IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-12, May 2019 E-ISSN: 2347-2693

"Separable Reversible Data Hiding using XOR and Permutation Encryption in Image"

Reysh Chandrikapure[1*], Pranjal Dhore[2], Nisha Balani[3]

[1,2,3]M. Tech , Department. of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Available online at: www.ijcseonline.org

Abstract:- To perk up the security as well as the quality of decrypted, recovered images, this paper proposes a classification permutation based separable-reversible data hiding in encrypted images. A classification permutation encryption in combination with the XOR-encryption is initially designed to advance the privacy of both pixel-value and pixel location. Then, each bit in the further data is embedded in the most significant bit (MSB) of the encrypted pixels which are indiscriminately chosen based on the data-hiding key in the smooth set. The quality of decrypted and recovered image can be significantly improved by exploiting the spatial correlation as the MSBs of smooth pixels are used to embed the additional data. Results of experimentation exhibit that the quality of decrypted image obtained by the proposed method is superior than to the existing methods. There is 100% probability for lossless recovery from proposed method.

Keywords - separable-reversible data hiding, encrypted images, RDH-EI, classification permutation.

I. INTRODUCTION

Hiding data into digital images and reconstructing the original image completely after the embedded data have been extracted is done indiscernibly using Reversible data hiding (RDH). Reversible data hiding in encrypted images (RDH-EI) is attracting attention with cloud computing emerging. In 2011, based on stream cipher, Zhang proposed a RDH-EI method in which the additional data was hidden by flipping the 3 least significant bits of part of encrypted pixels obtained by the bitwise XOR encryption, and the fluctuation function was designed to deduce the secret data and recover the original image. Given RDH-EI methods are called as the joint RDH-EI given that the data extraction and image recovery are conducted at the same time and needs both the encryption and data-hiding key. Separable RDH-EI is said to be in picture when methods that data extraction and image recovery can be performed separately, and the data extraction in separable RDH-EI needs data-hiding key only.

This separable RDH-EI is divided into two categories. First is pre-processing an original image before encryption to reserve a space for hiding the data. Second is to straight embed the secret data into an encrypted image. In 2012, a separable RDH-EI method was proposed by Zhang, wherein a content-owner encrypts the original image by bitwise exclusive-or operation with an encryption key, and a data-hider may constrict the LSBs of the encrypted image to make a bare space for data to hide. Zhang's method achieves separable between image decryption and data extraction, high quality of decrypted and recovered images, and error free for data extraction. However, it is complicated to recover the original content without any error if the size of additional data is greater than 0.04 bpp (i.e., bit per pixel). To perk up the probability of lossless recovery of recovered image, a separable RDH-EI method based on prediction error was proposed by Wu *et al.*, in which an bonus data was embedded to MSB of encrypted pixels by means of bit replacement, and the original image content was recovered on the basis of prediction error. Method that Wu proposed provides a good visual quality and improved reversibility of recovered image for higher payload embedding. However, there are the following problems existing in Wu's method: [1] Low quality of decrypted image.

[2] Low probability of lossless recovery for a texture image especially. [3] Risks information disclosure. The exclusive-or encryption randomly distributes the encrypted pixels value in the range [0,255], but the position of original pixel is the same.

To solve the above mentioned problems, this paper proposes a separable RDH-EI method which is based on classification permutation. All the pixels in an image are classified as smooth set and unsmooth set. The classification permutation is intended to protect privacy of position of encrypted pixels and make the data-hider easily find smooth pixels without knowing the content of original image. Embedding the additional data is performed by modifying the MSB of the encrypted pixels selected randomly in the smooth set which based on data-hiding key. For obtaining a lossless recovered image, the MSB of each marked pixel is deduced by the unmarked pixels, located in the 3×3 or 5×5 neighbourhood of it.

Investigational results reveal that the visual quality of decrypted image obtained by the proposed method outperforms than that of Zhang's and Wu's method. Also the content of original image can be reconstructed without any error for all tested images.

II. LITERATURE SURVEY

Recently, some reversible marking data hiding had been reported in the literature. Lossless recovery of original image holding embedded data was first invented by Chris W. Honsinger et.al which was carried out in the spatial domain. It uses modulo-256 addition, here eight-bit grayscale images are considered, to embed the hash value of the original image for validation. The embedding formula had both the original and the marked image. The hash function is operated on the original image and on the secret key to get watermarked image. Because of using modulo-256 addition the over or underflow is prevented and the reversibility is achieved. Some annoying salt-and-pepper noise, however, is generated due to possible grayscale value flipping over from 0 to 255 in either direction during the modulo-256 addition.

B. Macq and F. Deweyand developed second reversible marking technique in the transform domain. This is based on a lossless multi-resolution transform and the also on the idea of patchwork. It uses modulo-256 addition. Note that, no experimental results for this technique have been reported till date.

J. Fridrichet.al talked about a spatial domain technique that losslessly compresses some selected bit plane(s) to leave space for data embedding. Because the necessary book-keeping data are also embedded in the cover image as an overhead, the method is reversible.
Since these techniques are aimed at authentication; the amount of hidden data is narrow. The capacity of method that is based on the idea of patchwork and modulo-256 addition is also limited apart from that the hidden data exhibit some robustness against high quality JPEG compression. Since it uses modulo-256 addition, it also exhibits salt-and-pepper noise. As a result, the use of this technique is limited towards applications. This inspection is valid to all lossless data hiding algorithms that are using modulo-256 addition to gain reversibility.

M. Goljan et.al stated the first reversible marking technique that is appropriate for large amount of data hiding. This technique initially segments an image into non-overlapping blocks, and then brings in a discriminating function to categorize these blocks into three groups: Regular (R), Singular (S), and Unusable (U). It further commences a flipping operation, which can alter an R-block to an S-block and vice versa. A U-block remains as it is after the flipping operation. By assigning, say, binary 1 to an R-block and binary 0 to an S-block, all R- and S-blocks are scanned in a selected chronological order, resulting in a biased binary sequence meaning that the binary numbers of 1 and 0 are imbalanced. This biased binary sequence is losslessly compressed to provide some space for data embedding and the compressed bit sequence is embedded into the image as an overhead for later reconstruction of the original image. In data embedding, the R-block and S-block are examined once again and the flipping operation is applied whenever essential to make the changed R-block and S-block sequence coincident with the data to be embedded followed by the overhead data mentioned above.

While it is doing well in reversible data hiding, the payload is still not enough for some applications. Specifically, the embedding capacity approximate ranges from 3 to 41 kb for a 512x512x8 cover grayscale image when the embedding amplitude is 4 (the estimated average PSNR of the marked image vs. the original image is 39 dB).

To increase the payload dramatically, a new lossless data hiding technique based on IWT i.e., integer wavelet transform (a 2^{nd} generation wavelet transform, which has avoided round-off errors) was developed. Because of the superior de-correlation capability of wavelet transform, the selected bit plane compression of IWT coefficients in high frequency sub bands produces larger space for data hiding, resulting in a 2-5 times payload. Particularly, its payload ranges from 15 to 94 kb for a 512x512x8 grayscale image at the same (39 dB) PSNR of the marked images in comparison with the original image. To achieve reversible data hiding, a histogram modification is applied in its pre-processing to put off over or underflow. This histogram modification cause, however, a relatively low PSNR of the marked image vs. the original image although there are no annoying artifacts. It is noted that reversible data hiding has concerned increasing attention recently, and more and more algorithms are being developed.

M.U.Celik et.al talked about a technique in which the host signal is quantized in the embedding phase and the residual is attained. Then the CALIC lossless image compression algorithm is accepted with the quantized values as side information, to efficiently compress the quantization left over to produce high capacity for the payload data. The packed in residual and the payload data are merged and embedded into the host signal via Generalized-LSB modification method. The payload of this method is from 15 to 143 kb for a 512x512x8 gray scale image as the PSNR is 38dB. Even though the payload is high, the PSNR is still low.

Zhicheng Ni et.al proposed a new reversible data embedding technique that makes use of the zero or the lowest point of the histogram and to some extent alters the pixel gray scale values to embed data. This technique can

be applied virtually to all types of images which can embed a large quantity of data (5–80 kb for a 512x512x8 gray scale image). This method gives excessive visual quality for all natural images. The PSNR of the marked image vs. the original image is assured to be higher than 48 dB. Until now, it has been successfully tested on dissimilar types of images, including some usually used images, medical images, texture images, aerial images, and all of the 1096 images available in CorelDraw database. The calculation of this technique is quite simple and the execution time is less. This lossless data hiding method is applied to immobile images. All these RDH techniques use the Histogram modification technique.

A more popular method is based on difference expansion (DE) , in which the difference of each pixel group is stretched, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the variation are all-zero and can be used for embedding messages.

A reversible data hiding algorithm, which can recover the original image without any distortion from the marked image uses the zero or the minimum points of the histogram of an image and somewhat amends the pixel gray scale values to embed data into the image. It can embed extra data than many of the existing reversible data hiding algorithms. Analytically and experimentally it is proved that the peak signal-to-noise ratio (PSNR) of the marked image produced by this method versus the original image is sure to be above 48 dB.
In some RDH techniques, the encrypted image is separated into several blocks and by flipping 3 LSBs of the half of pixels in each block room can be evacuated for the embedded bit. The data extraction and image recovery is done by finding the part which is flipped in one block. This procedure can be carried with the help of spatial correlation in decrypted image. Some other RDH methods employed spatial correlations using a dissimilar estimation equation and side match method to achieve lower error rate.

III. PROPOSED PLAN

Here, we would like to present the previously existing systems and their methodologies. The present system consists of five phases: (A) image encryption, (B) data hiding, (C) data extraction, (D) image decryption and (E) image recovery.

A. Image Encryption

Let's assume an image *X* (original) with a size *MxN* pixels which is in uncompressed format; each pixel *xij* is represented by 8 bits with gray value falling into [0,255], where $1 \le i \le M$, $1 \le j \le N$. Here, all the pixels in original image are initially classified into smooth and non-smooth pixels. In the encrypted image, classification permutation method is then premeditated for advancing the pixel-position privacy. Also, the classification permutation enables to differentiate the smooth pixels in the encrypted image with not knowing the original images' content. Here, a binary matrix $T = \{tij \mid 1 \le i \le M, 1 \le i \le N\}$ called the type-mark is used to represent the type of corresponding pixel in original image. Alternatively, if $tij=0$, the corresponding pixel *xij* is smooth pixel in the original image; otherwise, the pixel *xij* is a non-smooth pixel. If the MSBs of all pixels in the 3×3 neighbourhood centred on this pixels *xij* are same for any non-boundary pixel *xij* in an original image *X*, we say the pixel *xij* is smooth; else it is considered as non smooth. That is,

$$t_{ij} = \begin{cases} 1 & , \ i = 1, M \text{ or } j = 1, N \\ 1 & , \ MSBs \text{ of all pixels in } \Delta_{ij}^{X} \text{ are not same} \\ 0 & , \ MSBs \text{ of all pixels in } \Delta_{ij}^{X} \text{ are same} \end{cases} \quad (1)$$

Where, Δ^{x}_{ij} is a 3×3 neighbourhood in the original image which is centred on the pixel *xij*. After pixel classification, the XOR-encrypted image is initially obtained by the XOR of the original bits along with the pseudo-random bits, generated according to the encryption key. The detailed XOR encryption method refers to Zhang's scheme. This step improves the privacy of the image content. Then the encrypted image is formed by scrambling the smooth and the non smooth pixels in the XOR-encrypted image in respective manner. The procedure of the proposed classification permutation method is described as given.
(1) According to the XOR-encrypted image and type mark, the smooth linear table *Ls* and non-smooth linear table *Ln* are generated by scanning order from top to bottom, left to right, respectively.

$$\begin{cases} L^{s} = \{l_m = x_{ij} | t_{ij} = 0, m = 1,2, \dots, N_s\} \\ L^{n} = \{l_k = x_{ij} | t_{ij} = 1, k = 1,2, \dots, N_n\} \end{cases} \quad (2)$$

Where *Ns* and *Nn* depicts the number of smooth and non smooth pixels respectively, and $Ns+Nn=M\times N$.

(2) Both linear tables *Ls* and *Ln* are randomly and respectively permuted based on the encryption key, given as *Ekey*(*Ls*) and *Ekey*(*Ln*), and it is connected to fabricate a linear table L.

$$L = E_{key}(L^{s}) \,||\, E_{key}(L^{n}) \quad (3)$$

(3) The encrypted image *E* is produced by scanning the linear table *L* into 2-dimensional with a size of $M\times N$. For understand the process of proposed encryption, Fig. 1 depicts an example of the proposed image encryption; Fig. 1 (a) is an original image with a size of 5×7 pixels. According to (1), we can find the type-mark of Fig.1 (a), as given in Fig.1 (b), where the smooth and non-smooth pixels are counted as 13 and 22, respectively. The ratio of smooth

pixels in the original image, α, is 13/35. Fig.1 (c) is the XOR-encrypted image, wherein the position of pixels in original image is the same. Comparison of Fig. 1(a) with Fig.1 (c) gives the value of pixels in the XOR-encrypted image differs from that of corresponding pixels in the original image. According to the type-mark in Fig.1 (b), it is known that the 13 pixels delineated by red line in Fig. 1(c) are the smooth pixels of the original image. Fig.1 (d) shows the encrypted image, where the first 13 pixels above the red line are the smooth pixels delineated by red line in Fig. 1(c). The back of the encrypted image shows non smooth pixels.

Note that the type-mark is also shared as part of the encryption key between the content-owner and receiver in the proposed encryption method. On the other hand, the data-hider does not need to know the type-mark including the ratio of smooth pixels. This makes the security of encrypted image to be improved and easy to find the smooth pixels in the encrypted image.

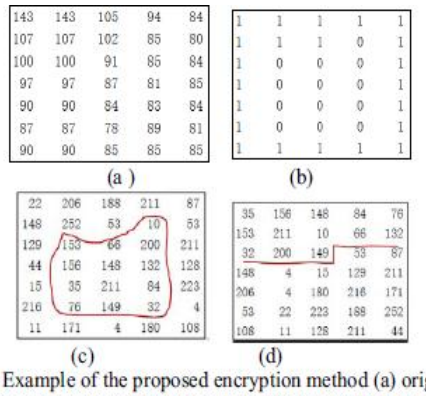

Fig.1 Example of the proposed encryption method (a) original image (b) type-mark (c) XOR-encrypted image and (d) encryption image

Additionally, we will be using a Master Base Record (MBR) table. An MBR is used for individual pixel value encryption i.e. we will be encrypting each selected pixel. This table is generated with respect to individual users; for each individual user his personal symmetric base encryption key is mentioned in the table and key will be generated as the image is encrypted. The table contains 256 values, one for each character.

B. Data Hiding

The data-hider, after receiving the encrypted image *E*, can embed some additional data by modifying the MSB of small portion pixels of the encrypted image. Let $D = \{dk|k=1,2,\ldots,Nd\}$ be a binary additional data that is to be embedded in the encrypted image, where *Nd* indicates the number of bits in the additional data. Data-hider pseudo randomly picks *Nd* encrypted pixels by looking at the data-hiding key that will be used to carry the additional data. For making the selected encrypted pixels smooth, one pseudorandom sequence with size of $\lfloor \beta MN \rfloor$, which is denoted as $R=\{ri|i=1,2,\ldots, \lfloor \beta MN \rfloor\}$, is initially created by the data-hiding key. Here *ri* is the real in interval [0,1], $\lfloor . \rfloor$ is the largest integer less than or equal to the given parameter. β is a parameter that is not more than the ratio of smooth pixels in the original image α. Finally the index sequence *A* is gained by sorting the real pseudorandom sequence *R*,

$$A = \{a_i | i = 1,2,\ldots,N_d\}$$
$$such\ that\ r_{a_1} \le r_{a_2} \le \cdots \le r_{a_{N_d}} \qquad (4)$$

Evidently, α_i is the integer in the given interval $[1, \lfloor \beta MN \rfloor]$ and the inequalities $a_i \neq a_j$ for $\forall\ i \neq j$. At the end, the *k*th ($k=1,2,\ldots,Nd$) bit in the additional data *D*, i.e. *dk*, is embedded by modifying the MSB of the pixel $e_{ik}j_k$ in the encrypted image,

$$e_{i_k j_k} = 128 \times d_k + mod\left(e_{i_k j_k}, 128\right), \qquad (5)$$

Where, *mod* (,) indicates modulus after division, *ik* and *jk* are the row and column coordinates of the pixel and are computed with,

$$\begin{cases} i_k = \lfloor a_k / N \rfloor + 1 \\ j_k = mod(a_k, N) + 1 \end{cases}, k=1,2,\ldots,N_d \qquad (6)$$

A marked encrypted image is constructed when all the bits are embedded.

Here, the data encryption is performed using MD5 generated key. The MD5 message-digest algorithm is a widely used hash function for producing a 128-bit hash value (data hiding key in our case). A second level encryption with the user key will be applied on the previously encrypted data which will result as a double encrypted format resulting in a 2 layer encryption.

C. Image Decryption

When the receiver has encryption key and does not know the data hiding key, the original image content can hardly be obtained. Decryption is performed to obtain the marked decrypted image $D0= \{d\_\_ K |1\le i\le M, 1\le i\le N\}$, which in some pixels are there whose MSB may be an error. The decrypted image $D = \{dij|1\le i\le M, 1\le i\le N\}$ is initially initialized to the marked decrypted image. To get the decrypted image with better quality, the value of the pixel *dij* is adjusted such that *tij*=0 by estimating its MSB,

$$d_{ij} = \begin{cases} 128 + mod(d_{ij}, 128), & if\ \sum_{\delta \in \Delta_{ij}^{D^0}} \left|\frac{\delta}{128}\right| \ge 4 \\ mod(d_{ij}, 128), & otherwise \end{cases} \qquad (8)$$

Where, Δ^{D0}_{ij} is a 3×3 neighbourhood centred on the pixel d^0ij in the marked decrypted image D^0.

As a part of decryption process data extraction steps will be to perform the two layer decryption (as we are using a two layer encryption) one with the MBR table value key and other with the user key.

D. Data Extraction

In this phase, we consider that only the receiver has the marked encrypted image along the data-hiding key. The *Nd* pixels, denoted as $e_{ik}j_k$ (k=1,2,…,*Nd*), in the marked encrypted image are obtained according to the data hiding key (6). The *Nd* embedded bits are achieved from,

$$d_k = \left\lfloor e_{i_k j_k}/128 \right\rfloor, k=1,2,\ldots,N_d \qquad (7)$$

Note that the receiver is unable get any information of and about the original image. Moreover, any attacker without the data hiding key is unable to pull out the additional data as he cannot acquire the pseudo-random position (*ik*, *jk*) of pixels whose MSB contains the additional data.

We have to reverse the hash function in this step in order to get the encrypted data. This is a user key decryption.

E. Image Recovery

The receiver on having the data-hiding key and encryption key can extract the embedded bits and get the recovered image $R=\{rij|1\le i\le M,\ 1\le i\le N\}$ with finer quality. This is because the pixels with embedding additional bits can be clearly recognized. According to (6), the receiver can calculate the position of pixels with added data in the encrypted image $\{(ik,jk)|k=1,2,\ldots,Nd\}$. It can easily achieve the position mark matrix of encrypted image $p^E=\{P^Eij|1\le i\le M,1\le i\le N\}$,

$$p^E_{ij} = \begin{cases} 1, & for\ (i_k,j_k), k = 1,2,\ldots,N_d \\ 0, & otherwise \end{cases} \qquad (9)$$

The position matrix of decrypted image given as $P=\{pij|1\le i\le M,\ 1\le i\le N\}$, can be obtained by performing the inverse procedure of the classification permutation for *PE*. According to the position matrix of decrypted image *P* and the marked decrypted image *D0*={d__ K |1≤*i*≤*M*, 1≤*i*≤*N*}, the recovered image $R=\{rij|1\le i\le M,\ 1\le i\le N\}$ can be reconstructed.

$$r_{ij} = \begin{cases} d^0_{ij}, & if\ p_{ij=0} \\ 128 \times \mu_{ij} + \mathrm{mod}(d^0_{ij}, 128), & otherwise \end{cases} \qquad (10)$$

Where, the value of u_{ij} is calculated with two cases.

i. If all pixels in the 3×3 neighborhood of pixel *pij* in the *P* are not all one,

ii. the value of u_{ij} is decided by the 3×3 neighborhood of pixel *pij* and d^0ij,

$$u_{ij} = \begin{cases} 1, & if\ \dfrac{\sum_{m=i-1}^{i+1}\sum_{n=j-1}^{j+1}(1-p_{mn})\times\left|\frac{d^0_{mn}}{128}\right|}{\sum_{m=i-1}^{i+1}\sum_{n=j-1}^{j+1}(1-p_{mn})} > 0.5 \\ 0, & otherwise \end{cases} \qquad (11)$$

Or else, the value of u_{ij} is given by the 5×5 neighbourhood of pixel *pij* and d^0ij,

$$u_{ij} = \begin{cases} 1, & if\ \dfrac{\sum_{m=i-2}^{i+2}\sum_{n=j-2}^{j+2}(1-p_{mn})\times\left|\frac{d^0_{mn}}{128}\right|}{\sum_{m=i-2}^{i+2}\sum_{n=j-2}^{j+2}(1-p_{mn})} > 0.5 \\ 0, & otherwise \end{cases} \qquad (12)$$

Image recovered will the result of the above performed steps.

IV. EXPECTED OUTPUT

The quality of decrypted images gained by the method proposed would be better than comparison with the method of Wu and Zhang in different test images and different embedding rate. Particularly, having the embedding rate as 0.0156, the decrypted image by the proposed method and the original one will be the same with high probability for all four test images i.e. the probabilities for lossless decryption would respectively be 0.99, 0.99, 0.97 and 0.99. When the embedding rate is kept 0.0625, PSNR of decrypted image by the proposed method is 12 dB and 20 dB higher than that by Zhang and Wu method, respectively. When embedding rate is kept as 0.1563, resulting PSNR of decrypted image by the proposed method will be slightly lesser than that by Zhang's method. Furthermore, we have the probability as 100% for lossless recovery by proposed method, even if for texture image Baboon at a high embedding rate of 15%. Conversely, the probability of Baboon image that is recovered, obtained by Zhang's and Wu's method is towards zero for the various embedding rates.

V. APPLICATIONS

Confidential transmission, video surveillance, military and medical applications are some of the areas of application for Separable RDH using image encryption. Also, information like private annotations, business logos, and critical intelligence can be embedded into a cover image in an invisible form so that many applications, like ownership claim of digital contents, copyright protection of media, covert communication between parties, etc., can be fulfilled.

VI. CONCLUSION

A classification permutation based separable reversible data hiding in encrypted image is proposed in this paper. In the image encryption phase, this work gives a classification permutation encryption with a combination of the XOR-encryption to get better privacy of encrypted image. Additionally, it is possible for the data hider to get the smooth pixels in the encrypted image without the original content and the encryption key together with the type-mark. This results in improved quality of decrypted images and recovered ones too.

REFERENCES

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

[2] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, April. 2011.

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

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

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

[6] K. Ma, W. Zhang, X. Zhao, et al., "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.

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

[8] T. Nguyen, C. Chang and W. Chang, "High capacity reversible data hiding scheme for encrypted images," Signal Process.: Image Commun., vol. 44, pp. 84-91, 2016.

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

[10] X. Wu andW. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," Signal Process., vol. 104, pp. 387-400, 2014.

[11] F. Chen, H. He, Y. Huo, "Self-embedding watermarking scheme against JPEG compression with superior imperceptibility", Multimed Tools Appl., DOI 10.1007/s 11042-016-3574-0, 2016.

[12] Z. Ni, Y.Q. Shi, N. Ansari, and W.Su, Reversible data hiding, IEEE Transactions on Circuits and Systems for Video Technology, Vol 16, no.3, Mar 2006, pp 354-362.

[13] Shilpa Sreekumar and Vincy Salam, Advanced Reversible Data Hiding with Encrypted Data, IJETT, Vol.13, no.7, Jul 2014, pp 310-313.

[14] VinitAgham and TareekPattewar, A Survey on Separable Reversible Data Hiding Technique, IMACST, Vol.4, no.1, May 2013, pp 9-13.

[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, Reversible data hiding, International Conference on Image Processing, ISSN 1522-4880, Vol.2, Oct.2002, pp 157-160.

[16] C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless Recoveryof an Original Image Containing Embedded Data," U.S. Patent6 278 791 B1, Aug. 21, 2001.

[17] B. Macq and F. Deweyand, "Trusted headers for medical images" DFG VIII-D II Watermarking Workshop, Erlangen, Germany,Oct. 1999.

[18] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication,"Proc.SPIE Security Watermarking Multimedia Contents, San Jose, CA, Jan.2001, pp. 197–208.

[19] M. Goljan, J. Fridrich, and R. Du, Distortion-free data embedding,Proc. 4th Inf. Hiding Workshop, Pittsburgh, PA, Apr. 2001, pp. 27–41.

[20] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. Yeo, Wavelettransforms that map integers to integers,Appl. Comput. HarmonicAnal., vol. 5, no. 3, pp. 332–369, 1998.

[21] LalitDhande, PriyaKhune, VinodDeore and DnyaneshwarGawade, Hide Inside-Separable Reversible Data hiding in Encrypted Image, IJITEE, ISSN:2278-3075, Vol. 3, Issue 9, Feb 2014, pp 88-91.

