International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Variable Data Hiding over Protected Images by Reversible Picture Transformation using UES Method

Navya M[1],Shamshekhar S Patil[2]

[1] *M. Tech Student , Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology,Bangalore-560056*

[2] *Associate Professor, Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology,Bangalore-560056*

Abstract – With the notoriety of outsourcing information to the cloud, it is imperative to ensure the protection of information and empower the cloud server to effectively deal with the information in the meantime. Under such requests, reversible data hiding in encrypted images (RDH-EI) draws in an ever increasing number of specialists' consideration. In this paper, we propose a novel system for RDH-EI in view of reversible image transformation (RIT). Not the same as all past encryption-based structures, in which the cipher texts may pull in the documentation of the inquisitive cloud, RIT-based system enables the client to change the substance of unique picture into the substance of another objective picture with a similar size. The changed picture, that resembles the objective picture, is utilized as the "encoded picture," and is outsourced to the cloud.

In this way, the cloud server can without much of a stretch implant information into the "encoded picture" by any RDH techniques for plaintext pictures. Also, in this manner a customer free plan for RDH-EI can be understood, that is, the information installing process executed by the cloud server is superfluous with the procedures of both encryption and unscrambling. Two RDH techniques, including customary RDH plot and bound together implanting and scrambling plan, are embraced to insert watermark in the encoded picture, which can fulfill distinctive needs on picture quality and expansive installing limit, separately.

***Key Words*: Image encryption, outsourced capacity in cloud, security insurance, Reversible Data Hiding (RDH), Reversible Image Transformation (RIT).**

1. INTRODUCTION

These days outsourced capacity by cloud turns out to be increasingly mainstream benefit, particularly for media documents, for example, pictures or recordings, which require substantial storage room. To deal with the outsourced pictures, the cloud server may insert some extra information into the pictures, for example, picture classification and documentation data, and utilize such information to distinguish the proprietorship or confirm the honesty of pictures. Clearly, the cloud specialist organization has no privilege to present lasting mutilation amid information installing into the outsourced pictures. In this way, reversible data hiding (RDH) innovation is required, by which the first picture can be lossless recuperated after the implanted message is removed. This system is likewise generally utilized as a part of Manuscript got November 05, 2015; overhauled April 09, 2016; acknowledged May 04, 2016. Date of production May 17, 2016,July 15, 2016. This work was upheld to a limited extent by the Natural Science Foundation of China under Grant 61572452 and Grant 61502007, to a limited extent by the China Postdoctoral Science Foundation under Grant 2015M582015, and to a limited extent by the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06030601.

Within the framework "RRBE,"(Reversing Room Before Encryption) the photograph proprietor first empties out room with the aid of using RDH technique in the obvious PE(Prediction Error). After that, the picture is encrypted and outsourced to the cloud and the cloud server can freely embed facts into the reserved room of the encrypted photograph. the primary approach beneath RRBE framework, which reserves room by embedding LSB's(Least Significant Bit) of some pixels into other pixels with a conventional RDH technique and then encrypts the picture, so the positions of these LSB's within the encrypted image may be used to embedded data.

On this paper, we endorse a unique framework for RDH-EIby means of using reversible image transformation (RIT). RIT transfers the semantic (content material) of the original image I into the semantic of any other photograph J , and "reversibility" way that I can be lossless restored from the converted photo. consequently RIT can be regarded as a special encryption scheme, known as "semantic transfer encryption." in different words, the resultant converted picture which is also the encrypted photograph E(I) will look similar with J. the photograph j is chosen to be beside the point with I however has the equal size of I , and consequently the content material of the photo I is blanketed. Because the "encrypted image" is in a form of plaintext, it'll avoid the notation of the cloud server, and the cloud server can effortlessly embed records into the "encrypted image" with conventional RDH techniques for plaintext images.

1.1 Existing System

To compress the block indexes, we first classify the blocks in step with their SD values before pairing them up. in reality, we determined that the SD values of most blocks pay attention in a small range close to zero and the frequency fast drops down with the growth of the SD fee, which is depicted from numerous sizes of 10000 snap shots from the boss base photograph database. class 0 for blocks with smaller SD's, and class 1 for blocks with larger SD's, and pair up the blocks belonging to the identical magnificence by means of assigning the general public of blocks to the magnificence 0, we can keep away from the big deviation of SD's(Standard Deviation)between a couple of blocks and effectively compress the indexes on the same time.
On this framework, a content proprietor encrypts the unique photograph the usage of a fashionable cipher with an encryption key .after generating the encrypted picture, the content owner palms over it to a records hider (eg: a database manager) and the records hider can embed auxiliary records into the encrypted picture by way of losslesly vacating some room according to a statistics hiding key. then a receiver ,perhaps the content owner himself or a licensed 0.33 birthday party can extract the embedded statistics with the records hiding key and in addition recover the authentic photograph from the encrypted version in line with the encryption key.
No matter the setting of IBE or PKI, there must be an technique to revoke users from the gadget whilst necessary. The authority of a few consumers is expired or the name of the game key of some consumer is disclosed. in the traditional PKI placing, the trouble of revocation has been nicely studied and several techniques are broadly accepted, inclusive of certificates revocation list or appending validity intervals to certificates.

1.2 Proposed System

Encryption is the technique of encoding messages or facts in one of these manner that handiest legal parties can access it. Encryption does now not of itself prevent interference, but denies the message content to the interceptor. in an encryption scheme, the meant information or message, referred to as plaintext, is encrypted the use of an encryption set of rules, producing cipher text which could only be examine if decrypted.
Statistics privatenes, or information privacy (or information safety), is the relationship between collection and the dissemination of the statistics, era in the current world, the public expectation of privateness, protection and the legal and political issues within the residing surrounding. Privacy concerns exist wherever in my opinion identifiable facts or other touchy information is accumulated, saved, used, and eventually destroyed or deleted in virtual shape or in any other case. Fallacious or non-existent disclosure manipulate can be the root cause for privacy problems.
In keeping with the pairing rule, the first block of the authentic photo is paired up with the forth block of the target photograph, because both of them is the first block of class 1 as shown within the CIT(Class Index Table); the second block of original picture is paired up with the ninth block of target image, due to the fact each of them is the second block of class 1, and so forth. The pairing result is indexed in desk I, which may be generated in step with the CIT of authentic photograph and the CIT of the goal photo.
Considering the fact that losselesly vacating room from the encrypted photos is incredibly hard and sometimes inefficient, why are we nevertheless so obsessed to locate novel RDH techniques operating without delay for encrypted pics , if we reverse the order of encryption and vacating room that is booking room previous to image encryption at content proprietor aspect, the RDH duties in encrypted PIX might be extra herbal and much simpler which leads us to the radical framework "Reserving room Before Encryption(RRBE).
Obviously fashionable RDH algorithms are the suitable operator for reserving room before encryption and may be effortlessly carried out to framework RRBE to obtain higher overall performance compared with techniques from framework VRAE(Vacating Room After Encryption).

2. LITERATURE SURVEY

Reversible (lossless) facts hiding (embedding) method, which allows the precise recovery of the unique host sign upon extraction of the embedded statistics. a generalization of the famous LSB (least enormous bit) modification is proposed because the statistics embedding approach, which introduces additional working factors at the capability-distortion curve. loosless healing of the unique is finished with the aid of compressing quantities of the sign that are prone to embedding distortion, and transmitting these compressed descriptions as a part of the embedded payload. A prediction based conditional entropy coder which makes use of static quantities of the host as facet facts improves the compression performance, and therefore the lossless facts embedding capability.
In 2016 J. Zhou et al [1] proposed a unique RDH-EI technique for joint decryption and extraction, in which the correlation of plaintexts is further exploited by way of distinguishing the encrypted and non-encrypted pixel blocks with a elegance SVM classifier to split the data extraction from image decryption, In 2012, Zhang [2] emptied out space for information embedding by using at once the usage of the everyday way of cipher textual content compression, this is, compressing the encrypted pixels in a lossless way through the use of the syndromes of parity check matrix of channel codes. in 2016 Qian et al[4] stepped forward the method of [2] by means of adopting low density parity test based totally Slepian wolf encoder which is also one of the maximum efficient strategies for cipher text compression.
Recently, In 2013 Zhang et al. [8] and in 2015 X.Hu[10] proposed the most advantageous histogram amendment

algorithm for RDH by using estimating the most appropriate change chance .Then again, cloud provider for outsourced storage makes it hard to guard the privateness of picture contents.

In the framework "RRBE," the photo proprietor first empties out room with the aid of the use of RDH method in the apparent pictures. After that, the photograph is encrypted and outsourced to the cloud and the cloud server can freely embed data into the reserved room of the encrypted photograph. the primary technique underneath RRBE framework become presented in 2013 through W. Zhang, X. Zhao[7], which reserves room with the aid of embedding LSB's of some pixels into different pixels with a conventional RDH technique and then encrypts the photograph, so the positions of these LSB's within the encrypted photo can be used to embed statistics. The method in [7] implies that the reason of RDH-EI can also be realized through RDH for plaintext photographs. Following this concept, In 2014 Zhang et al.[5] reserve room in photographs by means of generating PE(Prediction Errors) and editing the histogram of PE, that is the maximum famous approach utilized in RDH for plaintext. to protect confidentiality, a special encryption scheme is designed in [5] to encrypt the PE's, In 2016 Cao et al.[3] advanced the strategies of [7], [5] by means of patch level sparse representation which can yield PE's with smaller entropy and thus bring about a large hiding room.

So far, many RDH techniques on snap shots were proposed. In essence, some of these strategies may be considered as a manner of semantic lossless compression [8], [11], wherein some area is stored for embedding greater statistics through lossless compressing the photograph. Herein, "semantic compression" way that the compressed picture ought to be near the authentic image, and as a result one could get a marked image with desirable visible first class because the residual a part of photographs, e.g., the prediction mistakes (PE), has small entropy and may be without difficulty compressed, nearly all current RDH methods first generate PEs because the host sequence [4],[9], and then reversibly embed the message into the host sequence through modifying its histogram with techniques like histogram shifting [5] or difference expansion [11]. Recently, Zhang et al. proposed the most useful histogram modification set of rules [8], [6] for RDH with the aid of estimating the surest change chance [10], [11].

Alternatively, cloud service for outsourced storage makes it tough to protect the privacy of photo contents. as an instance, currently many private pix of hollywood actress leaked from icloud. Despite the fact that RDH is helpful for dealing with the outsourced pictures, it cannot protect the photo content material. Encryption is the most famous technique for defensive privacy. So it's far interesting to implement RDH in encrypted pix (RDH-EI), via which the cloud server can reversibly embed facts into the photograph however cannot get any knowledge about the photo contents. Stimulated through the desires of privateness protection, many techniques were provided to increase RDH methods to encryption area. From the point of view of compression, these techniques on RDH-EI belong to the following frameworks [7]. Framework i "vacating room after encryption (VRAE)" and framework ii "reversing room before encryption (RRBE)."

Inside the framework 'VRAE," the cloud server embeds statistics with the aid of lossless vacating room from the encrypted photos by means of using the concept of compacting encrypted photos [10], [14]. Compression of encrypted facts can be formulated as source coding with facet facts on the decoder [14]. Usually the side statistics is the correlation of plaintexts this is exploited for decompression via the decoder. In [12], Zhang divided the encrypted picture into several blocks. Through flipping three LSBs (least vast bits) of the half of pixels in each block, room can be vacated for the embedded bit. The information extraction and photo recovery continue through locating which element has been flipped in one block. This method may be found out with the assist of spatial correlation within the decrypted photograph.

Hong et al. [13] ameliorated Zhang's approach on the decoder side with the aid of similarly exploiting the spatial correlation the use of a distinctive estimation equation and side in shape technique. For each methods in [11] and [13], decrypting photograph and extracting records ought to be mutually finished. These days, Zhou et al. [1] proposed a singular RDH-EI approach for joint decryption and extraction, wherein the correlation of plaintexts is further exploited with the aid of distinguishing the encrypted and non-encrypted pixel blocks with a magnificence SVM syndromes of parity test matrix of channel codes. Qian et al. [4] improved the technique of [2] by using adopting low density parity check based Slepian Wolf encoder which is likewise one of the maximum efficient methods for the cipher text compression for the encryption information.

3. SYSTEM ARCHITECTURE

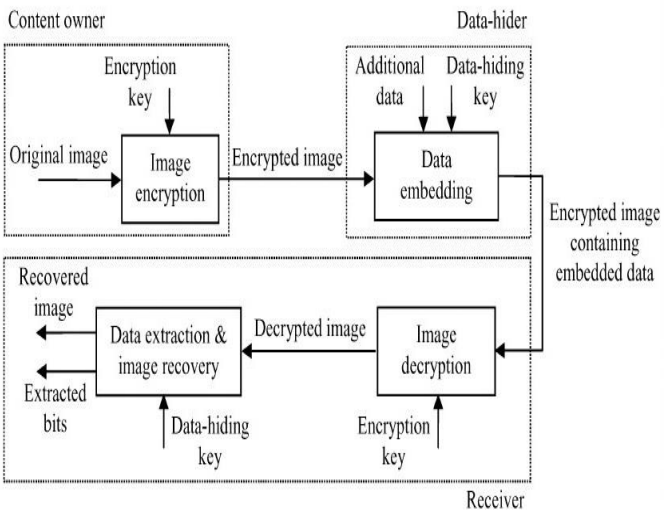

Fig 3: System Architecture

Machine structure diagram represents the flow of series process. Fig 3 depicts the variations between the radical framework and former frameworks, which indicates that, by using frameworks VRAE (vacating room after encryption) and RRBE (reserving room before encryption) , the user's pictures are saved within the shape of cipher text within the cloud account, even as by the RIT-primarily based body work, the photo is saved in a form of plaintext.

In the framework VRAE shown in Fig 3, along with schemes in and , the image owner (the sender) encrypts the photograph I into E(I) with a key k. the cloud server embeds statistics by way of compressing the encrypted picture E(I) and generates Ew(I) that is stored in the cloud. While getting a retrieval request, the cloud server returns Ew(I) to the receiver, maybe a certified third celebration, who generates I through a procedure of joint decompression and decryption with the key okay. Herein, Ew(I) can be simply Ew(I) or a changed version received by getting rid of the embedded data. Observe that the cloud server cannot restore E(I) from Ew(I) ,when you consider that decompression have to be joined with decryption with the help of ok. On this framework, the complexity is taken on by the receiver who ought to join the manner of de-compression and decryption to get the original picture.

Inside the framework RRBE proven in Fig 3 such as schemes in [13], the picture proprietor (the sender) reserves room from the photograph I and encrypts it into E(I)with a key okay, and then sends it to the cloud server who embeds records into the reserved room and generates Ew(I).Ew(I)is saved within the cloud, from which the cloud server can extract the records that is used for control. While an authorized user (the receiver) desires to retrieve the image, the cloud server can repair E(I)from Ew(I)and send E(I)to the user who can decrypt E(I) and get I with the key ok. Inside the framework RRBE, the complexity is borne via the sender who ought to reserve room for RDH by means of exploiting the redundancy inside the image and consequently the RDH technique used by the cloud must be distinct with the sender that is, the RDH method utilized by cloud is sender-associated.

Inside the RIT based totally framework depicted in Fig 3, the photo I is "encrypted" into some other plaintext photograph E(I)with a key okay, so all snap shots of the users, encrypted or not, can be stored within the cloud within the shape of plaintexts. The cloud server can embed/extract information into/from E(I)with any classical RDH technique for plaintext pics and E(I)can be recovered from the watermarked image Ew(I)through the cloud and dispatched returned to the legal person who anti-transforms it to get the original image I with the key k.

4. ALGORITHMS

Algorithm1: Procedure of Transformation.

Input: An original image I and a secret key K.

Output: The encrypted image E(I).

1) Select a target image J having the same size as I from an image database.
2) Divide both I and J into several non-overlapping 4×4 blocks. Assuming that each image consists of N blocks, calculate the mean and SD of each block.
3) Classify the blocks with quantile of SD's and generate CITs for I and J respectively. Pair up blocks of I with blocks of J according the CITs as described in Section III-A.
4) For each block pair (B_i, T_i) $(1 \le i \le N)$, compute the mean difference u_i. Add u_i to each pixel of B_i and then rotate the block into the optimal direction $\theta_i (\theta_i \in \{0^\circ, 90^\circ, 180^\circ 270^\circ\})$, which yields a transformed block T_i.
5) In the target image J, replace each block T_i with the corresponding transformed block T_i for $1 \le i \le N$ and generate the transformed image J .
6) Collect u_i 's and θ_i 's for all block pairs, and compress them together with the CIT of I . Encrypt the compressed sequence and the parameter α by a standard encryption scheme such as AES with the key K.
7) Take the encrypted sequence as AI, and embed AI into the transformed image J with an RDH method such as the one in [7], and output the encrypted image $E(I)$.

Algorithm 2: Procedure of Anti-Transformation.

Input: The encrypted image $E(I)$and the key K.

Output: The original image I.

1)Extract AI and restore the transformed image J from E(I)with the RDH scheme in [7].
2)Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I ,u_i , θ_i $(1 \le i \le N)$ and α.
3)Divide J into non-overlapping N blocks with size of 4×4. Calculate the SD's of blocks, and then generate the CIT of J according to the %α quantile of SD's.
4) According to the CITs of J and I , rearrange the blocks of J as described in Section III-A.

5. MODULES

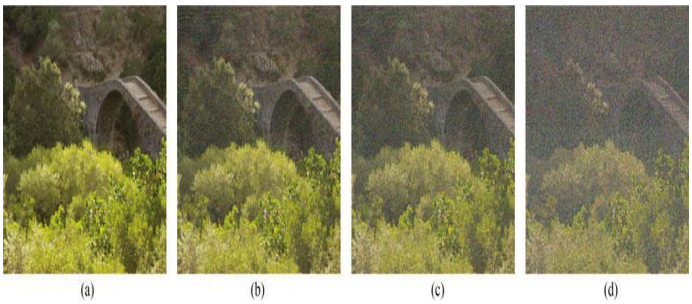

Fig 5:Distortion of the encrypted images with various payloads by applying UES in the test images.

Distortion of the encrypted images with various payloads by applying UES in the test images (a) Encrypted image.(b) Marked image(1.0 bpp).© Marked image(1.7 bpp). (d) Marked image(2.4 bpp).

5.1 Traditional RDH on the Encrypted Image

It must be noted that someone of classical RDH technique for plaintext photograph may be implemented to embed and extract watermark in the encrypted photo E(I) in the RIT primarily based scheme. For instance, we pick out the technique proposed by way of Dragoi and might be. The scheme of Dragoi et al. is in short defined as follows. For every pixel, a least rectangular predictor is computed on a square block focused at the pixel, that can adaptively make use of each neighbor pixel's difference in a neighborhood place. The most exciting aspect of the approach is the truth that the same predictor can be found out on the receiver aspect, avoiding the want of embedding a huge amount of extra statistics. Having expected the contemporary pixel, the prediction mistakes (PE) might be shifted for vacating room or be extended for embedding one message bit for greater info please talk to [7].

5.2 Unified Embedding & Scrambling (UES) on the Encrypted Image

The amount of AI is already massive. So it's far difficult for classic RDH methods to earn big embedding capability at the same time as still keeping high visible excellent. To meet the demand of large payloads, the cloud server can insert watermark with a unified embedding and scrambling method called UES [14], which intentionally degrades photo.

In such manner a marked image with meaningless form can be produced just like the manner of conventional encryption based totally RDH-EI schemes. in fact, in some utility cases, the cloud server does now not want to bear in mind the satisfactory of marked photograph as performed in all preceding RDH-EI.

In Fig.5 (a) and (b).,Inside the first step the cross set is expected via rounding the end result of (8) and inside the 2d step the triangle set is anticipated by rounding the result of (9).

After prediction, data embedding may be finished as follows:

1) Compute the prediction errors;
2) Compress prediction errors the use of run-period and Huffman coding; and
3) Without delay insert the compressed prediction errors and the watermark into the anticipated locations via replacing the expected pixels.

On the receiver side, after extracting the watermark, the decoder desires to decompress the prediction mistakes and upload it to anticipated pixel price through CBP, so that it will losslessly generate the pixel price. Observe that the original united states of America approach in [14] is not reversible, because, to expand payloads, it replaces the prediction error Eij .Because the reference pixels (circle set) remains unchanged each at embedding and extraction, they can be extracted to make up a sub sampled photograph. Then the sub sampled picture can be employed by way again to in addition embed extra statistics, which is called degree embedding. in truth, such system may be repeated and recognise multi stage embedding as proven in Fig.5, for you to further degrade the visual first class of the photograph. Word that the embedding payload of can be controlled by using parameters, the prediction error threshold T determining which pixel may be changed by using outside message and the embedding level. manifestly the payload will increase with the boom We examine the exceptional of image shape subjectively by using visual inspection and objectively measured by way of SSIM [15] between marked photo and encrypted picture. Fig.5 suggests Snapshots are gradually decreasing with increasing payloads. In addition in Fig.5 we use check snap shots in experiment a for instance to expose the distortion level for numerous embedding payloads. With the increase of embedding payload, the photo end up an increasing number of blurred. It is validated that can significantly increase the embedding capacity to be had for the cloud server.

6. CONCLUSION AND FUTURE WORK

In this paper we propose a singular framework for RDH-EI primarily based on RIT. unique from previous frameworks which encrypt a plaintext photograph right into a cipher textual content form ,RIT-based totally RDH-EI shifts the semantic of authentic picture to the semantic of any other photo and as a consequence protect the privateness of the authentic image. due to the fact the encrypted image has the shape of a plaintext image, it will keep away from the notation of the curious cloud server and it's miles loose for the cloud sever to select any individual of RDH techniques for plaintext pix to embed watermark.

We comprehend an RIT primarily based method by using enhancing the picture transformation approach in [15] to be reversible. By way of RIT, we are able to rework the unique photograph to an arbitrary selected target picture with the same size, and restore the authentic image from the encrypted picture in a lossless way. RDH strategies together with PEE (Prediction Error Expansion) based totally RDH and are followed to embed watermark inside the encrypted photo to meet one of a kind wishes on photo best and embedding capacity.

Several thrilling problems may be taken into consideration inside the future, including how to enhance the fine of the encrypted photo and how to make bigger concept of RIT to audio and video.

ACKNOWLEDGEMENT

Any achievement, be in scholastic does not depend solely on the individual effort but on the guidance, encouragement and cooperation of intellectuals, elders and friends, a number of personalities, in their own capacities have helped me in presenting this paper. I would like to take this opportunity to thank them all.
I express my immense gratitude to my guide Mr. Shamshekhar S Patil, Associate Professor, Department of Computer Science and Engineering, Dr.Ambedkar Institute of Technology,Bengaluru, for his valuable guidance,suggestions ,advice and cooperation.

BIBLIOGRAPHY

[1]J. Zhou et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 3, pp. 441–452, Mar. 2016.
[2]X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[3]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.
[4]Z. Qian and X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 4, pp. 636–646, Apr. 2016.
[5]W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Process., vol. 94, pp. 118–127, Jan. 2014.
[6]X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans.Inf. Forensics Security, vol. 10, no. 3, 653–664, Mar. 2015.
[7]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.
[8]W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.
[9]I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, Apr. 2014.
[10]X. Hu et al., "Fast estimation of optimal marked-signal distribution for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 8, no. 5, pp. 779–788, May 2013.
[11]W. Zhang, X. Hu, and N. Yu, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Trans Image Process., vol. 24, no. 1, pp. 294–304, Jan. 2015
[12]X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[13]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, Apr. 2012.
[14]W. Liu,W. Zeng, L. Dong, and Q.Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[15]Y. Lee and W. Tsai, "A new secure image transmission technique via secret-fragment visible mosaic images by nearly reversible color transformation," IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 4, pp. 695–703, Apr. 2014.