International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

Reversible Data Hiding with Multiple Data for Multiple Users in an Encrypted Image

Asad Malik, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

Hongxia Wang, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

Hanzhou Wu, Institute of Automation, Chinese Academy of Sciences (CAS), Beijing, China & State Key Laboratory of Cryptology, Beijing, China

Sani M. Abdullahi, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

ABSTRACT

This article presents a new method which embeds multiple data from multiple users in an encrypted image. Here, the data from several users is embedded into an encrypted image. Initially, the image is encrypted by the owner followed by embedding phase, where the encrypted image is divided into four sets. Two of them are used to embed the secret data, while others are remain unaltered. The secret data from multiple users are embedded into Most Significant Bit (MSB) of the encrypted image using their location maps. In the extraction phase, an individual owner can extract the data from the encrypted image using the assigned private key. Subsequently, in the image decryption and recovery phase, images can be recovered using the unaltered neighbor pixels. However, the secret image can be recovered losslessly using the encryption key only. The proposed scheme allows the extraction of the embedded information only for the authorized user out of several users without knowing the cover information. Various simulations have been made related to this, which show the high embedding rate and accuracy.

KEYWORDS

Cloud Computing, Encrypted Image, Image Recovery, Prediction, Reversible Data Hiding

1. INTRODUCTION

Reversible Data Hiding (RDH) is known as lossless and it is a scheme which is the key element in many applications in the field of secret communication, copyright protection and content authentication of digital multimedia (Barni, Bartolini, Cox, Hernandez, & Perez-Gonzalez, 2001; Tian, Zhao, Ni, Qin, & Li 2013). Reversibility of such scheme means losslessly reconstructing the original image as well as recovering the secret embedded information from the cover media.

Primarily reversible data hiding scheme has been proposed by Barton (1997). After that many other RDH schemes have been proposed and those can be find in the open literature. Mainly these schemes are classified into the following three categories such as lossless compression (Fridrich,

DOI: 10.4018/IJDCF.2019010104

Goljan, & Du, 2001; Celik, Sharma, Tekalp, & Saber, 2005), Difference Expansion (DE) (Tian, 2003; Hu, Lee, & Li, 2009) and Histogram Shifting (HS) (Ni, Shi, Ansari, & Su, 2006; Xuan, Yao, Yang, Gao, Chai, Shi, & Ni, 2006). Lossless compression means to compress the original media losslessly and make the space to embed additional information into it, which can be subsequently recovered losslessly after extraction of embedded data. DE-based embedding idea was initially proposed by Tian (2003) having higher hiding capacity but with a disadvantage as it degrades the quality of recovered image to a large extent. Improvement in the hiding capacity and quality of stego-image can be seen in many successive schemes. Later, several improved techniques for DE-based embedding have come into existence. They include prediction, sorting (Kamstra, & Heijmans, 2005; Sachnev, Kim, Nam, Suresh, & Shi, 2009) and location map reduction (Hu, Lee, & Li, 2009). HS-based scheme was initially proposed by Ni (Ni, Shi, Ansari, & Su, 2006) and proposed the algorithm by them is simpler than DE approach and requires less computation than most of other algorithms. Histogram shifting method uses peak and zero (or maximum and minimum) bins in the histogram of the input image pixel values and then, make the room for data hiding by shifting the bin intensities from peak to zero points. And hiding information has been done by modifying the pixels assuming the peak value. Moreover, HS provides a high visual quality and maintains a high Peak Signal-to-Noise Ratio (PSNR). However, the capacity that Ni's algorithm can provide might not be sufficient for most applications, so many scholars have studied and tried to improve Ni's algorithm. Intensities between the maximum points to raise the hiding capacity is used by (Hwang, Kim, & Choi, 2006), but the threshold of embedding capacity is not sufficient for hiding. Chung, Huang, Yang, Hsu, & Chen (2009) come out with a method used in dynamic programming procedure to maximize histogram shifting to improve the hiding capacity. His method increases capacity indeed, but it has two main drawbacks. It is suitable only for specific types of images. Further it needs much execution time which depends on pair of pixels and zero bins in histogram.

However, Reversible Data Hiding in Encrypted Domain (RDH-ED) is also much popular for secret communication and it has a wide application in cloud computing (Shi, Li, Zhang, Wu, & Ma, 2016). In this technique content owner encrypts the cover media before sending the cover information to the cloud. The cloud owner without knowing original content of the cover media can embed the additional information. At the receivers' side, both additional embedded information and original content of cover media are recovered individually. RDH-ED can be classified into two categories (Shi, Li, Zhang, Wu, & Ma, 2016) as follows. First one is Vacating Room Before Encryption (VRBE) (Ma, Zhang, Zhao, Yu, & Li, 2013), where the content owner performs preprocessing before encryption of cover information. The second one is Vacating Room After Encryption (VRAE) (Zhang, 2011), where the data hider performs operations on encrypted cover information. In Zhang (2011), the original image is encrypted by a stream cipher, after data hider divides the encrypted image into blocks where each block is responsible to carry one bit of information. Flipping, three Least Significant Bits (LSB) of half of the pixels into the encrypted image blocks. Further improvement of this approach (Hong, Chen, & Wu, 2012) uses the side-match scheme to decrease the error rate of extracted bits. Zhang (2012) proposed a separable method where, some part of encrypted bits are responsible to carry the parameters and remaining part in compression by LSB using data hiding key to create space in order to accommodate the additional data. The receiver has three options which are, extracting the additional data with the help of data hiding key, recovering similar image by using encryption key and lastly if the receiver wants to recover original information of cover media without any error using both keys. The proposed scheme (Zhang, 2012) guarantees an error free data extraction but it is not suitable for high payload. Further, Qian (Qian, & Zhang, 2016) improved payload capacity and also shows that the secret data can be embedded into the encrypted image by a histogram modification. After that there are some other schemes that achieved more payload capacity and gain better image quality by using image preprocessing (Zhang, Ma, & Yu, 2014). Recently there are some other works done in the field of RDH-ED (Yin, Luo, & Hong, 2014; Qin, & Zhang, 2015; Xu, & Wang, 2016; Huang, Huang, & Shi, 2016; Wu, Shi, Wang, & Zhou, 2017).

Sharing information with multiple users in encrypted domain can be quite useful in many applications, such as multiparty system or leveled information sharing system, which are quite popular in cloud computing. In multiparty system, each user is concerned about his personal information or relevant information that belongs to him/her. Information embedding into encrypted media by third party for specific user is a very considerable research area in the field of reversible data hiding. A more extensive case could be a situation where the embedding of multiple data for multiple users along with their unique key into single cover media. This extended idea could be used to categorize a group of people in cloud environment.

This paper proposes a novel idea to embed multiple data in encrypted image for multiple users along with their own personal keys. In our proposed method encrypted image is decomposed into four sub-parts in data hiding phase, two of the sub-parts are unchanged, thus used for prediction and other two sub-parts are responsible to carry additional data. These two-sub parts are further divided into the number of users. Each user's data is embedded separately using the corresponding uniquely defined key. Other contribution of this method is to perfectly recover the original image without any distortion by using encryption key.

The rest of this paper is organized as follows. The problem is elaborated in Section 2. Section 3 shows the general framework of the proposed method. Experimental results are shown in Section 4. Section 5 gives the concluding remarks and scope of the future work.

2. MOTIVIATION

In this section, the novel idea of our proposed framework is elaborated. An image is encrypted by content owner and sent to the cloud where the private keys are generated by the cloud and shared through some secure channel for each user. Without knowing any information about original content of the image, the cloud embeds the secret information for the corresponding users by using their private keys. Each user is only authorized to access his information using his private key (independent of other users) without knowing the original content of the image. At last, the image owner can recover the original image without any distortion only by using the embedding key.

The scenario can be suitable for sharing information via cloud for multiple users where each user have his own private key (shared by the cloud), therefore enabling each user to have access only to his own personal information consequently maintaining the security and privacy between users. An illustration of the proposed idea is given in Figure 1. An application of this idea may be seen in near future with the banking systems operating in cloud environment. Here the encrypted data of an account holder can have multiple information embedded into it. But any part of this information can be accessed by any employee of the bank who has been granted the access by the cloud to that particular information.

3. PROPOSED SCHEME

The idea of the proposed novel scheme is divided into four phases: image encryption, data embedding for multiple users, data recovery corresponding to the users, and image reconstruction, as depicted in Figure 2. Initially, cover image is encrypted by stream cipher and sent to the data hiding phase. In the data hiding phase, data $(D_1, D_2, \ldots, D_k)$ are uniquely embedded using unique keys $(Key_1, Key_2, \ldots, Key_k)$ corresponding to each user. In the third phase, each user has his own private key and location map therefore, by using the private key, the user can extract his personal information. The final phase reconstructs the image without any distortion by using encryption key.

In the image reconstruction phase, each user has two choices, either to reconstruct the filtered image with high PSNR value or perfectly reconstruct the original image. The idea of proposed

Figure 1. Illustration of the idea

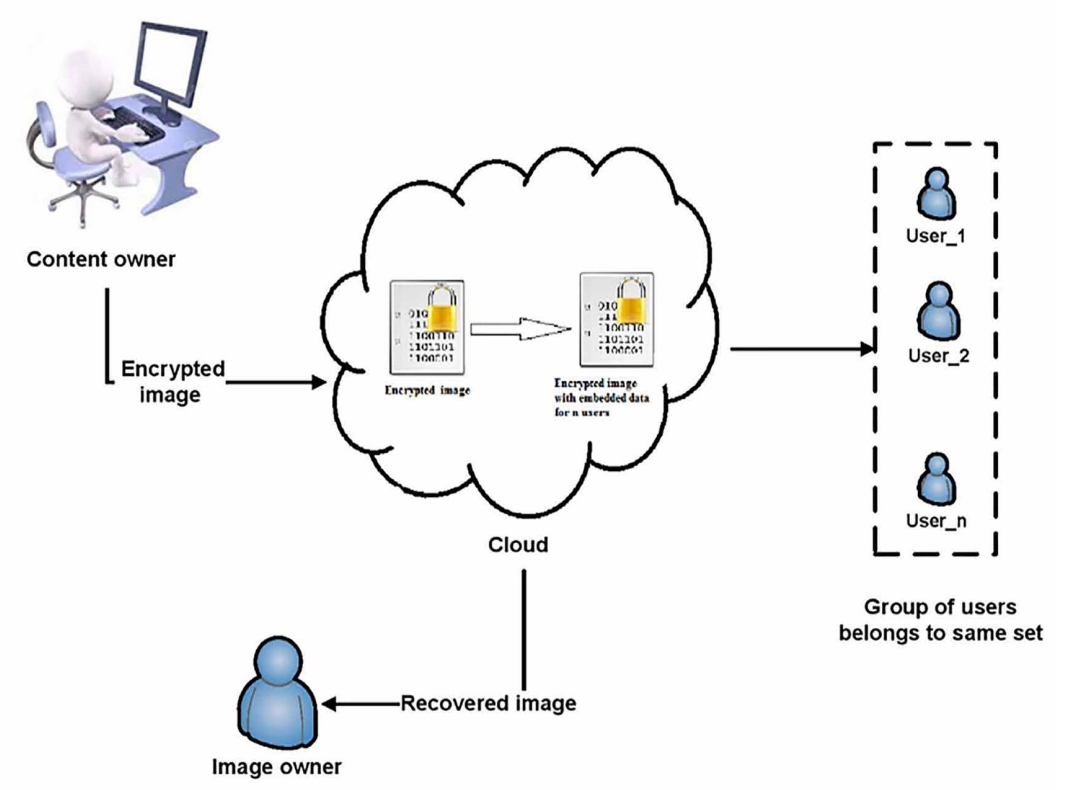
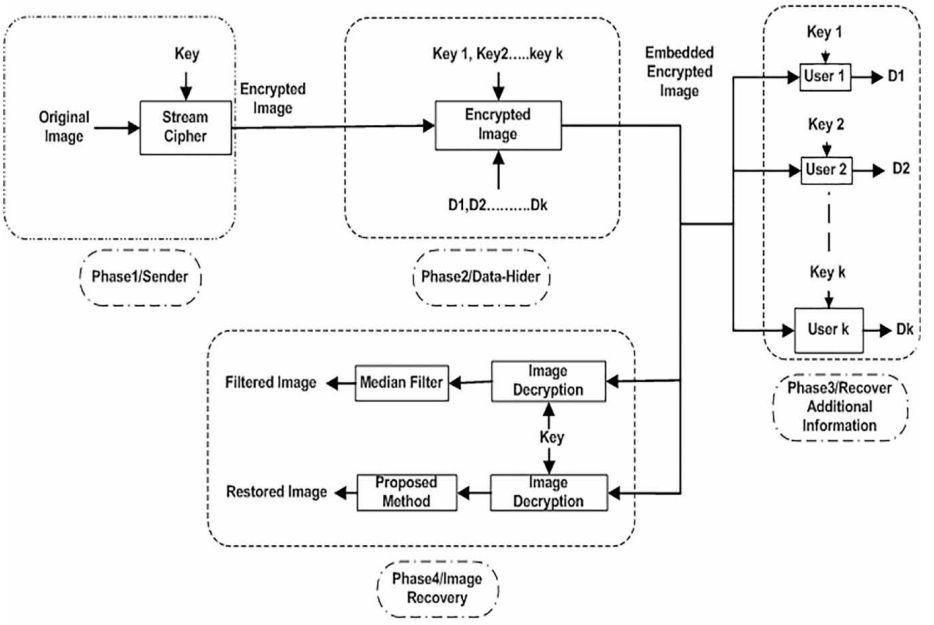


Figure 2. Sketch of proposed scheme



scheme is to embed the additional bit into most significant bits or the second most significant bits into qualified pixel.

3.1. Image Encryption

Assume that original gray scale image has size $M \times N$; each pixel of image falling into [0,255] is represented by 8 bits. The content owner of image changes the original image into plain bits by decomposing each pixel converted into 8 bit by using Equation (1).

$$b_{i,j,u} = \left\lfloor \frac{O_{i,j}}{2^u} \right\rfloor \qquad \text{where } u = 0, 1, 2, \ldots, 7 \tag{1}$$

where $O_{i,j}$ represent the value of pixel at the i^{th} row and j^{th} column from the original image $b_{i,j,u}$, represents each of the 8 bits corresponding to pixel value $O_{i,j}$. Where $1 < i < M$ and $1 < j < N$. The content owner selects the encryption key $k_{i,j,u}$ to generate pseudorandom bit using a stream cipher function, and encrypt the bit stream of the original image by applying XOR operation using Equation (2).

$$e_{i,j,u} = b_{i,j,u} \oplus k_{i,j,u} \qquad \text{where } u = 0,1,2,\ldots,7 \tag{2}$$

where $k_{i,j,u}$ represents the key stream bit, $e_{i,j,u}$ is the generated cipher bit, and $\oplus$ denotes the XOR operation, by the Equation (3) an encrypted version of the original image is generated.

$$E(i,j) = \sum_{u=0}^{7} e_{i,j,u} \times 2^{u-1} \tag{3}$$

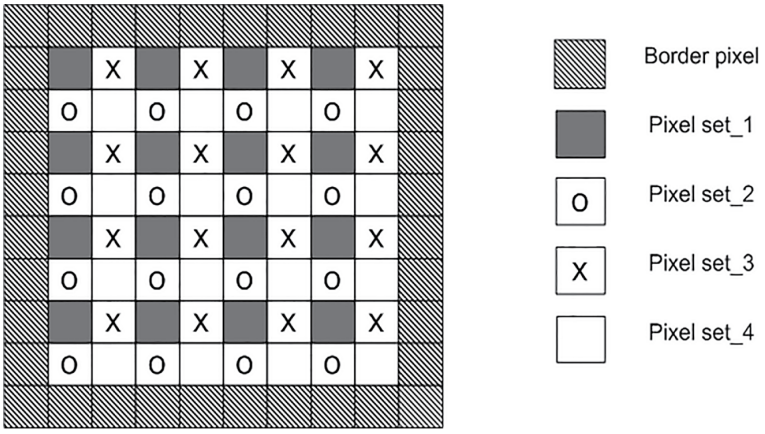
3.2. Data Embedding

In the data embedding phase, for each user, data hider doesn't know about original content of image, before embedding the extra information by the data hider into encrypted version of image, the border pixels are excluded. The remaining pixels are responsible for carrying the additional data. After excluding the border pixels, the remaining pixels of the encrypted image are decomposed into four subsets namely E^1, E^2, E^3, E^4 by using Equation (4).

$$\begin{cases} E^1(i,j) = E(2i-1, 2j-1) \\ E^2(i,j) = E(2i-1, 2j) \\ E^3(i,j) = E(2i, 2j-1) \\ E^4(i,j) = E(2i, 2j) \end{cases} \tag{4}$$

where $i = 1, 2, 3, \ldots, M/2$ and $j = 1, 2, 3, \ldots, N/2$. The decomposition of pixels can be visualized in Figure 3. After the decomposition of the encrypted image, any of the two alternate decomposed sets (E^1 and E^3 or E^2 and E^4) are forbidden to change while the remaining two are qualified pixels which are responsible for carrying the additional data.

Figure 3. Decomposition of pixels



The qualified pixels are further divided into subsets of pixel set as depicted in Equation (5). The number of subset of pixel set is equal to the number of users. This means each user has its location map where the secret information is embedded. The data hider embeds secret information uniquely for individual users with their personal key.

$$S_k = \{i \mid i \bmod D = k\} \tag{5}$$

where $i = 1, 2, 3, \ldots, p$ and p is the size of two decomposed pixel sets, S_k is the set of location assigned to user *k* and *D* is the number of users. According to user's private key, secret bits are encrypted to embed into MSB of the corresponding location map for user *k* as in Equation (6).

$$B_{emb}(d) = B(d) - b * 2^{m-1} + (S_k(d) \oplus P_k(d)) * 2^{m-1} \tag{6}$$

where $B_{emb}(d)$ is the modified encrypted pixel associated with the $d\text{th}$ bit of the additional data. Here m=8 if the secret bit is embedded into first MSB and m=7 if the secret bit is embedded into second MSB, *b* is the MSB of the $B(d)$ pixel. $S_k(d)$ is the secret bits and, $P_k(d)$ is the key for user k, here we assume private key size of each user is equal to secret bit size. At last, bit sequence replaced in encrypted image for user k in order to same sequence of pixels. In the same way, all the user secret information embedded at assigned set of locations pixel.

Example: In the second phase of data embedding for each user, suppose data hider wants to embed the secret information for two users (U_1, U_2) in the encrypted image as shown in Figure 4. Let the encrypted image be of size 7×7 pixels. Our model excludes the border pixels. And remaining pixel will be used to carry the secret information. Further it is divided into four sets, in which two sets namely qualified encrypted pixels will be used for data hiding. The remaining two sets along with the excluded border pixels will be used for prediction during image recovery. Each pixel will be used for hiding one bit of data. Let the qualified encrypted pixels be represented by U_2

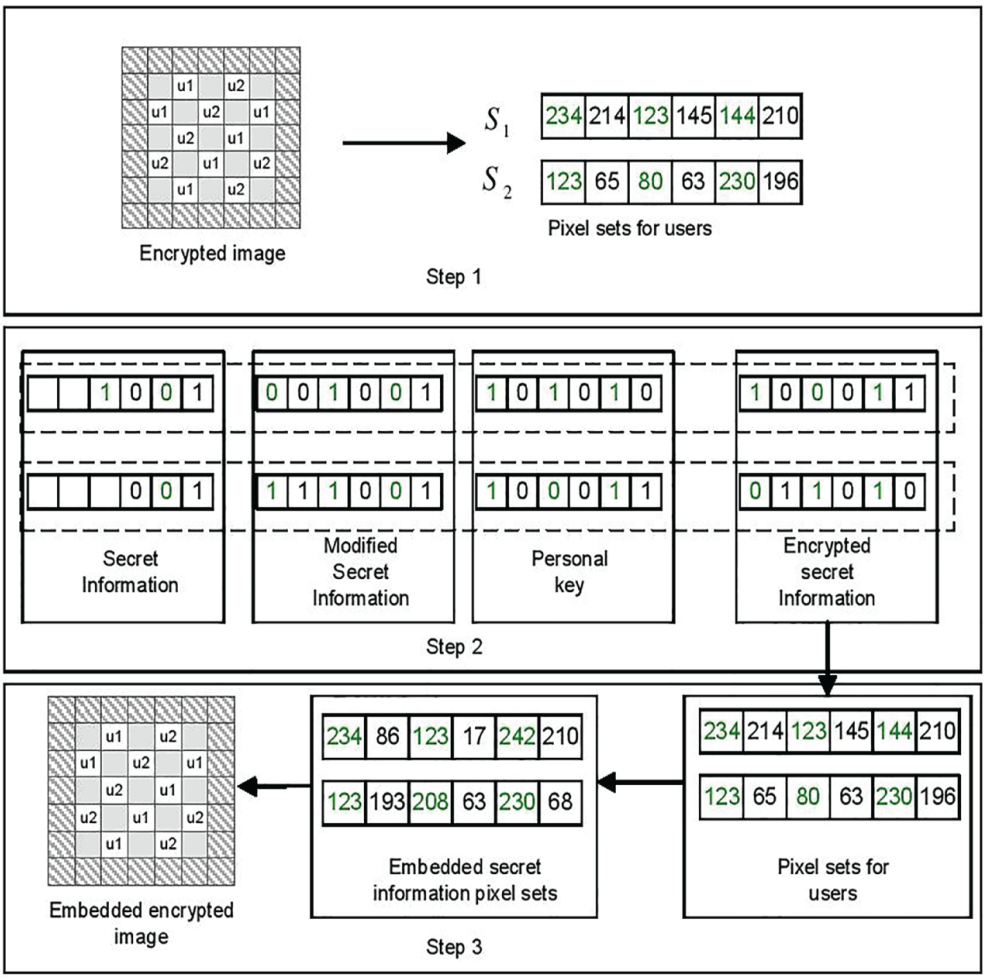
$S_1 = \{ 234, 214, 123, 145, 114, 210 \}$

$S = \{ 34, 123,214, 65, 123, 80, 145, 63, 114, 230, 210, 196 \}.$

According to the proposed scheme, set of qualified pixels are divided into two subsets, and $S_2 = \{ 123, 65, 80, 63, 230, 196 \}$ as shown in Figure 4. Let the secret information for each user be 1001 and 001. Note that the data hider has to modify the secret information according to the number of assigned pixels. This is due to the difference between the original size of secret information and the assigned size for each user. The original size of secret information of U_1 is four, is three and the assigned size for each user is six.

Second step for data hider, the secret information has to be modified according to the assigned location for each user. If the beginning bit of secret information is 0 it has to add ones in the beginning of the secret information and equate its size with assigned size. If the secret information starts with

Figure 4. An example of information embedding for two users



1 it has to add zeros. The new modified secret information for U_1 is 001001 and for U_2 it is 111001. Each user has its own personal key which is generated by data hider at the time of information embedding. Let the generated key for U_1 be 101010 and for U_2 be 100011. Subsequently we apply XOR operation between modified secret information and randomly generated secret key as follows.

$U_1(001001 \oplus 101010 = 100011)$ and $U_2(111001 \oplus 100011 = 011010)$.

Finally, the data hider is ready to embed secret information for each user into the assigned pixels. Embedding is done by replacing the MSB of assigned pixels with modified encrypted secret bit. The encrypted original pixel sets is replaced by the embedded encrypted pixels $S_1 = \{234, 86, 123, 17, 242, 210\}$ and $S_2 = \{123, 193, 208, 63, 230, 68\}$.

3.3. Data Extraction for Each User

In the data extraction phase, each user has it's own private key $P_k(d)$ and location map which is shared by data hider through another private channel and some other parameters like k, D. Initially, with the help of location map each user finds the sets of assigned pixel related to him (for $User_1$ assigned pixels is B_{emb}) where the data has already been embedded independently using parameter *D* and *k*in the embedding phase. The necessary information for each user to extract individual secret data is given in Table 1. Each user needs private key $P_k(d)$ and pixel set location for extracting his individual secret information. Using Equation (7) each user will able to extract the embedded information from pixel set location B_{emb} using its own private key. Here

$$S_k(d) = \left(\left\lfloor \frac{B_{emb}(d)}{2^{(m-1)}} \right\rfloor \bmod 2 \right) \oplus p_k(d), \quad \text{where} \quad 1 < d < L_k \text{ and } 1 \le k \le D \tag{7}$$

where L_k is the size of encrypted bits for user *k*.

Table 1. Necessary information for user to extract embedded data

Users	Personal key	Pixel set for user
$User_1$	$P_1(d)$	$B_{emb}(\text{Pixel set for } User_1)$
$User_2$	$P_2(d)$	$B_{emb}(\text{Pixel set for } User_2)$
$User_3$	$P_3(d)$	$B_{emb}(\text{Pixel set for } User_3)$
⋮	⋮	⋮
$User_D$	$P_D(d)$	$B_{emb}(\text{Pixel set for } User_D)$

3.4. Image Decryption and Recovery

In the image recovery phase, our proposed scheme is based on separable reversible data hiding method. Although there are many methods to recover the original image perfectly but they required both embedding key as well as encrypted key. In our proposed scheme, recovery of image can be made in two different ways with variation in quality, only by using an encryption key. First one gives good quality filtered image and second can perfectly recover original image by using the method (Wu, et al., 2014) which uses embedding of the extra bits into MSB of qualified pixels.

In this phase, the receiver needs to generate $8\ M \times N$ pseudo random bits by using encryption key $k_{i,j,u}$ to generate the key matrix. After that apply XOR operation between corresponding pixels of embedded encrypted image and generated the key matrix to reconstruct the image. This is called directly decrypted image. It already has embedded information. In this directly decrypted image we can improve the image quality by using median filter with good PSNR. In our proposed method we recover the original image perfectly. Here we take the average of four neighbor forbidden pixels by the Equation (8). As we know there exist correlation among neighboring pixels of natural images and by this fact pixels can be predicted accurately. $D_1(i,j)$

$$D_{est}(i,j) = \frac{D_{dec}(i+1,j) + D_{dec}(i-1,j) + D_{dec}(i,j+1) + D_{dec}(i,j-1)}{4} \tag{8}$$

where $D_{est}(i,j)$ and $D_{dec}(i,j)$ are the estimated value and directly decrypted value respectively of the pixel location (i,j). Two possible values are achieved by changing the MSB of targeted pixel, either MSB was changed from 0 or from1. If targeted pixel bit was changed from 0 then the value of pixel must be $D_0(i,j)$ otherwise value calculated in the Equation (9) and Equation (10).

$$D_0(i,j) = D(i,j) - b * 2^{m-1} \tag{9}$$

$$D_1(i,j) = D(i,j) - b * 2^{m-1} + 1 * 2^{m-1} \tag{10}$$

Two prediction errors E_0, E_1 are considerable as calculated in the Equation (11) and Equation (12).

$$E_0 = \left| D_0(i,j) - D_{est}(i,j) \right| \tag{11}$$

$$E_1 = \left| D_1(i,j) - D_{est}(i,j) \right| \tag{12}$$

Minimal prediction error $D_{\min}(i,j)$ is favorable to be chosen as in Equation (13). To recover the original image, we replace the determined pixel $D_{\min}(i,j)$ directly into decrypted image.

$$D_{\min}(i,j) = \begin{cases} D_0(i,j), & if\ E_0 < E_1 \\ D_1(i,j), & if\ E_0 \geq E_1 \end{cases} \tag{13}$$

4. EXPERIMENTAL RESULTS

This section explains about the experimental results obtained by the proposed scheme. Two common parameters viz. bit per pixel (bpp) and Peak Signal to Noise Ratio (PSNR) are considered for analyzing the performance. The distortion has been measured by PSNR and accordingly the formulation of PSNR is given as

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}(dB) \tag{14}$$

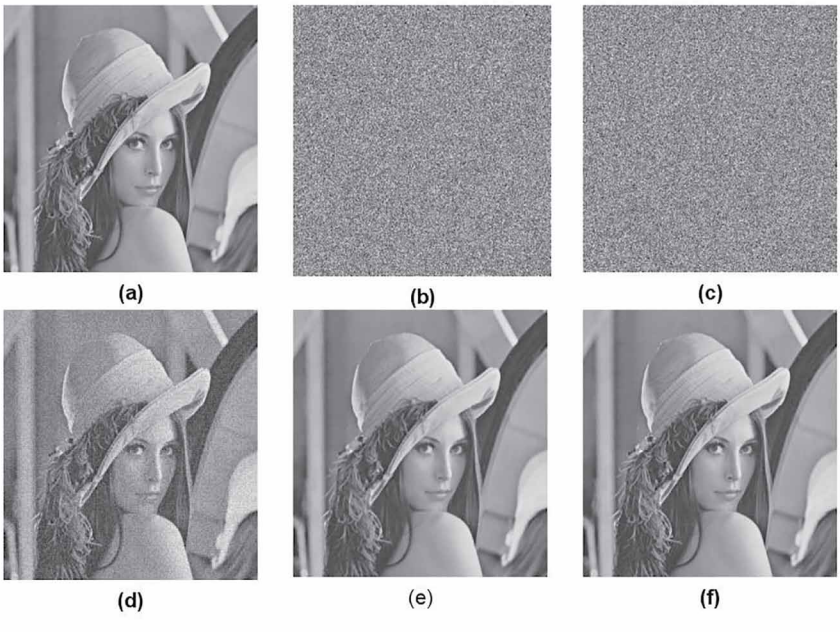
where

$$MSE = \frac{1}{N \times M} \sum_{I=0}^{N-1} \sum_{j=0}^{M-1} (O_{i,j} - R_{i,j})^2 \text{ and } dB \text{ is defined as decibel.} \tag{15}$$

In the above expression $O_{i,j}$ and $R_{i,j}$ denote the original image and the recovered image at pixel location (i, j) respectively. If one has obtained a large value of PSNR then it shows that the constructed image is of high quality.

Two separate experiments have been conducted to validate the present scheme. Accordingly, in the first experiment standard grayscale image of Lena with size 512×512 pixel has been considered as shown in Figure 5(a). It has taken as the main test image to understand the proposed scheme. In the initial phase the image has been encrypted by the stream cipher as given in Figure 5(b) and after that it has been sent for the data hider phase. In the data hider phase, data hider embeds the extra

Figure 5. Experiment for Lena image (TIF Format): (a) Original Lena image; (b) Encrypted image;(c) Embedded encrypted image; (d) Directly decrypted image with PSNR=18.1000; (e) Recovered image using median filter;(f) Recovered image using proposed method



information into the encrypted image according to the users, which can be visualized in Figure 5(c). Next, reconstruction phase has been conducted and in this phase the image has been directly decrypted and the obtained results are shown in Figure 5(d). Using median filter on the directly decrypted image one can obtain the Figure 5(e). Finally, the complete original image has been recovered as depicted in Figure 5(f).

In the detailed outcome, the total number of embedding capacity is divided into the number of users. And each user has limited space in encrypted domain to embed the extra bits. There are two conditions to embed the extra information into the assigned pixel location. In the first condition, each user has same size of information for the assigned locations whereas inthe second condition the users have different size of information. In the second case padding with the sequence of zero or one has been made with respect tothe first bit of bit string. Compensation has been made to equate the number of bits in the bit string to the number of bits in the assigned bits location. If the first bit of extra information is 0 then padding with the 1s at the beginning of the sequence has to be made to equalize the bits size. However, if the bit starts from 1, padding with 0s at the beginning of the sequence has to be made to equate the bitssize. This phenomenon can be visualized from Table 2. Let the size of image be (512×512) pixels. It means total embedding capacity of the image is 130050 bits after excluding border pixels. Let's suppose the experiment is based on two users viz. $User_1$ and $User_2$. And their maximum embedding capacity size can be considered as l_1 and l_2 where $l_1 = l_2 = 6500$ bits. Each user has different embedding key to embed bits, with embedding rate 0.4959 bits per pixel (bpp).

Next the second experiment is based on the proposed separable method. Here a comparison has been made with (Wu, & Sun, 2014) for the validation of the proposed scheme. Wu (Wu, & Sun, 2014) performed the experiment considering the airplane image to embed 40,960 bits by separable method with embedding rate 0.1563bpp and the obtained result is shown in Figure 6(a).

His experiment shows that if the user has only encryption key then the resultant image look like original image with PSNR=32.38dB. Wu (Wu, & Sun, 2014) requires both the embedding and encryption keys to recover the original image without any error. Here it is worth mentioning that using the proposed method we have obtained exactly the same result as Wu (Wu, & Sun, 2014). However, in the present method rather than using both the embedding and encryption keys, only one key i.e. encryption key has been used to recover the original image without any error. Moreover, the performance has been compared with different methods for maximum embedding rate with lossless recovery as shown in Figure 7.

Further the proposed method has been investigated using 10 different standard gray scale images as shown in Figure 8 with highest embedding capacity of image size 512×512 pixels. In Table 3 maximum embedding capacity, PSNR without filter, PSNR using median filter and PSNR with proposed scheme have been shown. A detailed comparison has been made with different existing methods considering various features and the obtained results are given in Table 4. From the results it can be concluded that the proposed method perfectly reconstruct the original image without the embedding for multiple users.

Table 2. An example of bit sequence modification

Original bit sequence		Modified bit sequence	
$User_1$	$User_2$	$User_1$	$User_2$
01001110	10101000	……11101001110	…..00010101000

Figure 6. Experiment for airplane image (TIF Format): (a) original airplane image; (b) Encrypted image;(c) Embedded encrypted image; (d) Directly decrypted image with PSNR=18.0975; (e) Recovered image using median filter;(f) Recovered image using proposed method

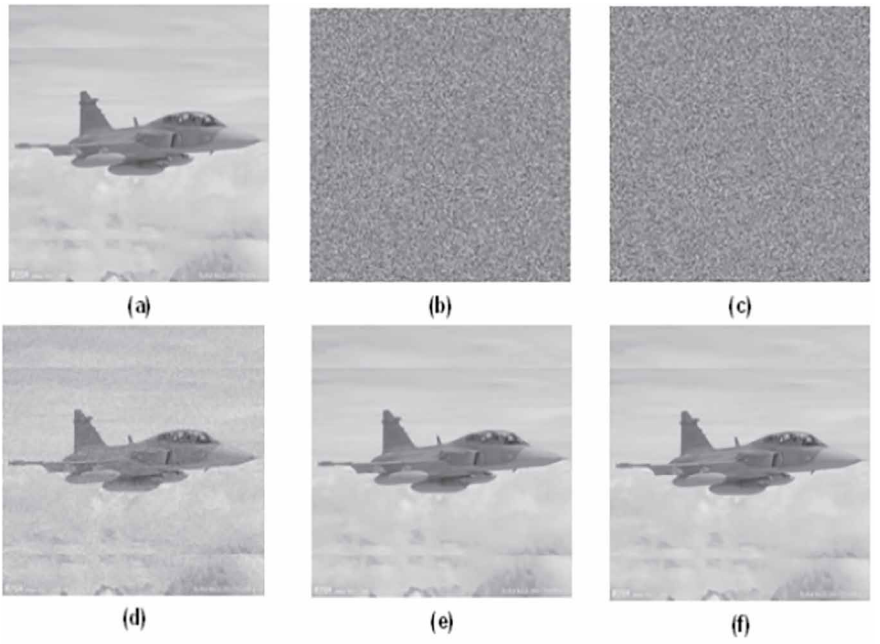


Figure 7. The performance comparison of maximum embedding rate with lossless recovery different methods

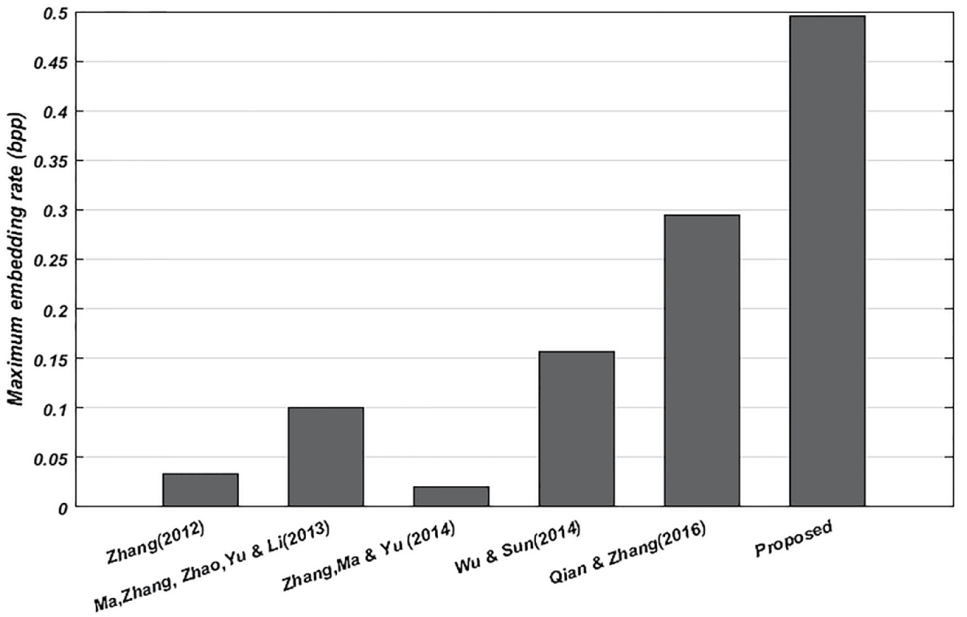


Figure 8. Test images used in the experiment

Table 3. Performance analysis of proposed method ten different 512 x 512 standard test images

Test image	Embedding frame size	Embedding capacity (bits)	Maximum embedding rate(bpp)	PSNR without filter	PSNR with filter	PSNR of proposed scheme
Lena	510*510	130050	0.4960	18.1000	37.2264	Infinity (i.e. .lossless)
Splash	510*510	130050	0.4960	18.0257	37.4902	Infinity (i.e. .lossless)
Plane	510*510	130050	0.4960	18.0975	38.0475	Infinity (i.e. .lossless)
Peppers	510*510	130050	0.4960	18.0795	33.7314	Infinity (i.e. .lossless)
Brain	510*510	130050	0.4960	18.0895	38.8709	Infinity (i.e. .lossless)
Boat	510*510	130050	0.4960	18.0935	36.6686	Infinity (i.e. .lossless)
Baboon	510*510	130050	0.4960	18.0563	24.5433	Infinity (i.e. .lossless)
Camera man	510*510	130050	0.4960	18.0056	35.3623	Infinity (i.e. .lossless)
Goldhill	510*510	130050	0.4960	18.0616	31.0916	Infinity (i.e. .lossless)
Lung	510*510	130050	0.4960	18.0916	37.0341	Infinity (i.e. .lossless)

5. CONCLUSION

In this paper a novel scheme has been proposed which is able to embed multiple data for multiple users in an encrypted image with high embedding capacity. Here the present technique has been developed based on separable method. The integral phases of this scheme include image encryption, data embedding, data extraction and image recovery. In image encryption phase, image is encrypted

Table 4. Comparisons to related work

Functionality / Method	Separable	Image preprocessing	Embedding multiple data	Perfect recover without embedding key
Proposed Method	Yes	No	Yes	Yes
Wu, & Sun, (2014)	No	No	No	No
Wu, & Sun, (2014) (Separable approach)	Yes	No	No	No
Zhang, (2011)	No	No	No	No
Hong, Chen, & Wu, (2012)	No	No	No	No
Zhang, (2012)	Yes	No	No	No
Ma, Zhang, Zhao, Yu, & Li, (2013)	Yes	Yes	No	No
Zhang, Ma, & Yu, (2014)	Yes	Yes	No	No
Qian, & Zhang, (2016)	Yes	No	No	No

by stream cipher and sent to data hider (cloud) to embed additional bits into the MSB of the assigned location map, corresponding to each user with their private key. In data extraction phase, using private key and location map, user can extract the additional data. In the image recovery phase, image owner can reconstruct the original image just only using the encryption key. Various observations have been made by applying the present scheme. Also a comparison has been made with the existing works. From the results one can find the present scheme gives high embedding capacity and high accuracy image recovery. However it is worth mentioning that there is always some scope of improvement and presently the authors are working in these directions. Hence the future work aims to improve the present scheme by assigning the location map dynamically for each user and one can try to improve the payload capacity.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (NSFC) under the grant No. U1536110

REFERENCES

Barni, M., Bartolini, F., Cox, I. J., Hernandez, J., & Perez-Gonzalez, F. (2001). Digital watermarking for copyright protection: A. communications perspective. *IEEE Communications Magazine*, *39*(8), 90–91. doi:10.1109/MCOM.2001.940043

Barton, J. M. (1997). U.S. Patent No. 5,646,997. Washington, DC: U.S. Patent and Trademark Office.

Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing*, *14*(2), 253–266. doi:10.1109/TIP.2004.840686 PMID:15700530

Chung, K. L., Huang, Y. H., Yang, W. N., Hsu, Y. C., & Chen, C. H. (2009). Capacity maximization for reversible data hiding based on dynamic programming approach. *Applied Mathematics and Computation*, *208*(1), 284–292. doi:10.1016/j.amc.2008.10.066

Fridrich, J. J., Goljan, M., & Du, R. (2001). Invertible authentication. *Security and Watermarking of Multimedia Contents*, *3*, 197–208. doi:10.1117/12.435400

Hong, W., Chen, T. S., & Wu, H. Y. (2012). An improved reversible data hiding in encrypted images using side match. *IEEE Signal Processing Letters*, *19*(4), 199–202. doi:10.1109/LSP.2012.2187334

Hu, Y., Lee, H. K., & Li, J. (2009). DE-based reversible data hiding with improved overflow location map. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(2), 250–260. doi:10.1109/TCSVT.2008.2009252

Huang, F., Huang, J., & Shi, Y. Q. (2016). New Framework for Reversible Data Hiding in Encrypted Domain. *IEEE Transactions on Information Forensics and Security*, *11*(12), 2777–2789. doi:10.1109/TIFS.2016.2598528

Hwang, J., Kim, J., & Choi, J. (2006). A reversible watermarking based on histogram shifting. In *Digital Watermarking* (pp. 348-361).

Kamstra, L., & Heijmans, H. J. (2005). Reversible data embedding into images using wavelet techniques and sorting. *IEEE Transactions on Image Processing*, *14*(12), 2082–2090. doi:10.1109/TIP.2005.859373 PMID:16370461

Ma, K., Zhang, W., Zhao, X., Yu, N., & Li, F. (2013). Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Transactions on Information Forensics and Security*, *8*(3), 553–562. doi:10.1109/TIFS.2013.2248725

Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, *16*(3), 354–362. doi:10.1109/TCSVT.2006.869964

Qian, Z., & Zhang, X. (2016). Reversible data hiding in encrypted images with distributed source encoding. *IEEE Transactions on Circuits and Systems for Video Technology*, *26*(4), 636–646. doi:10.1109/TCSVT.2015.2418611

Qin, C., & Zhang, X. (2015). Effective reversible data hiding in encrypted image with privacy protection for image content. *Journal of Visual Communication and Image Representation*, *31*, 154–164. doi:10.1016/j.jvcir.2015.06.009

Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(7), 989–999. doi:10.1109/TCSVT.2009.2020257

Shi, Y. Q., Li, X., Zhang, X., Wu, H. T., & Ma, B. (2016). Reversible data hiding: Advances in the past two decades. *IEEE Access: Practical Innovations, Open Solutions*, *4*, 3210–3237. doi:10.1109/ACCESS.2016.2573308

Tian, H., Zhao, Y., Ni, R., Qin, L., & Li, X. (2013). LDFT-based watermarking resilient to local desynchronization attacks. *IEEE Transactions on Cybernetics*, *43*(6), 2190–2201. doi:10.1109/TCYB.2013.2245415 PMID:23757528

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(8), 890–896. doi:10.1109/TCSVT.2003.815962

Wu, H. Z., Shi, Y. Q., Wang, H. X., & Zhou, L. N. (2017). Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification. *IEEE Transactions on Circuits and Systems for Video Technology*, *27*(8), 1620–1631. doi:10.1109/TCSVT.2016.2556585

Wu, X., & Sun, W. (2014). High-capacity reversible data hiding in encrypted images by prediction error. *Signal Processing*, *104*, 387-400.

Xu, D., & Wang, R. (2016). Separable and error-free reversible data hiding in encrypted images. *Signal Processing*, *123*, 9–21. doi:10.1016/j.sigpro.2015.12.012

Xuan, G., Yao, Q., Yang, C., Gao, J., Chai, P., Shi, Y. Q., & Ni, Z. (2006, November). Lossless data hiding using histogram shifting method based on integer wavelets. In IWDW (pp. 323-332). doi:10.1007/11922841_26

Yin, Z., Luo, B., & Hong, W. (2014). Separable and error-free reversible data hiding in encrypted image with high payload. *The Scientific World Journal*. PMID:24977214

Zhang, W., Ma, K., & Yu, N. (2014). Reversibility improved data hiding in encrypted images. *Signal Processing*, *94*, 118–127. doi:10.1016/j.sigpro.2013.06.023

Zhang, X. (2011). Reversible data hiding in encrypted image. *IEEE Signal Processing Letters*, *18*(4), 255–258. doi:10.1109/LSP.2011.2114651

Zhang, X. (2012). Separable reversible data hiding in encrypted image. *IEEE Transactions on Information Forensics and Security*, *7*(2), 826–832. doi:10.1109/TIFS.2011.2176120

Asad Malik is currently working as a PhD Scholar at the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan, China since 2015. He has received his Master degree in Computer Application from the Department of Computer Science, Jamia Millia Islamia University, New Delhi, India in the year 2015. His research interests include in the area of information security, reversible data hiding and image processing.

Hongxia Wang received the BS degree from Hebei Normal University, Shijiazhuang, in 1996, and the MS and PhD degrees from University of Electronic Science and Technology of China, Chengdu, in 1999 and 2002, respectively. She pursued postdoctoral research work in Shanghai Jiao Tong University from 2002 to 2004. Since September 2013, she has been a visiting scholar at Computer Science Department of Northern Kentucky University in USA. Currently, she is a professor with School of Information Science and Technology, Southwest Jiaotong University, Chengdu. Her research interests include multimedia information security, digital forensics, information hiding and digital watermarking. She has published 100 peer research papers and wined 9 authorized patents.

Hanzhou Wu is currently with the Institute of Automation, Chinese Academy of Sciences. He received his PhD degree from the Southwest Jiaotong University (China) in 2017 and was once a visiting scholar at the New Jersey Institute of Technology (USA) for two years. His research interests include reversible watermarking, steganography, steganalysis, multimedia forensics and machine learning applications. He has published around 20 research papers. He serves as a reviewer for several peer journals such as IEEE Transactions on Information Forensics and Security, IEEE Communication Letters, IET Image Processing, Security and Communication Networks, Journal of Visual Communication and Image Representation and so on.

Sani M. Abdullahi is currently a PhD student at the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China. He received his BSc in Computer Science from Usman Dan Fodio University, in 2009 and his MSc in Advanced Computer Science with Specialty in Computer Security from The University of Manchester, UK, in 2013. His research interests include Information Security, Biometrics, Multimedia Security and Digital watermarking.