a quadratic residue modulo n even if $(a|n) = 1$. Consider the case that an odd positive integer n is factorised into two odd prime p and q. The Jacobi symbol of 1 is possibly the product of two Legendre symbols of -1. That means both $x^2 \equiv a \pmod{p}$ and $x^2 \equiv a \pmod{q}$ have no solutions and thus $x^2 \equiv a \pmod{n}$ has no solutions even though the value of Jacobi symbol is 1. To solve this ambiguity, we need to check whether the value of each Legendre symbol is 1.

We have discussed how to determine whether a quadratic congruence equation is solvable and now we want to find its solutions. It is widely known that factoring a large composite integer is of significant difficulty. The hardness of integer factorisation has formed a cornerstone of a variety of modern cryptosystems such as the Rabin cryptosystem. In other words, Eq. (22) is very difficult to solve when n is the product of two large primes p and q. However, if p and q are known, then the Chinese remainder theorem (CRT) can be applied to solve for x. First of all, let us consider an example of the CRT. Let p and q be two relatively prime moduli and α and β be two known integers, the CRT states that there exists an integer x such that

$$\begin{aligned} x &\equiv \alpha \pmod{p}, \\ x &\equiv \beta \pmod{q}. \end{aligned} \tag{27}$$

and such x is a unique solution modulo $n = pq$. Now, we want to solve Eq. (22) by solving

$$\begin{aligned} x &\equiv x_p \pmod{p}, \\ x &\equiv x_q \pmod{q}. \end{aligned} \tag{28}$$

where

$$\begin{aligned} x_p^2 &\equiv a \pmod{p}, \\ x_q^2 &\equiv a \pmod{q}. \end{aligned} \tag{29}$$

We can use trial and error to solve for x_p and x_q and express the solutions by

$$\begin{aligned} x_p &\equiv \pm\sqrt{a} \pmod{p}, \\ x_q &\equiv \pm\sqrt{a} \pmod{q}, \end{aligned} \tag{30}$$

For odd primes $p, q \equiv 3 \pmod 4$, there exists an efficient formula for solving Eq. (29). That is,

$$\begin{aligned} x_p &\equiv \pm a^{\frac{p+1}{4}} \pmod{p}, \\ x_q &\equiv \pm a^{\frac{q+1}{4}} \pmod{q}. \end{aligned} \tag{31}$$

The CRT has a unique solution for Eq. (28) formulated by

$$x \equiv (x_p \cdot q \cdot b_q + x_q \cdot p \cdot b_p) \pmod{n}. \tag{32}$$

where b_q is a unique modular multiplicative inverse of q with respect to the modulus p, and b_p is a unique modular multiplicative inverse of p with respect to the modulus q. That is to say,

$$\begin{aligned} q \cdot b_q &\equiv 1 \pmod{p}, \\ p \cdot b_p &\equiv 1 \pmod{q}. \end{aligned} \tag{33}$$

Let us rewrite Eq. (33) by

$$\begin{aligned} q \cdot b_q + p \cdot y_p &= 1, \\ p \cdot b_p + q \cdot y_q &= 1. \end{aligned} \tag{34}$$

where y_p and y_q are unknown and irrelevant to our problem. Since $\gcd(p, q) = 1$, Eq. (34) has the form

$$\alpha x + \beta y = \gcd(\alpha, \beta). \tag{35}$$

where α and β are arbitrary integers and x and y are solvable with the extended Euclidean algorithm. Thus, both b_q and b_p in Eq. (33) can be solved accordingly. By substituting the solutions for x_p and x_q in Eq. (31) into Eq. (32), the four square roots for Eq. (22) are obtained by

$$\begin{aligned} x_1 &\equiv (+a^{\frac{p+1}{4}} \cdot q \cdot b_q + a^{\frac{q+1}{4}} \cdot p \cdot b_p) \pmod{n}, \\ x_2 &\equiv (+a^{\frac{p+1}{4}} \cdot q \cdot b_q - a^{\frac{q+1}{4}} \cdot p \cdot b_p) \pmod{n}, \\ x_3 &\equiv (-a^{\frac{p+1}{4}} \cdot q \cdot b_q + a^{\frac{q+1}{4}} \cdot p \cdot b_p) \pmod{n}, \\ x_4 &\equiv (-a^{\frac{p+1}{4}} \cdot q \cdot b_q - a^{\frac{q+1}{4}} \cdot p \cdot b_p) \pmod{n}. \end{aligned} \tag{36}$$

REFERENCES

[1] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[2] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security Privacy*, vol. 7, no. 4, pp. 61–64, Jul./Aug. 2009.
[3] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.
[4] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.
[5] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, Jan. 2013.
[6] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 108–117, Mar. 2013.
[7] J. R. Troncoso-Pastoriza and F. Perez-Gonzalez, "Secure signal processing in the cloud: Enabling technologies for privacy-preserving multimedia cloud processing," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 29–41, Mar. 2013.
[8] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," in *Foundations of Secure Computation*, R. A. DeMillo, Ed. Orlando, FL, USA: Academic, 1978, pp. 169–180.
[9] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.
[10] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.
[11] J. Benaloh, "Dense probabilistic encryption," in *Proc. Workshop Sel. Areas Cryptogr. (SAC)*, Kingston, ON, Canada, May 1994, pp. 120–128.
[12] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Espoo, Finland, May 1998, pp. 308–318.
[13] D. Naccache and J. Stern, "A new public key cryptosystem based on higher residues," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, San Francisco, CA, USA, Nov. 1998, pp. 59–66.
[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Prague, Czech Republic, Mar. 1999, pp. 223–238.
[15] I. Damgård and M. Jurik, "A Generalisation, a Simpli.cation and Some Applications of Paillier's Probabilistic Public-Key System," in *Proc. Int. Workshop Pract. Theory Public Key Cryptogr. (PKC)*, Feb. 2001, pp. 119–136.
[16] C.-C. Chang and S.-M. Tsu, "Arithmetic operations on encrypted data," *Int. J. Comput. Math.*, vol. 56, nos. 1–2, pp. 1–10, Apr. 1995.
[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[18] B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When seeing isn't believing [multimedia authentication technologies]," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 40–49, Mar. 2004.
[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[20] G. L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," *IEEE Trans. Consum. Electron.*, vol. 39, no. 4, pp. 905–910, Nov. 1993.
[21] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, San Diego, CA, USA, May 2015, pp. 1–11.
[22] 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.
[23] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U.S. Patent 5 646 997, Jul. 8, 1997.
[24] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 2, p. 986842, Dec. 2002.
[25] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
[26] C.-T. Li, "Reversible watermarking scheme with image-independent embedding capacity," *IEE Proc.-Vis., Image Signal Process.*, vol. 152, no. 6, pp. 779–786, Dec. 2005.
[27] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
[28] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.
[29] W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.
[30] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE*, vol. 6819, Feb. 2008, Art. no. 68191E.
[31] P. Puteaux and W. Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," in *Proc. Int. Conf. Image Process. Theory, Tools Appl. (IPTA)*, Montreal, QC, Canada, Nov./Dec. 2017, pp. 1–6.

[32] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[33] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[34] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[35] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *J. Vis. Commun. Image Represent.*, vol. 28, pp. 21–27, Apr. 2015.

[36] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 3, pp. 441–452, Mar. 2016.

[37] C. Qin and X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content," *J. Vis. Commun. Image Represent.*, vol. 31, pp. 154–164, Aug. 2015.

[38] Z. Qian, S. Dai, F. Jiang, and X. Zhang, "Improved joint reversible data hiding in encrypted images," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 732–738, Oct. 2016.

[39] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[40] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[41] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in *Proc. 16th Eur. Signal Process. Conf.*, Lausanne, Switzerland, Aug. 2008, pp. 1–5.

[42] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[43] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[44] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[45] J. Zhou, O. C. Au, G. Zhai, Y. Y. Tang, and X. Liu, "Scalable compression of stream cipher encrypted images through context-adaptive sampling," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1857–1868, Nov. 2014.

[46] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.

[47] Z. Qian, X. Zhang, and G. Feng, "Reversible data hiding in encrypted images based on progressive recovery," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1672–1676, Nov. 2016.

[48] Z. Qian, H. Zhou, X. Zhang, and W. Zhang, "Separable reversible data hiding in encrypted JPEG bitstreams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 6, pp. 1055–1067, Dec. 2018.

[49] C.-C. Chang and C.-T. Li, "Privacy-preserving reversible watermarking for data exfiltration prevention through lexicographic permutations," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, vol. 1, Sendai, Japan, Nov. 2018, pp. 330–339.

[50] X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Process.*, vol. 104, pp. 387–400, Nov. 2014.

[51] I. C. Dragoi, H. G. Coanda, and D. Coltuc, "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, Kos, Greece, Aug. 2017, pp. 2186–2190.

[52] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[53] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Trans. Cybern.*, vol. 46, no. 5, pp. 1132–1143, May 2016.

[54] K. Chen and C.-C. Chang, "High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 334–344, Jan. 2019.

[55] H.-T. Wu, Y.-M. Cheung, and J. Huang, "Reversible data hiding in Paillier cryptosystem," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 765–771, Oct. 2016.

[56] X. Wu, B. Chen, and J. Weng, "Reversible data hiding for encrypted signals by homomorphic encryption and signal energy transfer," *J. Vis. Commun. Image Represent.*, vol. 41, pp. 58–64, Nov. 2016.

[57] M. Li and Y. Li, "Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding," *Signal Process.*, vol. 130, pp. 190–196, Jan. 2017.

[58] B. Chen, X. Wu, and Y.-S. Wei, "Reversible data hiding in encrypted images with private-key homomorphism and public-key homomorphism," *J. Vis. Commun. Image Represent.*, vol. 57, pp. 272–282, Nov. 2018.

[59] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," *Signal Process., Image Commun.*, vol. 39, pp. 226–233, Nov. 2015.

[60] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1622–1631, Sep. 2016.

[61] S. Xiang and X. Luo, "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 11, pp. 3099–3110, Nov. 2018.

[62] C.-C. Chang, C.-T. Li, and Y.-Q. Shi, "Privacy-aware reversible watermarking in cloud computing environments," *IEEE Access*, vol. 6, pp. 70720–70733, 2018.

[63] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," MIT Lab. Comput. Sci., Cambridge, MA, USA, Tech. Rep. MIT/LCS/TR-212, Jan. 1979.

[64] G. H. Hardy *et al.*, *An Introduction to the Theory of Numbers*, R. Heath-Brown, Ed., 6th ed. Oxford, U.K.: Oxford Univ. Press, 2008.

CHING-CHUN CHANG received the B.B.A. degree in information management from National Central University, Taiwan, in 2015. He is currently pursuing the Ph.D. degree with the Department of Computer Science, University of Warwick, U.K. He engaged in a short-term scientific mission supported by the European cooperation in science and technology actions at the Faculty of Computer Science, Otto von Guericke University Magdeburg, Germany, in 2016. He participated in a research and innovation staff exchange scheme supported by Marie Skłodowska-Curie actions at the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, USA, in 2017. He has started research activities at the School of Computer and Mathematics, Charles Sturt University, Australia, in 2018, and at the School of Information Technology, Deakin University, Australia, in 2019. His research interests include watermarking, steganography, secret sharing, applied cryptography, digital forensics, multimedia security, image processing, data science, computer vision, machine learning, and artificial intelligence. He received the Marie-Curie Fellowship, in 2017.

CHANG-TSUN LI received the B.Eng. degree in electrical engineering from National Defence University (NDU), Taiwan, in 1987, the M.Sc. degree in computer science from the U.S. Naval Postgraduate School, USA, in 1992, and the Ph.D. degree in computer science from the University of Warwick, U.K., in 1998. He was an Associate Professor with the Department of Electrical Engineering, NDU, from 1998 to 2002, and a Visiting Professor with the Department of Computer Science, U.S. Naval Postgraduate School, in 2001. He was a Professor with the Department of Computer Science, University of Warwick, until 2017, and a Professor with Charles Sturt University, Australia, from 2017 to 2019. He is currently a Professor with the School of Information Technology, Deakin University, Australia. His research interests include multimedia forensics and security, biometrics, data mining, machine learning, data analytics, computer vision, image processing, pattern recognition, bioinformatics, and content-based image retrieval. The outcomes of his multimedia forensics research have been translated into award-winning commercial products protected by a series of international patents and have been used by a number of police forces and courts of law around the world. He is currently an Associate Editor of the *EURASIP Journal of Image and Video Processing* (JIVP) and an Associate of Editor of *IET Biometrics*. He was involved in the organization of many international conferences and workshops and also served as a member of the international program committees for several international conferences. He is also actively contributing keynote speeches and talks at various international events.

KAIMENG CHEN received the B.Sc. and Ph.D. degrees from the University of Science and Technology of China, Hefei, China, in 2010 and 2016, respectively. He was a Visiting Scholar with Feng Chia University, Taiwan, in 2018. He is currently an Assistant Professor with the Computer Engineering College, Jimei University, Xiamen, China. He is a principle investigator of a project of the National Science Foundation of Fujian Province, China, and a co-investigator of two projects of the National Natural Science Foundation of China. His research interests include data hiding, image processing, databases on new hardware, hybrid storage, and non-volatile memory technology.