IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 30, 2020, accepted August 6, 2020, date of publication August 11, 2020, date of current version August 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3015882

High-Capacity Reversible Data Hiding in Encrypted Images Using Multi-Layer Embedding

ASAD MALIK[1], PEISONG HE[2], (Member, IEEE), HONGXIA WANG[2], (Member, IEEE), AHMAD NEYAZ KHAN[3], SAIED PIRASTEH[4], AND SANI M. ABDULLAHI[5], (Member, IEEE)

[1]School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China
[2]College of Cybersecurity, Sichuan University, Chengdu 610065, China
[3]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[4]Department of Surveying and Geoinformatics, Faculty of Geosciences and Environmental Engineering, Southwest Jiaotong University, Chengdu 611756, China
[5]Sichuan Wai Zhimaoyuan IT/Edu Consulting Firm Company Ltd., Chengdu 610023, China

Corresponding author: Peisong He (gokeyhps@scu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61972269 and Grant 61902263, in part by the Fundamental Research Funds for the Central Universities under Grant YJ201881and Grant 2020SCU12066, and in part by the China Postdoctoral Science Foundation under Grant 2020M673276.

ABSTRACT Reversible Data Hiding in Encrypted Images (RDH-EI) has gained much popularity in the field of signal processing and cloud computing. In this study, we propose a high-capacity RDH-EI scheme using multi-layer embedding. It ensures that after extraction of the embedded additional data from the marked encrypted image, the original image is recovered completely. Broadly, the method comprises three parties: the content owner, the data hider/ cloud owner, and the receiver. In the beginning, the image is encrypted by the content owner using encryption based on the chaotic behaviour of PWL-memristor and sent to the data hider. At the data hider's side, even-odd value embedding technique is applied in multiple layers of the encrypted image to increase the embedding capacity. Meanwhile, the auxiliary information consisting of location map (LM) for each layer and the number of layers, to be used in the recovery phase, is recorded during the embedding. After completing the embedding procedure, permutation operation is applied on the marked encrypted image to prevent the perceptual information leakage. Finally, at the receiver's side the embedded additional data and the original image is recovered losslessly with the help of valid keys and shared auxiliary information. From the experimental results, it is observed that the quality of the directly decrypted image is 51.0 dB or above. The advantage of the proposed scheme is that the PSNR is almost same for each layer, i.e. even for the n number of layers used, the PSNR is 51.0 dB or above. Moreover, we applied chosen plaintext attack to test the encryption function and in case of any cropping attack on the marked encrypted image during the transfer, the cover image can be recovered with less distortion.

INDEX TERMS Reversible data hiding (RDH), cloud computing, encrypted image, high capacity, image recovery.

I. INTRODUCTION

Nowadays, the digital data communication over the Internet is a very important component for our modern society. With the growth of digital data communication, the security of digital data over the Internet is becoming a challenging task for the researchers. The basic taxonomy of techniques used in the security systems for digital data over the Internet can be seen in Fig. 1. The security systems of digital data depends on users' requirements i.e. original digital content security, authentication based security, imperceptible way security etc. The main aim of any security system is to establish secure communication for digital data over the Internet between sender and receiver. Basically, it can be achieved in two ways: cryptography and data hiding. Cryptography is the method where the digital data is converted into completely unreadable form, so that the adversary cannot identify the original digital media. The conventional data hiding technique such

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

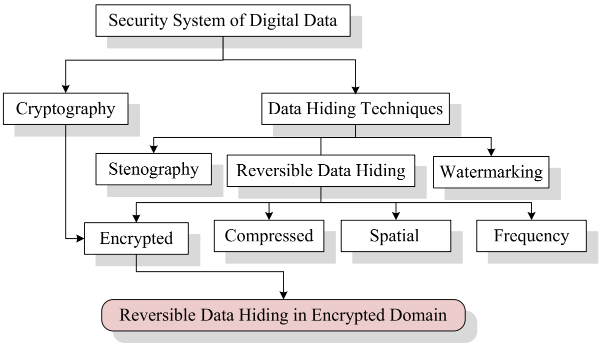


FIGURE 1. **Taxonomy of security systems for digital data.**

as steganography, watermarking and Reversible Data Hiding (RDH) [1]–[4] have some special characteristics. Steganography is used for covert communication over the Internet which means secret digital data is embedded in cover media in an imperceptible way, so that the adversary does not get any knowledge of its existence. Whereas, in digital watermarking, the focus is on how to reliably recover the embedded data from a possibly degraded marked media. Robustness is the main concern in watermarking, and original cover media's recovery is not taken care of. Another type of data hiding known as RDH, has its pros and cons over the popular data hiding techniques. RDH focusses on the recovery of both the embedded data and the original media in a lossless manner from the marked media. In some sensitive scenarios, RDH plays an important role and used extensively in many areas like law, forensics, military imagery, and medical imagery. By this technique, the content owner embeds the additional data into the cover media (image, audio, video), and later allows the intended receiver to recover the embedded additional data and original media from the marked media losslessly. Basically, RDH can be categorized into compressed, spatial, frequency, and encrypted domain.

In recent years, with the growing popularity of cloud based services, users rely on cloud server to upload their multimedia files. The uploaded multimedia files can be accessed from the cloud server any time and anywhere. But, the users demand privacy of their original multimedia files from the cloud servers. In this scenario, the use of Reversible Data Hiding in Encrypted Images (RDH-EI) [5]–[7] has become popular. This not only provides independence for security from the third party but also gives freedom to the data hider/ cloud service provider to embed the additional data into it, without revealing the original content of media. And the receiver can recover the original media as well as the embedded additional data.

The two important metrics to show the performance of RDH-EI schemes are the Embedding Rate (ER) and the visual quality of the directly decrypted image. However, visual quality is measured in terms of Peak Signal to Noise Ratio (PSNR) in Decibel (dB) and the ER is measured in terms of Bit Per Pixels (bpp). During the embedding process distortion is introduced which results in the PSNR of directly decrypted image being effected by embedding rate. For a good RDH-EI scheme, researchers have to maintain an optimum balance between ER and the PSNR of directly decrypted image.

It is worth highlighting the following aspects of the proposed scheme.

- Our proposed RDH-EI scheme is a combination of PWL memristor and even-odd embedding technique, where PWL memristor is used to secure the original content of gray-scale image and even-odd embedding technique is used to efficiently encrypt the image at data hiding phase.
- The proposed RDH-EI scheme falls in the category of Vacating Room After Encryption (VRAE), i.e. the preprocessing step is not required at the content owner phase, and allows multi-layer embedding which further enhance the embedding capacity at the data hiding phase.
- Experimental results show that the proposed scheme is independent of image texture and PSNR of the marked encrypted image after the direct decryption is at least 51dB or above for more than 1 bpp. And it also shows that, after applying chosen plaintext attack, the encryption function achieves better security performance. Besides, in case of any cropping attack on the marked encrypted image during the transfer, the cover image can be recovered with less distortion.

The rest of the paper is organized as follows: Section 2 provides with the related work. Section 3 explains the framework of the proposed scheme in detail. We present experimental results in Section 4. Section 5 concludes the remarks and future work.

II. RELATED WORK

Barton proposed the notion of a RDH scheme in the year of 1997 [1]. Subsequently, many RDH schemes have been proposed, which can be broadly classified into the following three categories: Difference expansion (DE) [2], histogram shifting (HS) [3] and Lossless compression [4].

In the first category, Tian [2] proposed a high capacity RDH method based on DE where the idea is based on two neighboring pixels used as group and each group is used to embed one bit of secret data by modifying their pixel difference. The DE technique achieved high embedding capacity but it distorted the marked media which leads to low visual quality. Furthermore, this idea was extended in various methods to improve: the embedding performance in pixel prediction step [8], location map compression [9] and generalized integer transformation [10].

HS-based method, representing the second category, was initially proposed by Ni *et al.* [3] in 2006. The algorithm is simpler than DE approach based algorithms as it requires less computational complexity. The method uses shifting of bin intensities from maximum (or peak) to minimum (or zero) in the histogram of the input image pixel values to make space for data hiding. Embedding here is realized by bin shifting from peak to zero, after the maximum value bin has been assumed. One of the advantages of HS-based schemes is high PSNR of the marked image. However, the capacity of Ni's algorithm is limited and depends on peak valued bin, which makes it inefficient for most of the applications. However, Ni's algorithm have formed a base for research in this area. Hwang *et al.* [11] used the pixel values from the image histogram between the maximum point and two left-right minimum points, to embed the additional data. However, the embedding capacity was low with PSNR as high as 48.40 dB. Chung *et al.* [12] used dynamic programming to choose the fittest peak valley pair from the histogram, to improve the embedding capacity. The drawbacks include dependence of the algorithm on the texture of the image where complexity in texture costs the increase in the execution time.

Lossless compression, the third category utilizes the redundancy in the original media and use compression to make space for embedding additional data. This is done in as lossless manner such that the additionally embedded data is extracted losslessly along with the complete recovery of the original media. Some new works in the field of RDH schemes have combined the feature of above techniques, e.g., prediction error as a special case of DE has been used to attain high PSNR and ER [13], [14]. Moreover, the idea of RDH schemes also growing with video processing as in [15], [16].

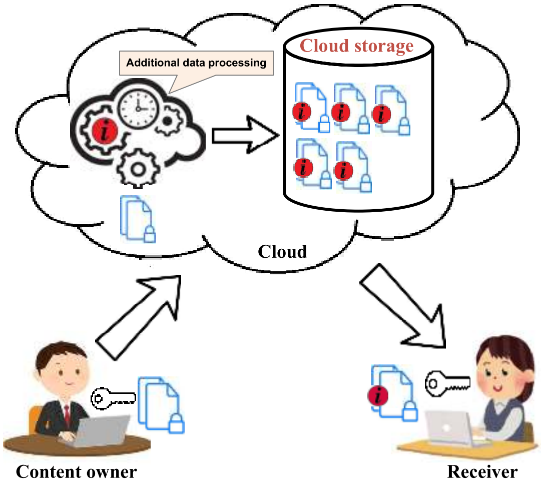


FIGURE 2. Securely encrypted file processing on Cloud.

With the valuable characteristics of RDH in plain image, the idea has attracted attention of many researchers to implement the technique in the field of cloud computing and signal processing for the encrypted domain. To explain it, with the help of a scenario as in Fig. 2, the content owner may wish to share an original image only with the receiver. The content owner of original image converts the original image into unintelligible form (i.e. encrypts the original image) before sending it to the cloud. That is, the adversary doesn't know the content of original image, in order to do so, a secure encryption technique is choosen, that resist against adversarial attacks, for example chaotic image encryption must resist against the chosen-plaintext attack [17]–[19]. In this way the cloud (or the adversary) doesn't know the original content of the image. In order to deal with the encrypted media, the cloud owner wishes to attach some additional data, related to the media for the sake of file management, such as origin information, multimedia file notation, authentication, and validation based data. The receiver can recover both the original media and the embedded additional data with valid keys. The extended version of RDH idea in the presence of third party (i.e. data hider) is known as Reversible Data Hiding in Encrypted Image (RDH-EI). The cloud owner can embed the additional data without any information being revealed about the original image. At the receiver's side, both the embedded additional data and the original media are recovered without any loss. Finding the optimum value for both the ER and the PSNR of the directly decrypted image is the main goal.

Furthermore, the idea of RDH has got much attention from the researchers, to develop with the third party without disclosing the original content. In the recreant study, RDH-EI schemes [20] are challenging and can be categorized in two major categories: Vacating Room After Encryption (VRAE) and Vacating Room Before Encryption (VRBE).

First, VRAE [5] which is more practical, where the embedding is performed after the image has been encrypted. Zhang [5] proposed the first RDH-EI scheme in 2011, where a stream cipher is used to encrypt the original image. After that, the encrypted image is decomposed into blocks where each block is responsible for carrying a bit of additional data. In order to embed the additional bit in each block, half of number of pixels are modified such that their three least significant bits (LSBs) are flipped. Further improvement of Zhang's scheme is done by Hong *et al.* [6] by side-matching to lower down the rate of error in the additional data extraction. Zhang [7] proposed a RDH-EI scheme based on separable manner,where the parameters are carried by a part of the encrypted bits and the Least Significant Bits (LSBs) of the remaining part of the encrypted bits are compressed in order to make space for the additional data using data the hiding key. Three cases arise at the receiver's side, 1) Extraction of the additional data with the use of the data hiding key, 2) Approximate image recovery with the use of decryption key and 3) Complete original image recovery with the use of both the keys. The scheme [7] provides lossless recovery of both the additional data and the original image but with a disadvantage of low payload. Further, Qian and Zhang [21] modified the histogram to enable additional data embedding enhancing the ER. VRAE exploits the redundancy in the encrypted image which has high entropy due to encryption. Thus, for high entropy, redundancy is low which results into low ER.

Second category is VRBE [22], where the spare space for additional data embedding is created by the content owner before the original image is encrypted. This is a preprocessing

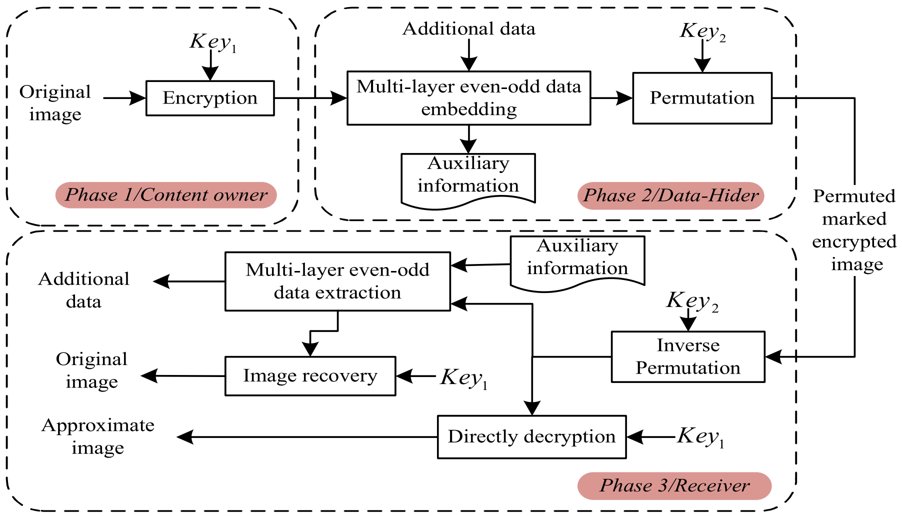


FIGURE 3. Illustration of the idea.

step taken before encryption. The VRBE method might be impractical as the content owner needs to do an extra effort to create the space for the data hider. In the method [22], payload is 0.5 *bpp* and the reconstructed image quality in PSNR is close to 40*dB*. Zhang *et al.* [23] exploited the pixel prediction errors to make space for additional data prior to encryption, by histogram shifting of these prediction errors. In [24], Xu and Wang proposed a scheme using histogram shifting and difference expansion where the interpolation-error is encrypted using a unique mode of encryption using stream cipher. In [25], Cao *et al.* proposed a high capacity RDH-EI using sparse coding technique and over-complete dictionary method in order to get a high embedding capacity. To further improve the embedding capacity, Huang *et al.* proposed a new image encryption method, which includes image block partition, stream cipher encryption, and block permutation [26]. Geetha and Geetha [27] has been presented multi-layered odd-even RDH-EI scheme, where non-overlapping block-wise disordering of bit planes with pixel and block scrambling to encrypt the original image and embedding is done by ± LSB based. Moreover, the average PSNR for 1 bpp and 1.5 bpp are 46.51 dB and 43.36 dB respectively. There are some classical RDH-EI schemes which have been presented with symmetric key cryptography [28]–[37] and some of the works with public key cryptography [38]–[46] in the recent years..

III. PROPOSED SCHEME

We have proposed a new scheme which allows multi-layer data embedding in encrypted images using well known even-odd value embedding technique. The idea can be divided into three basic phases namely: 1) image encryption, 2) data embedding, and 3) data extraction and image recovery. A sketch of the proposed scheme can be visualized in Fig. 3. The original image is encrypted by the content owner in phase 1. In phase 2, the data hider, without knowing the original content of image, can embed the additional data into it. The procedure of embedding the additional data into the encrypted image, using multi-layer even-odd embedding technique followed by the recording of the auxiliary information(i.e information of layer wise even/odd value of pixels and the number of layers). To the best of our knowledge, this is the first work to use even-odd embedding in encrypted images. In order to improve the privacy and security during the transmission of the marked encrypted image, the data hider applies permutation operation on the marked encrypted image. In phase 3, the receiver recovers the additional data and the original image with the help of shared auxiliary information and in accordance with the valid keys possessed. The auxiliary information and the keys are shared through another private channel. If the receiver does not have the auxiliary information, he/she can recover image similar to the original image(i.e approximate image), with quality of directly decrypted image being constant.

A. IMAGE ENCRYPTION

In our proposed scheme, image encryption is applied to convert the original image I into unreadable form, where I has size $\ell = M \times N$, each pixel value of image lies in [0,255] and is represented by 8 bits. We have used a popular Chaos-based Chua's circuit with PWL memristor for image encryption [47]. Three chaotic sequence sets are generated i.e. $P = \{p_i | i = 1, 2, \ldots \ell\}$, $Q = \{q_i | i = 1, 2, \ldots \ell\}$, $R = \{r_i | i = 1, 2, \ldots \ell\}$ by the Chua's circuit using PWL memristor as in [48], where each sequence is of length equal to ℓ. The normalized Chua's circuit with a PWL memristor is given below, which has the characteristics of a chaos attractor.

$$\left.\begin{aligned} \frac{dx(\tau)}{d\tau} &= a(y(\tau)) - x(\tau) - \bar{f}(x(\tau)) \\ \frac{dy(\tau)}{d\tau} &= x(\tau) - y(\tau) + z(\tau) \\ \frac{dz(\tau)}{d\tau} &= -by(\tau) \end{aligned}\right\} \tag{1}$$

$$\bar{f}(x(\tau)) = \begin{cases} \bar{n}x(\tau) + \dfrac{\overline{m}-\bar{n}}{2}(|x(\tau)+1| - |x(\tau)-1|) \\ \quad \dfrac{dx}{d\tau} < 0 \\ \bar{q}x(\tau) + \dfrac{\bar{p}-\bar{q}}{2}(|x(\tau)+1| - |x(\tau)-1|) \\ \quad \dfrac{dx}{d\tau} \geq 0 \end{cases} \tag{2}$$

where $a, b, \overline{m}, \bar{n}, \bar{p}, \bar{q} \in R$ (R is real number set) and $a, b > 0$

After choosing the system parameters $a = 10$, $b = 18$, $\bar{n} = -0.15$, $\overline{m} = -1.56$, $\bar{p} = \bar{q} = -0.8$, the resulting chaotic attractor is shown in Fig. 4.

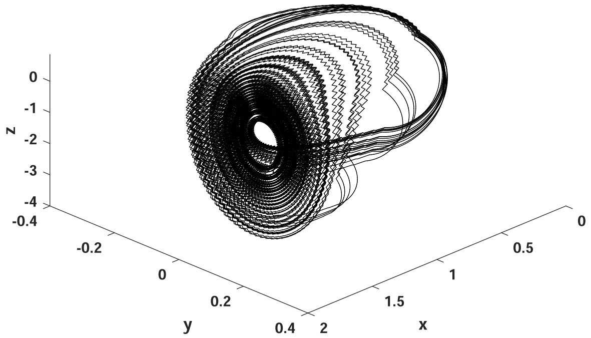


FIGURE 4. Chaotic attractor with the PWL memristor.

Next, with the help of quantization Eq: 3, the chaotic sequence sets are P, Q is used to give quantization sets P', Q' with the maximum value M and N respectively i.e. p_i is converted into $p'_i = f(p_i, M)$ and q_i is converted into $q'_i = f(q_i, M)$ where $p'_i \in P'$ and $q'_i \in Q'$. Also, the chaotic sequence set S is converted to quantization set S' using the quantization Eq: 4 i.e s_i is converted into $s'_i = f(s_i)$ where $s'_i \in S'$. The quantization function (a mapping technique where finite large set is converted to finite smaller set) are defined by

$$f(\hat{e}, L) = (\lfloor 10^3 \times (|\hat{e} - \lfloor \hat{e} \rfloor|) \rfloor) mod (L-1) + 1 \tag{3}$$

$$f(\hat{e}) = (\lfloor 10^3 \times (|\hat{e} - \lfloor \hat{e} \rfloor|) \rfloor) mod\ 256 \tag{4}$$

where L is the maximum value which we need after quantization and $\hat{e}$ is the element of chaotic sequence.

Furthermore, original image is scrambled using the sequence P', Q', same as in [49] and subsequently the scrambled image goes through pixel replacement using the sequence S'. Note that in the scrambling process, statistical property of pixels remain same but changes when the pixel replacement function is applied. The pixel replacement function is defined by

$$I_e = S' \oplus I_{sc} \tag{5}$$

where I_{sc} is the scrambled image.

Finally, the encrypted image I_e is generated. The decryption is the reverse process of the encryption. Moreover, the memristor is a passive circuit element which have the property of a resistor with memory [50]. The use of PWL memristor as a memory device in computers will further reduce power consumption by saving the time for data reloading.

The initial parameters (x, y, z) in Chua's circuit with a PWL memristor are used as an encryption key, $Key_1 = (x, y, z)$. However, it is noticeable that instead of a chaotic generator, as used in our method, a pseudo-random sequence generated with a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) can also be used or, for example, the Advanced Encryption Standard (AES) algorithm can also be used in Output Feedback (OFB) mode.

B. DATA EMBEDDING IN AN ENCRYPTED IMAGE

In the data embedding phase, the data hider embeds the additional data in the encrypted image I_e, even if the data hider is unaware of the content of original image and encryption key (Key_1). Getting comprehensive, the even-odd value embedding method is used to embed one bit of additional data per pixel. The embedding order of each layer involves scanning from left to right, and then from top to bottom (scan line order).

The Location Map (LM) in the embedding phase for each layer is recorded as a part of the necessary auxiliary information, that will be used to recover the original image and the additional embedded data in the recovery phase. The LM for each layer, refers to the even and odd valued pixel for that particular layer.

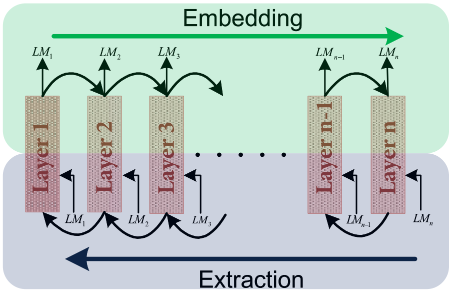


FIGURE 5. Layer wise embedding and extraction.

The procedure for the additional data embedding depends on whether the encrypted pixel value is even or odd. Let, the additional data be d and $d_1, d_2 \cdots d_k$ be the corresponding bit sequence, where k represents k^{th} bit of the additional data. If $d_k = $ '1', then we increase the pixel value by one for the corresponding even pixel value and decrease the pixel value by one for the corresponding odd pixel value. And, if the additional data bit is $d_k = $ '0' then the corresponding pixel value is left unchanged. In layer 1, after the marked encrypted image and the LM is generated, the LM is recorded as a part of the auxiliary information. If the pixel value is even, LM is recorded as '0' otherwise '1'. Similarly in layer 2, after additional data embedding, the LM is recorded for the second layer as a part of the auxiliary information. Continuing this procedure for the remaining layers till all the bits of the additional data are embedded completely. At the data hider side as shown in Fig. 5, the embedding of additional data

Algorithm 1: Block Permutation

```
Input:
$I$: Image, $s$: Block size, $Key_2$: Permutation key
$w$: '0' Permutation and '1' Inverse permutation
Output:
$I_p$: Permuted image
Initialization:
$[L, B] = size(I)$, $a = fix(\frac{L}{s})$, $b = fix(\frac{B}{s})$
        // fix, rounds values toward zero
Generate a random sequence $R$ having size $a \times b$, with
  the initial state $Key_2$
$[\sim, loc_0] = sort(R)$
        // sort, sorts the elements
$[\sim, loc_1] = sort(R, 'descend')$
k=1
for $i \leftarrow 1$ to $a$ do
    for $j \leftarrow 1$ to $b$ do
        $c_i = ceil(loc_w(k)/b)$
            // ceil, nearest integer toward
            positive infinity
        $c_j = loc_w(k) - (c_i - 1) \times b$
        $V = I((s \times i - s + 1) : s \times i, (s \times j - s + 1) : s \times j)$
        $I((s \times i - s + 1) : s \times i, (s \times j - s + 1) : s \times j) =$
          $I((s \times c_i - s + 1) : s \times c_i, (s \times c_j - s + 1) : s \times c_j)$
        $I((s \times c_i - s + 1) : s \times ci, (s \times c_j - s + 1) : s \times c_j) = V$
        $k = k + 1$
    end
end
$I_p = I$
return $I_p$
```

(in the 1st layer) produces binary location map (for the 1st layer), then the embedding of additional data (in the 2nd layer) is done producing binary location map (for the 2nd layer) and so on till we reach the n-th layer. After, LM generation for the last or the n-th layer, we get the marked encrypted image. That is, after all the additional data bits are embedded, the marked encrypted image is generated after embedding is done in the last layer and the axillary information (LM and the number of layers) of each layer is collected. The marked encrypted image (I_d) is further processed by the permutation function. Moreover, the permutation operation can be understand by the Algorithm 1. We have chosen the block permutation operation on (I_d) to convert it into permutated marked encrypted image(I_p) using the initial value as a key Key_2. In [51], lower the block size higher the security, in order to keep the security high, we have chosen the block size 4 and the 'rand' function from MATLAB is used to get the random sequence R, where Key_2 is the initial state. This scheme can survives illegal modification to some extent due to this inherent chaotic property. detailed embedding procedure can be seen in Algorithm 2.

Algorithm 2: Embedding Additional Data Into Encrypted Image

```
Input:
$I_e$: Encrypted image, $d$: Additional data
$Key_2$: Permutation key, $n$: Number of layer
Output:
$I_p$: Permuted marked encrypted image
$A$: Auxiliary information.
Initialization:
Step1: Set the $layer = 1$;
while $layer \leq n$ do
    for $i \leftarrow 1$ to $size(I_e, 1)$ do
        for $j \leftarrow 1$ to $size(I_e, 2)$ do
            if additional data bit $d_k$ is '0' then
                Do nothing
            else
                if $I_e(i, j)$ is the even value then
                    $I_e(i, j) = I_e(i, j) + 1$;
                else
                    $I_e(i, j) = I_e(i, j) - 1$;
                end
            end
        end
    end
    A($Layer$) $\longleftarrow$ Construct the $LM$
    $layer = layer + 1$;
end
Step2:The number of layer and LM for each layer is
  considered as auxiliary information (A).
Step3:The marked encrypted image $I_d$ is generated.
Step4:Apply the permutation operation on $I_d$,
  to generate $I_p$ by using $Key_2$.
```

C. EXTRACTION OF ADDITIONAL DATA AND RECONSTRUCTION OF IMAGE

At the receiver's side, to extract the additional data and recover the original image, the receiver must have both the keys (Key_1, Key_2) and the auxiliary information shared via some private channel. First of all, the receiver applies the reverse permutation operation on I_p using Key_2 to get marked encrypted image(I_d). Marked encrypted image (I_d) with the help of auxiliary information (A) is used to extract the additional data correctly. As shown in Fig. 5, the recovery of additional data (in the n-th layer) is done by using binary location map (for the nth layer), then the recovery of additional data (in the (n-1)-th layer) is done by using binary location map (for the n-1-th layer) and so on till we reach the 1st layer. After, we use the LM to extract additional data for the first layer, we get the encrypted image. After extracting the additional data from each layer, all the additional data is combined together to generate the original additional data.

For the image recovery, the receiver performs the same procedure until the additional data is extracted completely,

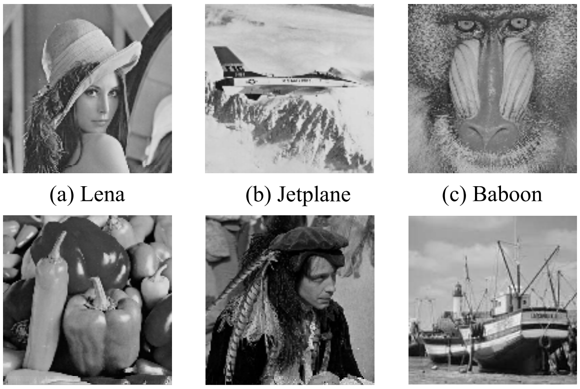
Algorithm 3: Extraction of the Additional Data and Recovery of the Original Image

```
Input:
  $I_p$: Permuted marked encrypted image
  $Key_1$: Encryption key, $Key_2$: Permutation key
  A: Auxiliary information
Output:
  $d$: Additional data
  $I$: Original image
Case1 : Additional data extraction.
Step1: With the help $Key_2$ reverse permutation is applied
  on $I_p$ to get the marked encrypted image $I_d$.
Step2: Separate the $LM$ for each layer and the number of
  layer from A.
while $layer \neq 0$ do
    for $i \leftarrow 1$ to size($I_d$, 1) do
        for $j \leftarrow 1$ to size($I_d$, 2) do
            if corresponding bit of LM is the same as the
              current pixel value then
                The embedded additional data bit is '0';
            else
                if $I_d(i, j)$ is the even value then
                    $I_d(i, j) = I_d(i, j) - 1$;
                else
                    $I_d(i, j) = I_d(i, j) + 1$;
                end
                The embedded additional data bit is '1';
            end
        end
    end
    $layer = layer - 1$;
end
Step3: $d$ is recovered from $I_d$.
Case2 : Recover the original image.
Step4: Do the steps from 1 to 3.
Step5: Using the $Key_1$ to recover the original image $I$.
```

up to the first layer (layer 1). After that, the key Key_1 is used to recover the original image losslessly. The detailed procedure of additional data extraction and image recovery can be understood by the Algorithm 3. If the receiver dose not have auxiliary information, he/she can recover the approximate image.

IV. EXPERIMENTAL RESULTS

In this section, we have evaluated the performance of the proposed method by performing experiments on some of the standard gray-scale images[1] as shown in Fig. 6. The size of each test image is 512 × 512 pixels. All the computation is done on a PC with a Pentium (R) Dual-core CPU E5700@3.00 *GHz* and 4 GB RAM. The operating system used is Window 10 professional 64-bit, and all the algorithms were implemented in MATLAB R2015b. For the image encryption Key_1, and permutation key Key_2: $Key_1 = (0.40001, 0.01, 0.11)$, $Key_2 =$ '$27450121'$' had been taken as constant values for our overall experiment. The visual quality and perceived quality of the recovered image are evaluated by using Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM) metrics respectively. The formulation of PSNR is given as



(a) Lena (b) Jetplane (c) Baboon

(d) Peppers (e) Man (f) Boat

FIGURE 6. Six 512 × 512 standard gray scale images.

$$PSNR = 10 \cdot \log_{10} \frac{255 \times 255}{MSE} (dB). \tag{6}$$

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_{i,j} - R_{i,j})^2. \tag{7}$$

where $I_{i,j}$ and $R_{i,j}$ denote the original image and the recovered image at the pixel location (i, j), respectively. A large value of PSNR shows that the constructed image has high visual quality.

Wang&Bovik introduced SSIM [52] to measure the degradation in the quality based on structural information. The range of SSIM lies between -1 and 1. The value 1 indicates that the images are identically same. SSIM between two image I and R is formulated as

$$SSIM(I, R) = \frac{(2\mu_I \mu_R + c_1)(2\sigma_{IR} + c_2)}{(\mu_I^2 + \mu_R^2 + c_1)(\sigma_I^2 + \sigma_R^2 + c_2)} \tag{8}$$

where,μ_I, μ_R, σ_I^2, σ_R^2 are the mean and variance of images I and R respectively, σ_{IR} is the covariance between image I and R. c_1 and c_2 are the predefined constants which are as follows:

$$\left.\begin{array}{ll} c_1 = (k_1, L)^2; & \quad where \quad k_1 \ll 1 \\ c_2 = (k_2, L)^2; & \quad where \quad k_2 \ll 1 \end{array}\right\} \tag{9}$$

where L is defined as the dynamic range of the pixel values.

Our first experiment is based on the standard gray-scale image *Lena* shown in Fig. 7 (a) with the single layer. To understand the phases in our proposed scheme, image *Lena* has been taken as the main test image. In the initial phase, image is encrypted by [47], which is having chaotic property. Fig. 7 (b) shows the encrypted version of the original image, next, the encrypted image is sent to the data hider. In the data

[1] http://decsai.ugr.es/cvg/dbimagenes/g512.php

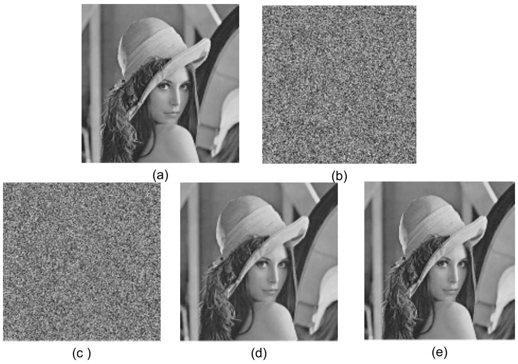


FIGURE 7. Experiment for the image Lena for the single layer embedding (a)Original Lena image; (b)Encrypted image; (c)Embedded encrypted image; (d)Directly decrypted image (PSNR=51.147 dB); (e)Completely recovered original image using the proposed method (where PSNR$\longrightarrow +\infty$ dB, SSIM=1.0).

hiding phase, data hider embeds the additional data into the encrypted image and then permutated. Here, the additional data is a randomly generated bit stream. The permutated marked encrypted image can be visualized in Fig. 7 (c). At the recovery phase, the directly decrypted image can be seen in Fig. 7 (d) with PSNR =51.147 dB. In our proposed method the original image is recovered completely, which can be seen in Fig. 7 (e) having PSNR tends to $+\infty$ dB and SSIM=1.0.

TABLE 1. Performance of proposed scheme with six standard gray-scale images for single layer.

Test image	Maximum ER (bpp)	PSNR (dB) marked	recovered	SSIM
Lena	1.0	51.147	$+\infty$	1
Jetplane	1.0	51.144	$+\infty$	1
Baboon	1.0	51.138	$+\infty$	1
Peppers	1.0	51.140	$+\infty$	1
Man	1.0	51.154	$+\infty$	1
Boat	1.0	51.133	$+\infty$	1
Average	1.0	51.142		1

Next, we have investigated our proposed method on six standard gray-scale images, having size of 512× 512 pixels as shown in the Fig. 6. Table 1 shows the performance of scheme, in terms of maximum embedding capacity for the single layer. The table shows PSNR (without additional data extraction), PSNR and SSIM (for the proposed scheme). It is analyzed from the PSNR and SSIM, that after data extraction and image recovery, our proposed scheme shows the property of complete reversibility.

Furthermore, we have demonstrated our results on multi-layer embedding on the test images shown in Fig. 6. The experimental results are shown in Table 2. It can be seen that up to four layers are used for embedding where the average PSNR of each layer lies between 51.00 and 51.50 dB and the maximum hiding capacity up to four layers is 4 bpp. If the PSNR value is larger than 35 dB, a human eye cannot distinguish between the marked image and the original image. In our proposed scheme, the degradation quality of the directly decrypted images is indistinguishable in the multi-layer even-odd embedding which means additional data can be embedded up to a large extent into an encrypted image without worrying about perceptible image quality of the directly decrypted image. From the fact of encryption technique, the encrypted image is become saturated i.e. the frequency of each pixel values is almost same. Moreover, the saturated encrypted image also shows the same number of even-odd values. In order to embed the encrypted additional information which is also show the saturation after encryption, only modify the approximately 50% of encrypted image pixels. In the result of directly decrypted image PSNR quality is always more than 50 dB. Additionally, applying multi-layer embedding, the resulted marked encrypted image pixel will change the encrypted pixel by approximately 50%. Hence, each layer for embedding, the proposed scheme gives guarantees for the PSNR of directly image is more than 50 dB.

TABLE 2. Performance of proposed scheme of directly decrypted images from layer 1 to layer 4.

Image	Layer 1 PSNR (dB)	ER (bpp)	Layer 2 PSNR (dB)	ER (bpp)	Layer 3 PSNR (dB)	ER (bpp)	Layer 4 PSNR (dB)	ER (bpp)
Lena	51.147	1.0	51.140	2.0	51.143	3.0	51.146	4.0
Jetplane	51.144	1.0	51.142	2.0	51.136	3.0	51.132	4.0
Baboon	51.138	1.0	51.134	2.0	51.137	3.0	51.133	4.0
Peppers	51.140	1.0	51.138	2.0	51.131	3.0	51.134	4.0
Man	51.139	1.0	51.133	2.0	51.121	3.0	51.123	4.0
Boat	51.133	1.0	51.136	2.0	51.138	3.0	51.142	4.0

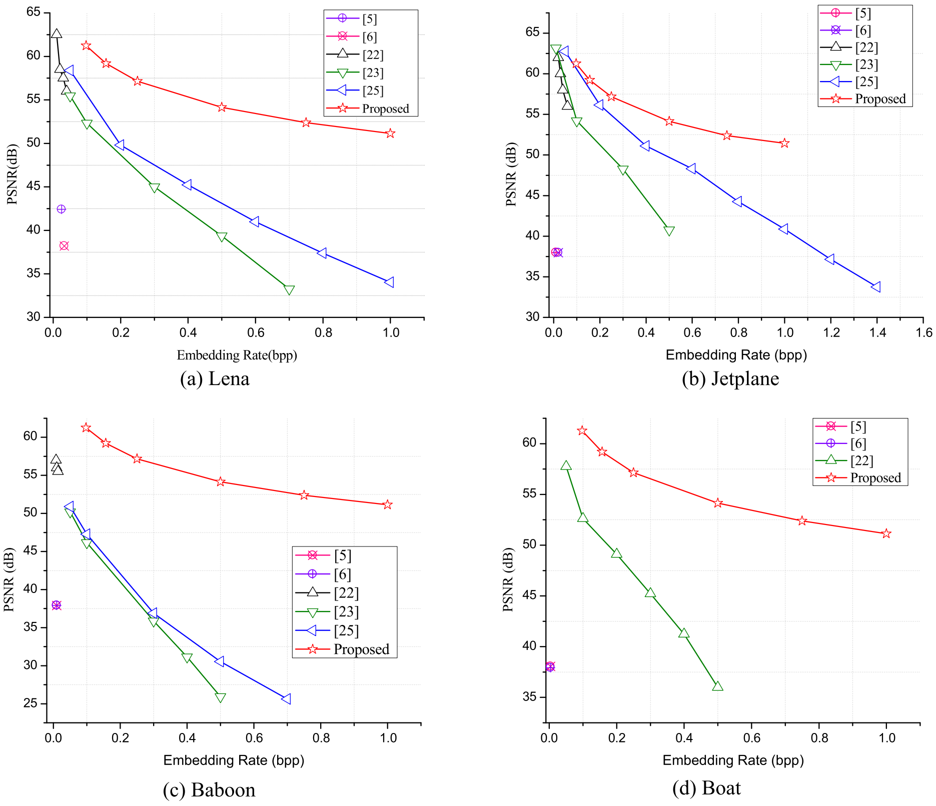
A. COMPARISON WITH THE RELATED SCHEMES

In depth analysis of both VRAE and VRBE is explained in [21]. Both are the methods used for vacating room in RDH-EI schemes for additional data embedding. The proposed scheme is compared in two aspects, with existing schemes following VRAE and VRBE methods like Qian and Zhang [21], Ma *et al.* [22], Xiao *et al.* [53], Puteaux *et al.* [54], Puyang and Puech [55], and Yin *et al.* [56]. These two aspects are evaluated in terms of: 1) maximum embedding capacity and 2) maximum embedding rate. Where, the schemes [22], [53]–[56] are based on VRBE and [21] is based on VRAE. Table 3, shows a high embedding capacity of the scheme [56] which is better than the other existing schemes but with a drawback of high distortion in the directly decrypted image. The technique for embedding additional data in [56] is based on VRBE i.e, applying preprocessing technique to create space for additional data. This technique uses Most Significant Bit (MSB) prediction and Huffman Coding.

In [55], [56], the image quality of the directly decrypted image is given a lesser priority and the original image is recovered completely at the receiver's side after post-processing of marked encrypted image. As compared with schemes [55], [56], our proposed scheme (considering the first layer) have lesser embedding capacity. But in our proposed scheme, when the embedding is done in the subsequent layers (second, third and so on), the overall embedding capacity drastically increases with each subsequent layer as shown in Table 2, without degradation of PSNR of the directly decrypted image,which signifies that our scheme is independent of texture of the original image unlike [54]–[56].

TABLE 3. Comparison of the maximum embedding capacity of our proposed scheme for the first layer with five other existing schemes.

Schemes		Ma [22]	Qian [21]	Xiao [53]	Puteaux [54]	Puyang [55]	Xiang [56]	Proposed
Lena	bits	225,443	77,332	128,974	256,115	303,038	677,118	262,114
	bpp	0.860	0.295	0.492	0.977	1.156	2.583	1.0
Jetplane	bits	241,172	77,332	128,974	257,687	339,214	794,296	262,114
	bpp	0.920	0.295	0.492	0.983	1.294	3.030	1.0
Baboon	bits	112,721	77,332	128,974	219,676	97,518	279,446	262,114
	bpp	0.430	0.295	0.492	0.838	0.372	1.066	1.0
Peppers	bits	212,336	77,332	128,974	254,017	−−	−−	262,114
	bpp	0.810	0.295	0.492	0.969	−−	−−	1.0
Man	bits	−−	77,332	128,974	257,163	301,990	615,776	262,114
	bpp	−−	0.295	0.492	0.981	1.152	2.349	1.0
Boat	bits	207,093	77,332	128,974	257,163	−−	−−	262,114
	bpp	0.790	0.295	0.492	0.981	−−	−−	1.0



(a) Lena

(b) Jetplane

(c) Baboon

(d) Boat

FIGURE 8. Performance comparison with related schemes [5], [6], [22], [23], [25] on four test images: (a) Lena (b) Jetplane (c) Baboon (d) Boat.

Ma *et al.* [22] is VRBE based scheme, where the original image is preprocessed by some existing RDH method, to vacate the space for the data hider. But, the limitation of this scheme is that vacating of space is texture dependent. Xiao *et al.* [53] have used the simplified version of the interpolation technique to create space for the additional data in the image preprocessing phase. In [53] the additional data is embedded into the encrypted image through flipping the MSBs of primarily assigned pixels to achieve a higher embedding capacity than [21]. In [54], the original image is preprocessed to exploit the correlation between two neighboring pixels to predict the MSBs of the pixel. This scheme is able to provide an embedding rate of less than 1 bpp. Our proposed scheme furnishes higher embedding capacity than [22], [53], [54]. Qian and Zhang [21] scheme shares two similarities with our proposed scheme: 1) they are based on VRAE and 2) both are independent of the original image texture. The advantage of our scheme over Qian *et al.* [21] scheme is that for the first layer, the embedding capacity is higher.

Furthermore, we have compared our proposed scheme with schemes [5], [6], [22], [23] and [25] in Fig. 8 which shows the graph of visual quality (PSNR) versus ER, for the directly decrypted image. For comparison, we have generated the results on standard test images *Lena, Jetplane, Baboon, Boat* as shown in Fig. 6. The comparison results in Fig. 8 show that the PSNR of the proposed scheme is higher than the other compared schemes for all the test images. The idea of gaining high PSNR in our proposed scheme is due to the even-odd value characteristic of the encrypted pixel value. The maximum change in the value of any modified pixel is '±1'. This makes it obvious that the distortion of marked media is very less as compared with the existing schemes.

B. SECURITY ANALYSIS

In order to demonstrate the visual security level, we have performed the statistical analysis on the proposed method. We have used well known different statistical metrics: correlations analysis, entropy analysis through Shannons's method, χ^2 test [54], Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI) [57] and PSNR for all the phases to analyze the security of the proposed method.

1) CORRELATIONS ANALYSIS

The metric used for correlation analysis is correlation coefficient (CoC). For a original image CoC is nearly equal to one whereas for encrypted image its value tends to be zero in an ideal condition. CoC of two adjacent pixels can be mathematically expressed as following:

$$CoC_{x,y} = \frac{CoV(x,y)}{\sqrt{V(x) \times V(y)}} \tag{10}$$

$$CoV(x,y) = \frac{1}{s}\sum_{s=1}^{s}(x_i - E(x))(y_i - E(y) \tag{11}$$

$$V(x) = \frac{1}{s}\sum_{s=1}^{N}(x_i - E(x))^2 \tag{12}$$

$$E(x) = \frac{1}{s}\sum_{s=1}^{s}(x_i) \tag{13}$$

where $E(x)$ is the sample mean of x, $V(x)$ is the sample variance of x,$CoV(x,y)$ is the covariance between x and y and s is the sample size.

2) ENTROPY ANALYSIS

$$S(I) = -\sum_{i=0}^{255} P(\beta i)\log_2 P(\beta i) \tag{14}$$

where I is the image with gray level (βi) for i ranging from 0 to 255 and $P(\beta i)$ representing the probability for each gray level. Higher value for Shannon's entropy ensures higher security.

3) CHI SQUARE (χ^2) TEST

$$\chi^2 = 256 \cdot (M \times N)\sum_{i=1}^{255}(P(\beta i) - \frac{1}{256})^2 \tag{15}$$

where χ^2 gives the divergence of the encrypted image from its theoretical image. It must be noted that the theoretical probability of gray level βi $(0 \leq i \leq 255)$ for image is $1/256$.

4) NPCR AND UACI

The number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) tests are used to evaluate any image encryption algorithm against differential attacks. These parameters calculate the amount of pixel change rate for an encrypted image whose original image has undergone a change in just one pixel value. The maximum theoretical value for NPCR and UACI are 100% and 33.33% respectively. The encrypted images, who have these values near to theoretical values, are considered more secure.

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} d(i,j)}{M \times N} \times 100\%, \tag{16}$$

where $d(i,j)$ is

$$d(i,j) = \begin{cases} 1, & \mathit{if} \quad I(i,j) = I'(i,j) \\ 0, & \mathit{else} \end{cases} \tag{17}$$

where I is the encrypted image and I' is the encrypted image after one pixel changed in the original image.

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|I(i,j) - I'(i,j)|}{255} \times 100\%, \tag{18}$$

In Table 4, the correlations for the six standard test images Fig. 6, between the adjacent pixels along the three directions i.e. horizontal, vertical and diagonal for the original, the encrypted and the marked encrypted image are given. The correlations for the original images are higher than those of the encrypted and the marked encrypted images, which tend to be zero.

For the image Lena in Fig. 9, for each of the three stages: original, encrypted and marked encrypted images, correlation can be visualized in the three directions: horizontal Fig. 9($a-c$), vertical Fig. 9($d-f$) and diagonal Fig. 9($g-i$). In terms of entropy, the values obtained for the original test images, have greater difference with the maximum theoretical value 8, when compared with the entropies for the encrypted and the marked encrypted images. This narrow difference in the entropies of encrypted and marked encrypted images ensure the security of our scheme. The chi square (χ^2) values for the original images are far more than the values of the encrypted and the marked encrypted images ensuring higher security to our scheme. Allied to this, NCPR values are closer to theoretical value 100%. Same is the case with UACI,

TABLE 4. Evaluation on the basis of quality of the original, encrypted and marked encrypted images for the six standard gray-scale images with size 512 × 512.

Test image		Correlation horizontal	Correlation vertical	Correlation diagonal	Entropy (bpp)	χ^2 test (square root)	NPCR %	UACI %	PSNR (dB)
Lena	Original image	0.9719	0.9850	0.9593	7.4456	340.6470	/	/	/
	Encrypted image	-0.0027	-0.0004	0.0047	7.9992	17.4290	99.6124	28.7129	9.2035
	Marked encrypted image	-0.0004	-0.0019	0.0037	7.9991	18.4762	99.6082	28.8257	9.1838
Airplane	Original image	0.9676	0.9628	0.9371	6.6776	826.2035	/	/	/
	Encrypted image	0.0042	-0.0223	-0.0007	7.9981	25.8675	99.6052	32.0157	8.1160
	Marked encrypted image	0.0013	-0.0191	-0.0004	7.9981	25.9407	99.5907	32.0137	8.1176
Baboon	Original image	0.8665	0.7586	0.7261	7.3579	396.0794	/	/	/
	Encrypted image	0.0026	-0.0039	0.0023	7.9990	18.5661	99.6227	28.0164	9.4824
	Marked encrypted image	0.0005	-0.0042	0.0042	7.9991	18.0249	99.6174	28.0930	9.4613
Peppers	Original image	0.9792	0.9826	0.9680	7.5715	334.9809	/	/	/
	Encrypted image	-0.0004	-0.0022	0.0003	7.9992	17.0747	99.6262	30.9973	8.4401
	Marked encrypted image	-0.0005	-0.0023	0.0008	7.9991	18.1521	99.6212	30.9221	8.4607
Man	Original image	0.9575	0.9700	0.9437	7.3574	523.6392	/	/	/
	Encrypted image	-0.0007	-0.0095	0.0003	7.9989	20.3773	99.6071	33.8052	7.6555
	Marked encrypted image	0.0029	-0.0076	0.0014	7.9988	20.7918	99.6105	33.8759	7.6436
Boat	Original image	0.9630	0.9787	0.9458	7.1238	602.5528	/	/	/
	Encrypted image	0.0004	-0.0136	-0.0013	7.9987	21.3729	99.6281	29.194551	8.9337
	Marked encrypted image	0.0014	-0.0104	-0.0017	7.9988	21.0985	99.6063	29.4661	8.9272

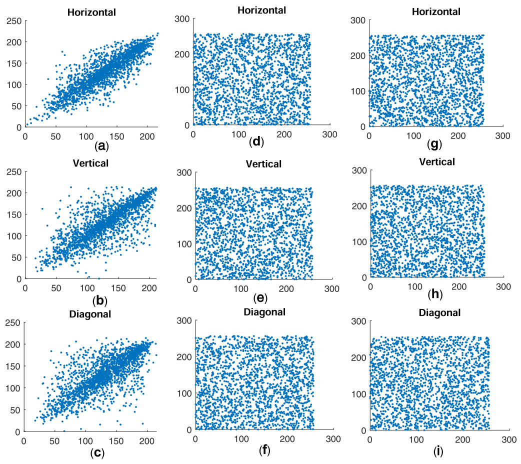


FIGURE 9. Correlation analysis for the three stages of the image Lena: original - (a) horizontal, (b) vertical, (c) diagonal; encrypted - (d) horizontal, (e) vertical, (f) diagonal; and marked encrypted - (g) horizontal, (h) vertical, (i) diagonal.

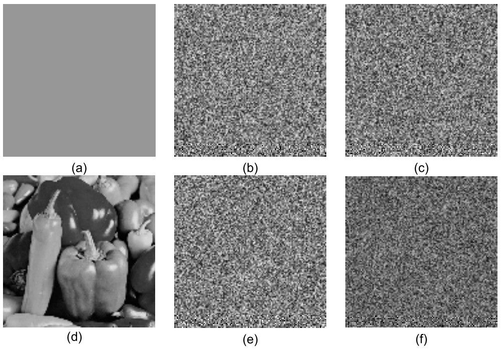


FIGURE 10. The performance of the chosen-plaintext attack: (a) chosen plain-image (I_{150}); (b) encrypted image of I_{150} (E_{150}); (c) the mask image of I_{150} (M_{150}); (d) the peppers image ($I_{peppers}$); (e) the encrypted image of $I_{peppers}$ (f) the recovered peppers image ($R_{peppers}$).

where the results approach the theoretical value 33.33%. These results support the security claim of our scheme. For all the results, in context of PSNR, the values are less than 10 dB supporting the fact that the original images are different from the encrypted and the marked encrypted images. Hence, it can be concluded that our scheme is secure.

C. CHOSEN PLAINTEXT ATTACK

In this subsection, we have applied chosen plaintext attack for the encryption scheme to test whether the encryption function is sufficiently secure. In order to do so, a grayscale image (I_{150}) is constructed which is having size 512 × 512, whose each pixel value fixed 150, which can be visualized in Fig. 10(a). Next, the Fig. 10(b) is the encrypted image (E_{150}) of I_{150}, where encryption key (Key_1). Furthermore, in order to predict the relationship between the plaintext and ciphertext, a mask image is (M_{150}) constructed by taking XOR operation between chosen plaintext and ciptertext ($M_{150} = I_{150} \oplus E_{150}$), the mask image can be visualized in Fig. 10 (c). In order to see the performance of chosen plaintext attack a peppers image ($I_{peppers}$) is chosen as shown in Fig. 10(d) whose encrypted image is $I_{peppers}$ Fig. 10(e). The recovered plain image is calculated by applying the constructed mask image and encrypted image of peppers, which can be calculated by $R_{peppers} = M_{150} \oplus E_{peppers}$ and visualised in Fig. 10(f). From the Fig. 10(f) it can be easily understood that the encryption function with the same key does not disclose any information. Moreover, the chosen encryption scheme has better permutation and diffusion, which makes the encryption scheme secure against the chosen plaintext attack.

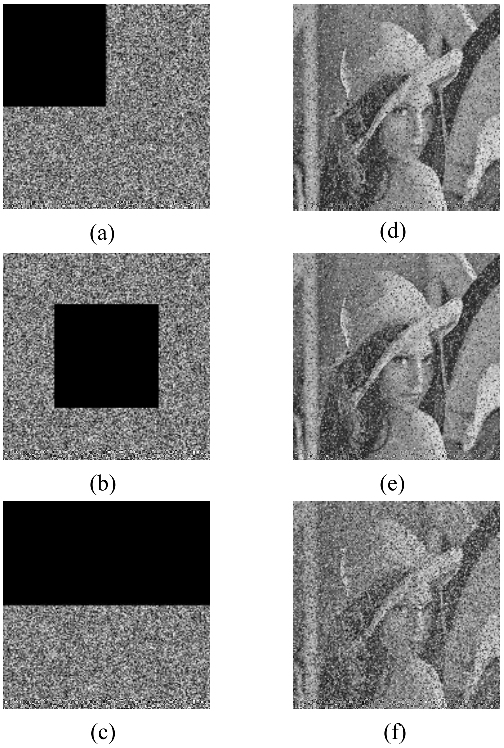


FIGURE 11. Modification of marked encrypted ($a - c$) and the corresponding directly decrypted ($d - f$) images.

D. CROPPING ATTACK

In this subsection, we have considered that if cropping attacker on marked encrypted image after the data hiding phase, the receiver can recover the original image successfully with some distortion. Hence, the scheme survives illegal cropping attack to some extent. Fig. $11(a - c)$ shows the cropping attack in marked encrypted image and Fig. $11(d - f)$ shows the corresponding recovered image. It shows, that even with different levels of cropping during the transmission, the legitimate receiver can decrypt the original image successfully with some level of noise.

V. CONCLUSION

In this study, we proposed a new RDH scheme for the encrypted images, using multi-layer even-odd value embedding technique. We divided the proposed scheme into three basic phases: First phase includes encryption of the original image, embedding the additional data in the data hiding phase has been considered in the second phase, and the last phase describes extraction of the additional data and recovery of the original image. In the first phase, the content owner of the original image encrypts the image by using encryption based on the chaotic behaviour of PWL-memristor. In the second phase, without knowing the original content of the original image, the data hider/service provider embeds the additional data into the encrypted image. In order prevent the perceptual information leakage to the marked encrypted image, permutation operation is applied on the marked encrypted image. In the third phase, after the receiver obtains the permuted marked encrypted image, the receiver must have both the keys along with the auxiliary information to extract the embedded data and recover the image losslessley, i.e. without any distortion.

If the receiver has both of the decryption and the permutation keys, the approximate cover image is recovered. The experimental results show that the proposed scheme achieves reversibility with high embedding capacity. Additionally, the scheme survives cropping attack in the post embedding phase with some distortion in the directly decrypted image. Future work can be done to optimize the size of the axillary information for further improvement of the scheme.

REFERENCES

[1] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U.S. Patent 5 646 997, Jul. 8, 1997. [Online]. Available: https://patentscope.wipo.int/search/en/detail.jsf;jsessionid=D4DCB9F1192E9572ED45918C47F043A5.wapp2nC?docId=US39264989&recNum=146&office=&queryString=&prevFilter=%26fq%3DICF_M%3A%22H04L%22%26fq%3DDP%3A2000&sortOption=Relevance&maxRec=16361

[2] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] 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.

[4] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," *Proc. SPIE*, vol. 4314, pp. 197–208, Aug. 2001. [Online]. Available: https://doi.org/10.1117/12.435400

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

[6] 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.

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

[8] V. Sachnev, H. Joong Kim, J. Nam, S. Suresh, and Y. Qing Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[9] Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 2, pp. 250–260, Feb. 2009.

[10] L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2082–2090, Dec. 2005.

[11] J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in *Proc. 5th Int. Workshop Digit. Watermarking (IWDW)* in Lecture Notes in Computer Science, vol. 4283. Berlin, Germany: Springer, 2006, pp. 348–361. [Online]. Available: https://doi.org/10.1007/11922841_28

[12] K.-L. Chung, Y.-H. Huang, W.-N. Yang, Y.-C. Hsu, and C.-H. Chen, "Capacity maximization for reversible data hiding based on dynamic programming approach," *Appl. Math. Comput.*, vol. 208, no. 1, pp. 284–292, Feb. 2009.

[13] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Process.*, vol. 93, no. 1, pp. 198–205, Jan. 2013.

[14] 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.

[15] Y. L. Chen, H. Wang, Y. Hu, and A. Malik, "Intra-frame error concealment scheme using 3D reversible data hiding in mobile cloud environment," *IEEE Access*, vol. 6, pp. 77004–77013, 2018.

[16] Y. Chen, H. Wang, H.-Z. Wu, Z. Wu, T. Li, and A. Malik, "Adaptive video data hiding through cost assignment and STCs," *IEEE Trans. Depend. Sec. Comput.*, early access, Aug. 5, 2019, doi: 10.1109/TDSC.2019.2932983.

[17] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, Nov. 2018.

[18] C. Li, D. Lin, B. Feng, J. Lu, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[19] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, p. 399, Sep. 2018.

[20] 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.

[21] 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.

[22] 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.

[23] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Process.*, vol. 94, pp. 118–127, Jan. 2014.

[24] D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Process.*, vol. 123, pp. 9–21, Jun. 2016.

[25] 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.

[26] F. Huang, J. Huang, and Y.-Q. Shi, "New framework for reversible data hiding in encrypted domain," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2777–2789, Dec. 2016.

[27] R. Geetha and S. Geetha, "Multi-layered 'odd-even' reversible embedding for encrypted images," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1S3, pp. 347–351, 2019. [Online]. Available: https://www.ijeat.org/wp-content/uploads/papers/v9i1s3/A10651291S319.pdf

[28] 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, Nov. 2018.

[29] Z.-L. Liu and C.-M. Pun, "Reversible data-hiding in encrypted images by redundant space transfer," *Inf. Sci.*, vols. 433–434, pp. 188–203, Apr. 2018.

[30] A. Malik, H. Wang, H. Wu, and S. M. Abdullahi, "Reversible data hiding with multiple data for multiple users in an encrypted image," *Int. J. Digit. Crime Forensics*, vol. 11, no. 1, pp. 46–61, Jan. 2019.

[31] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Process.*, vol. 153, pp. 109–122, Dec. 2018.

[32] C. Qin, Q. Zhou, F. Cao, J. Dong, and X. Zhang, "Flexible lossy compression for selective encrypted image with image inpainting," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 11, pp. 3341–3355, Nov. 2019.

[33] Z. Qian, H. Xu, X. Luo, and X. Zhang, "New framework of reversible data hiding in encrypted JPEG bitstreams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 351–362, Feb. 2019.

[34] J. Qin and F. Huang, "Reversible data hiding based on multiple two-dimensional histograms modification," *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 843–847, Jun. 2019.

[35] K. Chen and C.-C. Chang, "Error-free separable reversible data hiding in encrypted images using linear regression and prediction error map," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31441–31465, 2019.

[36] H. Wu, F. Li, C. Qin, and W. Wei, "Separable reversible data hiding in encrypted images based on scalable blocks," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 25349–25372, Sep. 2019, doi: 10.1007/s11042-019-07769-w.

[37] H.-Z. Wu, Y.-Q. Shi, H.-X. Wang, and L.-N. Zhou, "Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 8, pp. 1620–1631, Aug. 2017.

[38] 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.

[39] Y.-C. Chen, C.-W. Shiu, and G. Horng, "Encrypted signal-based reversible data hiding with public key cryptosystem," *J. Vis. Commun. Image Represent.*, vol. 25, no. 5, pp. 1164–1170, Jul. 2014.

[40] A. Malik, H.-X. Wang, Y. Chen, and A. N. Khan, "A reversible data hiding in encrypted image based on prediction-error estimation and location map," *Multimedia Tools Appl.*, vol. 79, nos. 17–18, pp. 11591–11614, Jan. 2020, doi: 10.1007/s11042-019-08460-w.

[41] 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.

[42] A. N. Khan, M. Y. Fan, M. I. Nazeer, R. A. Memon, A. Malik, and M. A. Husain, "An efficient separable reversible data hiding using paillier cryptosystem for preserving privacy in cloud domain," *Electronics*, vol. 8, no. 6, p. 682, Jun. 2019.

[43] D. Xiao, Y. Xiang, H. Zheng, and Y. Wang, "Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism," *J. Vis. Commun. Image Represent.*, vol. 45, pp. 1–10, May 2017.

[44] A. Malik, H. Wang, T. Chen, T. Yang, A. N. Khan, H. Wu, Y. Chen, and Y. Hu, "Reversible data hiding in homomorphically encrypted image using interpolation technique," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102374.

[45] A. Malik, H. Wang, A. N. Khan, Y. Chen, and Y. Chen, "A novel lossless data hiding scheme in homomorphically encrypted images," in *Digital Forensics and Watermarking*, H. Wang, X. Zhao, Y. Shi, H. J. Kim, and A. Piva, Eds. Cham, Switzerland: Springer, 2020, pp. 213–220.

[46] A. N. Khan, M. Y. Fan, A. Malik, and M. A. Husain, "Advancements in reversible data hiding in encrypted images using public key cryptography," in *Proc. 2nd Int. Conf. Intell. Commun. Comput. Techn. (ICCT)*, Sep. 2019, pp. 224–229.

[47] Z. Lin and H. Wang, "Efficient image encryption using a chaos-based pwl memristor," *IETE Tech. Rev.*, vol. 27, no. 4, pp. 318–325, 2010.

[48] C. Li, M. Wei, and J. Yu, "Chaos generator based on a PWL memristor," in *Proc. Int. Conf. Commun., Circuits Syst.*, Jul. 2009, pp. 944–947.

[49] F. Gao and X. Li, "Bitmap encryption study based on chaotic sequences," *J. Beijing Inst. Technol.*, vol. 25, no. 5, pp. 447–450, May 2005. [Online]. Available: http://en.cnki.com.cn/Article_en/CJFDTotal-BJLG200505018.htm

[50] T. Driscoll, H.-T. Kim, B.-G. Chae, M. Di Ventra, and D. N. Basov, "Phase-transition driven memristive system," *Appl. Phys. Lett.*, vol. 95, no. 4, Jul. 2009, Art. no. 043503.

[51] A. Mitra, Y. S. Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," *Int. J. Comput. Sci.*, vol. 1, no. 2, pp. 127–131, 2006.

[52] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[53] D. Xiao, Y. Wang, T. Xiang, and S. Bai, "High-payload completely reversible data hiding in encrypted images by an interpolation technique," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 11, pp. 1732–1743, Nov. 2017.

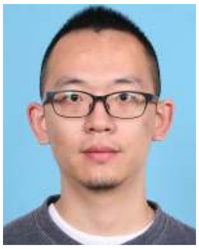
[54] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[55] Y. Puyang, Z. Yin, and Z. Qian, "Reversible data hiding in encrypted images with two-MSB prediction," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2018, pp. 1–7.

[56] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Trans. Multimedia*, vol. 22, no. 4, pp. 874–884, Apr. 2020.

[57] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu.*, vol. 1, pp. 31–38, Apr. 2011.

ASAD MALIK received the B.Sc. degree (Hons.) in computer application from Aligarh Muslim University, in 2012, the master's degree in computer application from Jamia Millia Islamia University, India, in 2015, and the Ph.D. degree from the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2020. His research interests include multimedia forensics and security, image processing, information hiding, and machine learning.



PEISONG HE (Member, IEEE) received the B.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2013, and the Ph.D. degree in cybersecurity from Shanghai Jiao Tong University, Shanghai, China, in 2018. He was working as a Visiting Student with the Rapid-Rich Object Search Laboratory, Nanyang Technological University, Singapore, from 2016 to 2017. In 2019, he joined Sichuan University, Chengdu, China, where he is currently an Assistant Researcher. His current research interest includes multimedia forensics and security.

HONGXIA WANG (Member, IEEE) received the B.S. degree from Hebei Normal University, Shijiazhuang, in 1996, and the M.S. and Ph.D. degrees from the University of Electronic Science and Technology of China, Chengdu, in 1999 and 2002, respectively. She engaged in postdoctoral research work at Shanghai Jiao Tong University, from 2002 to 2004, and worked at the School of Information Science and Technology, Southwest Jiaotong University, from 2004 to 2018. She is currently a Professor with the College of Cybersecurity, Sichuan University, Chengdu. Her research interests include multimedia information security, digital forensics, information hiding, and digital watermarking. She has published 100 peer-research articles and wined ten authorized patents.

AHMAD NEYAZ KHAN received the B.Sc. (Hons.) and master's degrees in computer applications from Aligarh Muslim University, India, in 2009 and 2012, respectively, and the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His research interests include information security, cryptanalysis, and reversible data hiding in encrypted domain.

SAIED PIRASTEH received the Ph.D. degree in geography (GIS, geoanalytics, and LiDAR) from the University of Waterloo, Waterloo, ON, Canada, in 2018, and the Ph.D. degree in geology (remote sensing and GIS) from Aligarh Muslim University, Aligarh, India, in 2004. He is currently holding a professorship position at the Faculty of Geosciences and Environmental Engineering, Southwest Jiaotong University, Chengdu, China. He is also a Senior Research Scientist Collaborator at the Mobile Sensing and Geodata Science Laboratory, University of Waterloo. He is the United Nations Global Geospatial Information Management (UN-GGIM) Academic Network Member. He has been working on integrating AI, ML, computer vision, development of geospatial algorithms, models, software, mobile, and web app in geosciences applications. He is the inventor and the Co-Founder of the Geospatial Infrastructure Management Ecosystem (GeoIME) and Geospatial Rapid Visual Screening (GeoRVS). His research interests include remote sensing and LiDAR data processing and applications in geology, geoenvironmental hazards, and disaster assessment toward implementing UN sustainable development goals (SDGs) 2030.

SANI M. ABDULLAHI (Member, IEEE) received the M.Sc. degree in advanced computer science with specialty in computer security from The University of Manchester, U.K., in 2013, and the Ph.D. degree in information security from the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2019. He is currently with Sichuan Wai Zhimaoyuan IT/Edu Consulting Firm Company, Ltd., Chengdu, China. He has published a number of reputable international journals and conferences, such as the IEEE Transactions on Information Forensics and Security, IEEE AVSS, IWDW, and IWDCF. His research interests include information security, biometrics, digital forensics, multimedia security, and digital watermarking.