iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** II **Month of publication:** February 2020

DOI: http://doi.org/10.22214/ijraset.2020.2098

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

Reversible Data Hiding in Encrypted Environment: A Review

Kavya S.[1], Anusree L.[2]
[1] *M-Tech Student,* [2] *Assistant Professor, Department of Electronics and Communication Engineering, LBS Institute of Technology For Women, Kerala*

Abstract: ***In recent years a huge attention is given to the technique called Reversible Data Hiding In Encrypted Images (RDHEI) due to the demand for high security requirement. RDHEI is a type of data hiding that supports the lossless recovery of the host image following the extraction of secret hidden data. Since the technique is lossless, it is suitable for applications like medical imaging, scientific investigation, military applications, cloud services, law enforcement etc. Based on the method of implementation RDHEI can be classified into different categories. Existing RDHEI are mainly classified as with or without preprocessing of the host image before image encryption. Here different existing RDHEI techniques and its basic procedures is discussed.***

Keywords: Security, Reversible Image Data Hiding in Encrypted Images (RDHEI) , Image recovery, Image encryption.

I. INTRODUCTION

Image Security has a major role in many fields. The desirable properties of secure communication is as follows.

A. Confidentiality

1) Only the transmitter and the intended receiver be able to identify the contents of the transmitted message [1].

2) Sometimes the hackers may intercept the message, so it is necessary that the message needs to be encrypted so that the transmitted message cannot be decrypted by an interceptor.

B. Authentication

1) Both sender and receiver should be able to confirm the identity of other party involved in communication [1].

C. Nonrepudiation and Message Integrity

1) Even if both the sender and receiver can authenticate each other, both of them want to ensure that the content is not altered by any eavesdroppers.

2) Network security measures are required to protect the data content during their transmission and hence to ensure that the data transmissions are done authentically.

3) One of the most common technique underlying virtually all automated network and the network security applications is encryption.

When the image is transmitted over the network there occurs various threads. Inorder to eliminate the threads of data transfer various security methods were introduced. The two important techniques used for secure communication is cryptography and data hiding.

In cryptography, the host data ie, the plain image is converted to an unreadable form called as the cipher data and is transmitted over the network. This technique basically allows the sender to change the data so that the hacker didn't gain any information from the hacked data. The receiver must be able to retrieve the original data from the changed data. The main drawback of cryptography is that the intruder is always aware about the transmission of the incomprehensible data.

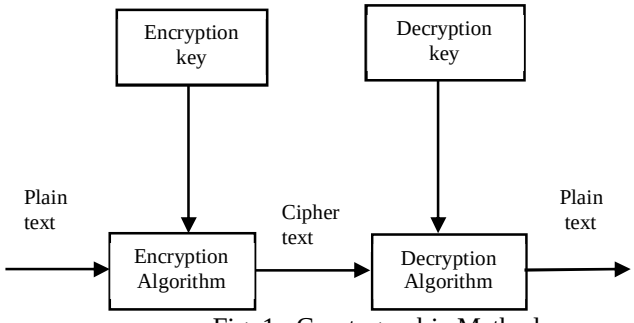


Fig. 1: Cryptographic Method

The second method used for secure communication is the data hiding technique. In this technique the data is disguised inside the cover file and is transmitted through the network. The cover file can be an image, audio, video etc. The main advantage of data hiding over cryptography is that it hides the existence of secret information. The Reversible data hiding is a type of data hiding in which the data embedding is done in such a way that the human eyes are difficult to distinguish between the original plain image and the data embedded image. Also this technique supports the lossless reconstruction of original image. There exists some applications in which both encryption and data hiding have to be used simultaneously, there comes the existence of the Reversible Data Hiding In Encrypted Images (RDHEI). Basically all the Reversible Data Hiding In Encrypted Images consists of three steps.

a) Image Encryption
b) Data Embedding
c) Data Extraction
d) Image Reconstruction

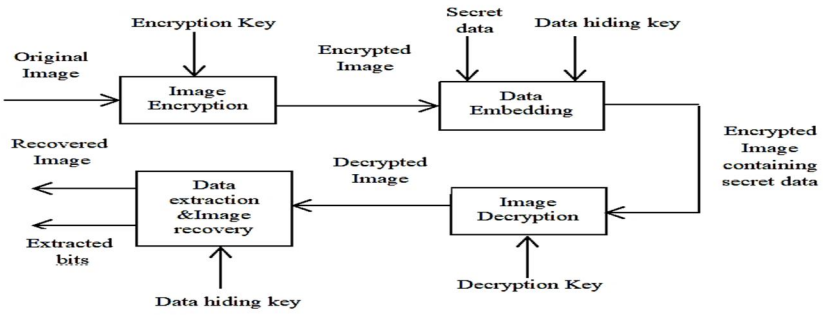


Fig 2: Reversible Data Hiding In Encrypted Images

In general all the reversible data hiding in encrypted images can be classified into two categories, the methods by vacating room after the encryption process and the methods by reserving room before the encryption process.

In the vacating room after the encryption technique, firstly the image is encrypted using any of the encryption algorithms and after that the room for hiding the extra data is vacated from the encrypted image by modifying some bits of the encrypted data and the data hider hides the secret data on to the vacated room. The main advantage of this technique is that it is comparatively simple and efficient. The limitation is that embedding capacity is limited as the encrypted image entropy has been maximized. In addition vacating the room losslessly from the encrypted image is difficult.

In the reserving room before encryption technique as the name suggests the room for hiding the secret data is reserved before the image encryption, ie the embedding room is created in the original image domain. The advantage of this technique is that embedding capacity is higher and better reversibility can be achieved. Sometimes this framework is impractical because the content owner need to perform an extra preprocessing before the image encryption, for reserving the room for hiding the secret data. This technique mainly uses the spatial correlations of the original image to reserve the room for hiding the data before the encryption of the image. Since the room for hiding the secret data is already reserved, the data hiding process is effortless. This method of reservation is beneficial because it saves time for creating space for data hiding on time.

II. LITERATURE SURVEY

In [2] Wen- Chung Kuo, Lih- ChyauWuu, Shao-Hung Kuo proposed a reversible data hiding method, this method incorporates the JPEG compression scheme on to data hiding method. In the image processing both the data hiding and the compression techniques plays an important role. Here both of these techniques are combined. The use of compression technique will lead to the reduction in the bandwidth requirement. Since the data hiding mainly focuses on the security and the compression focuses on to the compression ratio and bandwidth requirement there is no relationship between these two techniques. This method can achieve high embedding capacity and good compression ratio. The limitation is that there are some errors in the original image reconstruction.

In [3] X.Zhang proposed a reversible data hiding in encrypted image method. Here the most common LSB modification technique is used for data hiding. Firstly the image is encrypted using an encryption scheme and then by flipping the last three LSB's the data hider can embed one bit of the data into each of the blocks. The spatial correlation between the original images and the interfered blocks exists, the interfered blocks should be less smoother when compared to the original blocks. Thus the original cover image can be recovered along with the secret data. Errors may occur in the data extraction as well as the image recovery when the selection of the blocks falls in the appropriate block size.

In [4] Xinpeng, Zhang proposed a separable reversible data hiding in encrypted images method. In this method, with the help of an encryption key the original uncompressed image is encrypted firstly. Then inorder to create additional space to accommodate extra data the data hider compresses the LSB's of the encrypted image. At the receiver side via the same secret data hiding key the data hided in the additional space can be easily extracted from the encrypted image. The main limitation of this method is that the embedding capacity is low and for high embedding capacity it can only generate low quality marked image and also all the processes are subjected to various errors on data extraction and image recovery. Basically these errors are occurring since the room for hiding data is vacated after the encryption process. So by adopting the technique of reserving room before encryption these errors can be minimized.

In [5] Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li proposed a method of Reversible data hiding in encrypted images by reserving room before encryption. Here the content owner firstly creates enough space to embed additional data and after that the image is encrypted using an encryption key and the data is embedded on to the extra space already reserved for hiding data. Here inorder to reserve the room for additional data the redundancy the cover image is utilized ie, by losslessly compressing the redundant image content extra space is created. The main limitation of this technique is that reserving room before encryption is not practically applicable. Also even if the errors can be minimized the complexity is comparatively higher. Vacating room after encryption is more practically applicable because for the encryption process the original image as such is required.

In [6] Chen, Chih-Wei Shiu, Yu-Chi, and Gwoboa Horng proposed encrypting signal-based reversible data hiding via public key cryptosystem. In this method homo-encryption technique is used, it allow the user to operate encrypted data directly without decryption. Here the system is more secure but the payload capacity is lesser. Here the content owner and data hider must be specific parties who knows the secret key with the receiver. Here a new notion of encrypted image based reversible data hiding is introduced, where the receiver sets his public/secret key pair. The content owner generates the encrypted signal, and then the data hider will hides the secret data to create the encrypted signal with the hidden embedded message by using the receiver's public key. This paper is the first to consider the issues of Reversible data hiding done in the encrypted domain by using the public key cryptosystem ie by using the shares.

In [7] Qin, Chuan, and Xinpeng Zhang proposed an Effective reversible data hiding in encrypted image with privacy protection for image content. In this technique the content owner firstly encrypts the image using an appropriate encryption key so that the data hider has no idea about the original content of the image. Here according to the secret bits for embedding the data hider modifies some LSB layers of some selected pixels in the encrypted image. Also here only few number of pixels are modified which leads to better visual quality. At the receiver side using the key the receiver can easily decrypt the marked encrypted image, also the hidden data can be perfectly extracted by utilizing the image smoothness characteristics. This method has improved visual quality.

In [8] Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. proposed a new framework for reversible data hiding in encrypted domain. Here the original pixels in the plain image are divided into various sub-blocks of size m x n and using an encryption key a key stream is generated and using that the pixels in the sub-blocks are encrypted. After that using a permutation key the sub-blocks are randomly permuted. Here the correlation between the adjacent pixels in the sub-blocks are maintained so that any reversible data hiding technique can be used here. Since reserving room before encryption is used the data hiding process is effortless. Basically here the room is reserved by exploiting the spatial correlations in the image. In this method the embedding capacity is large and pure reversibility can be achieved. Sometimes this method becomes impractical because it requires the content owner to perform an extra preprocessing before content encryption.

In [9] Nuzhat Ansari and Rahila Shaikh proposed a keyless approach for reversible data hiding in encrypted images using visual cryptography. Maintaining the confidentiality and privacy of images is an important issue to be solved, for that various encryption schemes were proposed. Basically there are two types of encryption, encryption with keys and without keys. In the first method encryption is done by suitable encryption algorithm using keys whereas in the second method the image is partitioned into random shares, here keys are not used. This paper is based on the second method ie, the keyless encryption. Since the image is divided into various shares the secrecy can be maintained. None of the shares reveal any information about the host image. Also here the difficulty in key management can be eliminated. For recovering the host image the receipt has to know about all of the shares. SDS algorithm is used here and it mainly consists of three steps, sieving, division and finally shuffling. Here the decryption is done without computation ie, the image is recovered using human visual system moreover various computation is involved during encryption and decryption and the results are viewed on the computer screen and so it is normal to use the additive color mode.

In [10] Pauline Puteaux and William Puech Proposed Reversible data hiding in encrypted images based on adaptive local entropy analysis. Here the transmitter side consists of two classic steps. First one is the image encryption with a secret key and second one is the secret message embedding by using a data hiding key. For the decoding scheme if the receipt has only the data hiding key, the

secret message can be extracted. But the limitation is that inorder to reconstruct the original image one have to know both the keys. Here for recovering the original image blocks a local entropy analysis is performed. In this approach the payload is smaller.

Pauline Puteaux and William Puech proposed an efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images, in which they described about two main approaches [11]. First one is the high capacity reversible data hiding with correction of prediction errors and second one is the high capacity reversible data hiding with embedded prediction errors [11]. In the first method higher payload can be achieved while the reconstruction can be done approximately whereas in the second method reconstruction can be done perfectly but the payload is lesser since we are embedding the location of prediction errors in the image itself. Based on the application we can choose which is one is better for the corresponding application. Here the whole process consists of various steps like prediction error detection, MSB error consideration, image encryption, data hiding by using the MSB replacement method and finally data extraction and image recovery. In the data extraction and image recovery stage there are three options, if the receipt has only the data hiding key then only the data extraction can be done, if the receipt has only the encryption key then the image can only be recovered and if the receipt has both the keys then data extraction as well as the image recovery can be done simultaneously. The usage of keys in this method will lead to the improved security. The data hiding rate which can be obtained in this scheme is 1 bits per pixel.

Paper Title	Authors	Year of Publication	Advantages	Short comings
"High embedding reversible data hiding scheme for JPEG" [2]	Kuo, Wen-Chung, Shao-Hung Kuo, and Lih-Chyau Wuu	2010	The proposed algorithm solves both the security issues as well as the bandwidth requirement.	Low embedding capacity, Low PSNR.
"Reversible data hiding in encrypted image" [3]	Zhang, Xinpeng	2011	The benefits of the scheme are high embedding capacity and faster implementation	Errors may occur in the image recovery and data extraction as well.
"Separable reversible data hiding in encrypted image" [4]	Zhang, Xinpeng	2011	The proposed scheme requires minimum memory space and it has better image reconstruction, practically more applicable.	Embedding capacity is low and for high embedding capacity it can only generate low quality marked image
"Reversible data hiding in encrypted images by reserving room before encryption" [5]	Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li	2013	This method has some benefits such as embedding capacity is higher and better reversibility can be achieved .	The main limitation of this technique is that reserving room before encryption is not practically applicable. Also even if the errors can be minimized the complexity is comparatively higher
"Encrypted signal-based reversible data hiding with public key cryptosystem" [6]	Chen, Yu-Chi, Chih-Wei Shiu, and Gwoboa Horng	2014	This method allow the user to operate the encrypted data directly without decryption.	Computation complexity is higher and low embedding capacity.
"Effective reversible data hiding in encrypted image with privacy protection for image content" [7]	Qin, Chuan, and Xinpeng Zhang	2015	This method has improved visual quality, high embedding capacity.	This scheme also has some drawback such as anyone with the encryption key can decrypt the image and also the presence of hidden data can be easily identified
"New framework for reversible data hiding in encrypted domain" [8]	Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi	2016	Since reserving room before encryption is used the data hiding process is effortless. embedding capacity is large and pure reversibility can be achieved	The main drawback is sometimes this method becomes impractical because it requires the content owner to perform an extra preprocessing before content encryption.
"A keyless approach for RDH in encrypted images using visual cryptography" [9]	Miss, Nuzhat Ansari, and Rahila Shaikh	2016	Keyless encryption and the decryption is done without computation ie, the image is recovered using human visual system	Algorithm is not Robust, low embedding capacity
"Reversible data hiding in encrypted images based on adaptive local entropy analysis" [10]	Pauline Puteaux and William Puech	2017	Provides high security to the image.	Limitation is that inorder to recover the host image one have to know both the keys
"An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images" [11]	Pauline Puteaux and William Puech	2018	The usage of keys in this method will lead to the improved security, improved reconstruction quality.	Embedding capacity is smaller

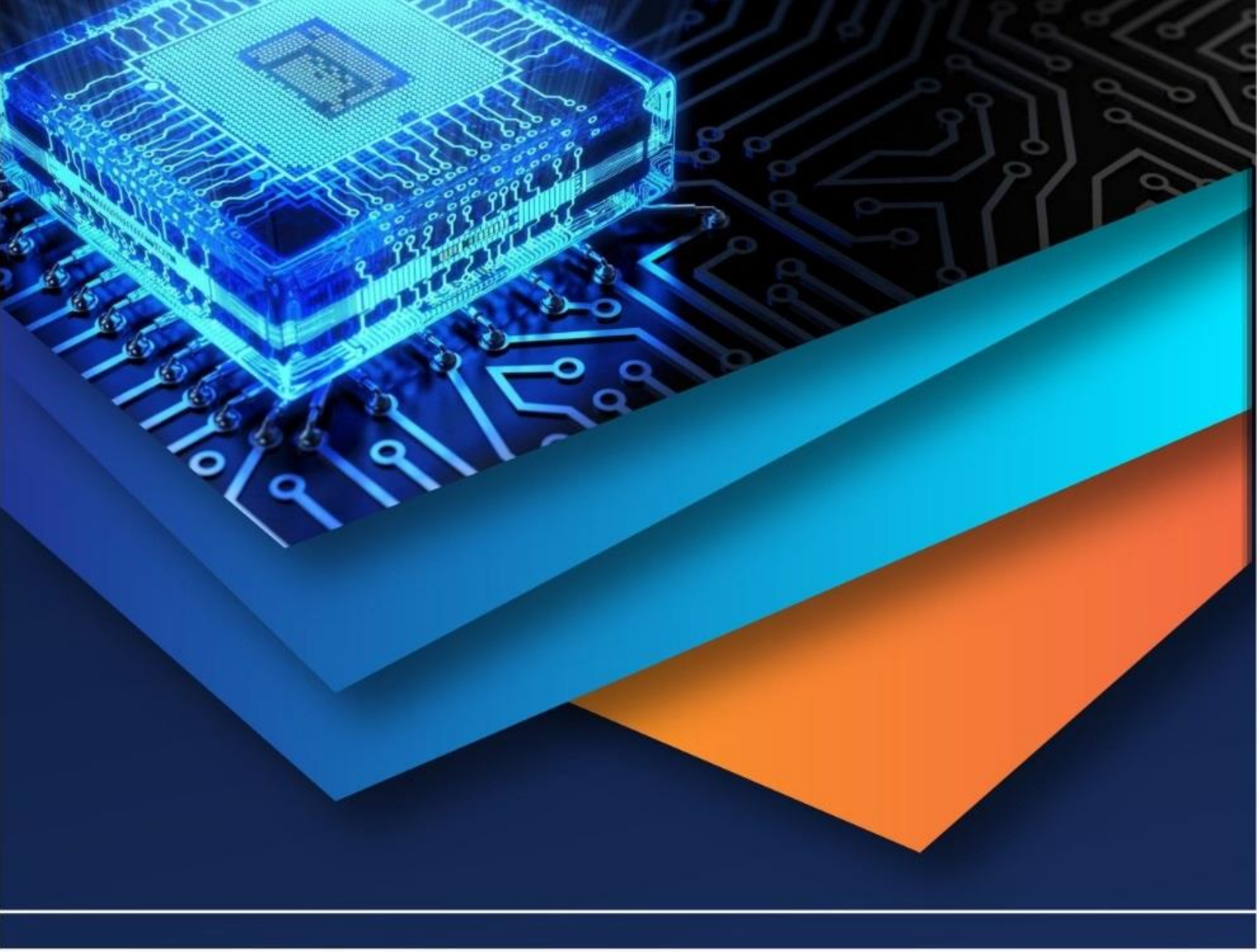
Table 1: Literature Survey Comparison Table

III. CONCLUSION

This paper presented a review on various existing reversible data hiding in encrypted environment techniques. Reversible Data Hiding In Encrypted Images is one of the topic receiving huge attention because of the need for high security requirement in many applications. Reversible image data hiding schemes mainly consists of various phases like image encryption, hiding of the secret data and finally the data extraction and the host image recovery. In general all the reversible data hiding in encrypted images can be classified into two categories, the methods by vacating room after the encryption process and the methods by reserving room before the encryption process [11]. Depending on the application one can choose which method has to be adopted. These techniques gives better security when compared to various existing methods for security. In the future research on reversible data hiding in encrypted images better encryption algorithms can be incorporated for achieving better security.

REFERENCES

[1] Shish, B. M. Rizwan, and Q. Abbas Ahmad, "Energy Saving Secure Framework for Sensor Network Using Elliptic Curve Cryptography," IJCA Special Issue on Mobile Ad-Hoc Networks, pp. 167-172, 2010.
[2] Wen-Chung, Shao-Hung Kuo, and Lih-Chyau Wuu Kuo, "High embedding reversible data hiding scheme for JPEG," In 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 74-77, 2010.
[3] Xinpeng Zhang, "Reversible data hiding in encrypted image," IEEE signal processing letters 18, vol. 18, no. 4, pp. 255-258, 2011.
[4] Xinpeng Zhang, "Separable reversible data hiding in encrypted image," IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826-832, 2011.
[5] Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li Ma, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Transactions on information forensics and security, vol. 8, no. 3, pp. 553-562, 2013.
[6] Yu-Chi, Chih-Wei Shiu, and Gwoboa Horng Chen, "Encrypted signal-based reversible data hiding with public key cryptosystem," Journal of Visual Communication and Image Representation, vol. 25, no. 5, pp. 1164-1170, 2014.
[7] Chuan, and Xinpeng Zhang Qin, "Effective reversible data hiding in encrypted image with privacy protection for image content," Journal of Visual Communication and Image Representation, vol. 31, pp. 154-164, 2015.
[8] Fangjun, Jiwu Huang, and Yun-Qing Shi Huang, "New framework for reversible data hiding in encrypted domain," IEEE transactions on information forensics and security, vol. 11, no. 12, pp. 2777-2789, 2016.
[9] Nuzhat Ansari, and Rahila Shaikh Miss, "A keyless approach for RDH in encrypted images using visual cryptography," Procedia Computer Science, vol. 78, pp. 125-131, 2016.
[10] Pauline Puteaux and William Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," In 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 1-6, November 2017, 10.1109/IPTA.2017.8310143ff. fflirmm-01889962f.
[11] Pauline Puteaux and William Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1670-1681, January 2018, ff10.1109/TIFS.2018.2799381ff. ffhal-01771437f.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY