

# International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 9, Issue 9, September 2020



TERNATIONAL

Impact Factor: 7.122

🖂 ijareeie@qmail.com @ www.ijareeie.com 9940 572 462 S 6381 907 438 



| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 9, September 2020 ||

### A Review on Reversible Data Hiding (RDH) Techniques

Priyanka Varathe<sup>1</sup>, Dr. Anil Khandelwal<sup>2</sup>

PG Student [Digital Communication], Dept. of ECE, VNS Group of Institutions, Bhopal, Madhya Pradesh, India<sup>1</sup> Assistant Professor, Dept. of ECE, VNS Group of Institutions, Bhopal, Madhya Pradesh India<sup>2</sup>

**ABSTRACT**: With the development in cloud storage and privacy protection, reversible data hiding in encrypted images (RDHEI) has increasing attention towards the technology that can embed additional data in the encryption form.[1] Reversible data hiding is a technique by using which we can embed essential data into images, audio, video and so on. This system applies a method of hiding data in an image and video by reserving room before encryption. The proposed conspire builds the measure of data that can be covered up in the picture or video which likewise ensures the lossless recuperation of picture or video after extraction is finished. All the past strategies for reversible data stowing away were grown with the end goal that they were clearing space for data covering up subsequent to scrambling the picture, which brings about presentation of some blunder rates at the hour of data extraction and picture recuperation. It is otherwise called new watermarking method which is utilized to verify a picture and video by inserting some data in it.

KEYWORDS: RRBE, RRAE, RDH, ABE, encryption, partitioning, self reversible embedding.

#### **I.INTRODUCTION**

Image encryption and data hiding are two main means for data security. The former aims to transform the meaningful image into a noise-like one to prevent image content leakage while the latter embeds secret data into a cover image imperceptibly. In image encryption, the original image is the one to be protected, while, in data hiding, the secret data is the information that should be undisclosed.[2] Traditional data hiding technology is usually irreversible, and the embedding process will bring permanent distortion to the original carrier, which is not accepted in some cases such as military images, medical images, and judicial evidence collection where the original carrier needs to be restored without distortion. Take into account requirements of lossless recovery of the original carrier, reversible data hiding (RDH) was proposed.

Presently a-days security is considered as most significant basic factor in any correspondence frameworks. Issues in such security frameworks are uprightness, protection, validation and non-renouncement, such issues must be taken care of cautiously. Here the security objectives are to be specific: secrecy, accessibility and trustworthiness that can be compromised by security assaults. So to shield the first data from such assaults the data concealing strategies are actualized. To keep up the security and validation, Reversible Data Hiding i.e. RDH strategies are identified with steganography and cryptography work [3]. Encryption and data stowing away are two strategies of data assurance. Data concealing procedures installs unique data which we would prefer not to reveal into spread media by presenting slight adequate alterations, while encryption methods changes over plaintext data into indistinguishable structure for example cipher text. It is valuable to install the data into a computerized media to impart the mystery messages. The proprietor can change the first substance of the media utilizing pictures, with the goal that the inserted data is hidden.[4] Encryption gives privacy to pictures and video just as it is successful procedure which changes over the first and mystery data to inconceivable one. On the off chance that we can apply RDH to scramble picture, at that point some great applications can be created through it. For instance: Suppose that a clinical picture data base put away in some server farm, at that point a few documentations can be implanted into the encoded adaptation of a clinical picture through a RDH procedure by a worker in the server farm. The worker can deal with the picture or confirm its respectability by utilizing the documentations without having the data on the first substance. This will ensure the patient's protection. Simultaneously, a specialist can unscramble and re-establish the picture for additional diagnosing by utilizing the cryptographic key.



#### | e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

#### || Volume 9, Issue 9, September 2020 ||

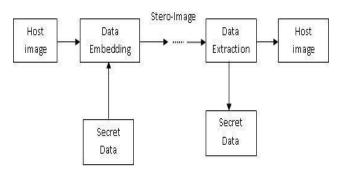


Figure 1: Block diagram of RDH

Reversible data stowing away in pictures or recordings is a strategy, by which the first substance can be recouped without misfortune after the implanted data is extricated. This method can be generally utilized in different fields, for example, clinical, military and law criminology, where mutilation of the first spread isn't permitted. Reversible data concealing strategy is utilized to implant extra data into spread media, for example, picture or video. As of late numerous new RDH methods are created which gives an overall structure for RDH. It works by first extricating the highlights of the first spread media and afterward compacting them without misfortune, additional room can be spared by implanting assistant data. All past techniques for RDH implant data by reversibly removing room from the encoded pictures, which may prompt a few mistakes while data is being separated and additionally picture is being re-established. Here a novel technique with a customary RDH calculation by saving room before encryption is proposed, and hence it isconceivable to reversibly install data in the scrambled picture and recordings. Goal of this framework is to accomplish method of made sure about transmission of profoundly delicate data over the web. Data stowing away into spread media, forexample, video is one of the difficult assignment contrasted with data covering up in pictures, however as recordings are safer path for inserting secure data than pictures, in proposed strategy it is conceivable to shroud the data in recordings by utilizing open key cryptography. In this framework, a novel strategy by saving room before encryption with a customary RDH calculation is proposed.

#### **II.RELATED WORK**

There are various techniques which provide security that are defined following:

#### A. Cryptography:

Cryptography is an art of securely transferring the message from sender to receiver. It uses the key concept for encryption the message data known as cryptography. It is used when communicating over the untrusted media such as internet. Cryptography is the technique that used in securely transfers the data with the use of algorithm which is unreadable by the third-party.

#### B. Categories of cryptography

#### *a) Symmetric-key cryptography:*

Symmetric-key cryptography is the technique that performed encryption and decryption by using single key. It is also known as secret key encryption.

#### **b)** *Asymmetric-keycryptography*:

It is also known as the public-key cryptography. In this two keys are used, one for encryption i.e. public and another for decryption i.e. decryption.

#### c) Hash Encryption:

Hash encryption performed by using the hash function. It provides security to user by using this concept. It produces fixed length signature for a message.

Here our concern with image encryption. Image encryption technique is different from simple encryption. The data hiding in image takes place following four steps thatare:

- Select the medium or carrier.
- Message which needed protection.
- A function that will be used to hide data in the cover media.
- Alternative key which provide authentication.



| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

#### || Volume 9, Issue 9, September 2020 ||

#### C.Types of Imagecryptography/Encryption

- a) Generation of encryption-key: It is generated by randomly by using random function. It uses 128-bit of value.
- **b**) Generation of pseudo-random sequence: It is generated by using encryption-key. For example RC-4 algorithm used to generate the pseudo random sequence using 128-bit encryption key.

#### D. Steganography:

Steganography word takes from Greek word that is made up of two words such as "stegan" and "graphy", it means cover or secret writing. It deals with composing hidden messages. It is the way of hiding data without the knowledge of third-party. Steganography provides the security to the message as well as content of the data. It is an art of hiding data by embedding messages within other, seemingly harmless messages. Steganography perform using three media:

- Hiding a message inside "text".
- Hiding a message inside" images".
- Hiding a message inside "audio" & "video".

It is the process of hiding a secret message within the carrier such as image, text, and audio.

#### E. Data hiding techniques:

Mainly the data hiding techniques are classified into two techniques:

#### 1. Reversible data hiding technique:

In this technique the message signal as well as the original cover can be with no loss recovered simultaneously.

#### 2. Irreversible data hiding technique:

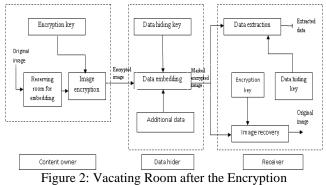
In this technique the message signal can be recovered with no loss but the original cover can be lost. So in general reversible data hiding techniques can be used now a days. Method of reversible data hiding are reserving room before encryption and vacating room after encryption as givenbelow:

#### *a)Vacating Room after the Encryption:*

In this method first encrypt the original image using the cipher with the encryption key. Next to this it is given to the data hider to hide some auxiliary data in it by with no loss vacating the room required for data hiding key. At receiver the content owner or an authorized third party can be extract the embedded data with the help of data hiding key and also recover the original image according to the encryption key. This method compresses the encrypted LSBs of image to vacate the room for additional data.

#### b) Reserving room before the encryption:

Vacating room from the encrypted images losslessly is sometimes difficult and not efficient, so if we reverse order of encryption and vacating room, i.e., reserving room before image encryption, the RDH tasks in encrypted images would be more natural and much easier which gives the novel framework, reserving room before encryption (RRBE). [5]





| e-ISSN: 2278 - 8875, p-ISSN: 2320 - 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 9, September 2020 ||

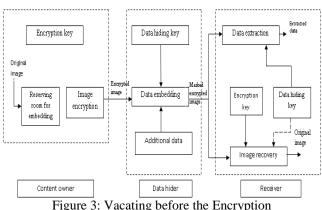


Figure 5: Vacating before the Encryption

There are some standard RDH algorithms available which are ideal for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. [4] This is because in this new framework, follow the customary idea that first lossless compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

#### **III.PERFORMANCE ANALYSIS OF A REVERSIBLE DATA EMBEDDING ALGORITHM:**

Data embedding in the reversible manner which is the data embedding without any loss embeds the data or payload into digital image in reversible manner. After data embedding the quality of original image may be degraded which is to be avoided. The attractive property of data embedding in reversible manner is reversibility, which is after data extraction the original quality image is restored back. Reversible data embedding hides some data in a digital image in such a way that an approved party image to its original state. The presentation of a reversible data-embedding algorithm can be measured using following,

- Data embedding capacity limit
- Visual quality
- Complexity

The data without any distortion embedding is the attractive feature of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be pleasing, particularly in military data and medical data. In such a circumstances, every small part of data is important.

From the application point of view, since the differentiation between the implanted image and original image is almost discernible from human eyes, reversible data implanting could be thought as a top secret communication channel since reversible data implanting can be used as an data transporter.

#### **IV.LITERATURE SURVEY**

A lot of examination on reversible data covering up has been done in the course of recent years. Some significant procedures are talked about here. Different methods have been proposed and research has been done in the field of reversibledata stowing away. Likewise many progressed strategies have been presented for reversible data covering up and visual cryptography. Some examination work in the territory of reversible data covering up is shown underneath:

Wei Liu et al. [7] in this proposition, goal dynamic pressure conspire is utilized which packs an encoded picture dynamically in goal, with the end goal that the decoder can watch a low goal variant of the picture, study nearby measurements dependent on it, and utilize the insights to decipher the following goal level. The encoder begins by sending a down inspected rendition of the code text. At the decoder, the comparing low-goal picture is decoded and unscrambled, from which a higher-goal picture is acquired by intra-outline forecast. The anticipated picture, along with the mystery encryption key, is utilized as the side data (SI) to translate the following goal level. This cycle is iterated until the entire picture is decoded. So this multi-goal approach makes it conceivable to approach part of the spatial source data to produce more solid spatial and worldly side data. Be that as it may, there is have to expand the proficiency of in general data pressure to evade the loss of any sort of data.

W. Puech et al. [8] proposed an investigation of the nearby standard deviation of the checked scrambled



#### | e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

#### || Volume 9, Issue 9, September 2020 ||

pictures so as to eliminate the installed data during the decoding step for assurance of mixed media dependent on Encryption and watermarking calculations depend on the Kirchhoff's guideline, all the subtleties of the calculation are known, and just the way to encode and unscramble the data ought to be mystery. The first is when there is homogeneous zones all squares in these zones are encoded in a similar way. The subsequent issue is that square encryption techniques are not strong to commotion. For sure, due to the huge size of the obstructs the encryption calculations per square, symmetric or lopsided can't be hearty to clamor. The third issue is data honesty. The blend of encryption and data covering up can take care of these sorts of issues subsequently by utilizing this methodology a reversible data concealing strategy for encoded pictures can implant data in scrambled pictures and afterward to unscramble the picture and to remake the first picture by eliminating the shrouded data yet it is preposterous to expect to utilize when high limit reversible data concealing technique for encoded pictures.

Christophe Guyeux et al. [9] built up another system for data concealing security, called confusion security. In this work, the connections among the two thoughts of security is developed and the convenience of mayhem security is explained, by introducing a novel data concealing plan that is twice stego and disarray secure. The point of this methodology is to demonstrate that this calculation is stego-secure and disarray secure, to contemplate its subjective and quantitative properties of flightiness, and afterward to contrast it and Natural Watermarking. A portion of the probabilistic models are utilized to order the security of data concealing calculations (Runge-Kutta calculation) in the Watermark Only Attack (WOA) structure. Subsequently technique has the subjective property of topological blending, which is helpful to withstand assaults yet can't be applied in KOA and KMA (Known Message Attack) arrangement because of its absence of expansively conspires which are far reaching.

Imprint Johnson et al. [10] proposed the oddity of switching the request for these means, i.e., first encoding andafterward compacting, without bargaining either the pressure proficiency or the data hypothetical security. In this strategy first data encryption is utilized and afterward the encoded source is compacted yet the blower doesn't approach the cryptographic key, so it must have the option to pack the scrambled data with no data on the first source. From the start, it creates the impression that solitary an insignificant pressure gain, assuming any, can be accomplished, since the yield of an encode or will look irregular. Nonetheless, at the collector, there is a decoder wherein both decompression and unscrambling are acted in a joint advance. In an expansive range in this methodology, the encoded data can be compacted utilizing appropriated source-coding standards as the key will be accessible at the decoder however sometimes the chance of first scrambling an data stream and afterward packing where blower doesn't know about the encryption key.

Jun Tian et al. [11] proposed reversible data installing which is likewise called lossless data inserting which implants imperceptible data into a computerized picture in a reversible style. As an essential necessity, the quality debasement on the picture after data implanting ought to be low. An enamoring highlight of reversible data installing is the reversibility for example one can eliminate the implanted data to reestablish the first picture. A typical methodology of high limit reversible data inserting is to choose an implanting zone for assume; the least noteworthy pieces of certain pixels in a picture and install both the payload and the first qualities around there required for accurate recuperation of the first picture into such territory. Here DE (distinction extension) method which finds additional extra room by investigating the repetition in the picture content too, DE procedure utilized to reversibly implant a payload into advanced pictures. The primary hugeness of this strategy is the payload limit and the visual nature of implanted picture is controlled as well as lossy compacted the decoder will discover it isn't bona fide and accordingly there will be no unique substance reclamation.

Patrizio Campisi et al. [12] present a novel strategy to indiscriminately assess the nature of a media correspondence interface by methods for an unusual utilization of advanced delicate watermarking. Data stowing away by computerized watermarking is typically utilized for interactive media copyright insurance, validness confirmation, or comparative purposes. Watermarking is here received as a strategy to give a visually impaired proportion of the nature of administration in interactive media interchanges. The overall watermark implanting system comprises of installing a watermark succession which is generally paired into have data by methods for a key. In the discovery stage the key is utilized to check the nearness of the installed succession. Concerning the area where the watermark installing happens which can recognize strategies working in the spatial space, DCT space, Fourier change area and in the wavelet change area and it permits one to aimlessly gauge the Quos gave by a coder/channel framework without influencing the nature of the video-correspondences yet has unpredictability of the Quos assessment methodology seems insignificant in correlation with MPEG-2/4 translating and versatile on-board exhibit handling.

StephaneBounkong et al. [13] approach can be utilized on pictures, music or video to implant either a powerful or delicate watermark. On account of hearty watermarking the technique shows high data rate and heartiness against malevolent and no pernicious assaults, while keeping a low actuated bending. This strategy depends on



#### | e-ISSN: 2278 - 8875, p-ISSN: 2320 - 3765| www.ijareeie.com | Impact Factor: 7.122|

#### || Volume 9, Issue 9, September 2020 ||

identified with a least critical piece adjustment in the ICA area. ICA permits the amplification of the data substance and minimization of the actuated twisting by disintegrating the spread content (for this situation the picture) into measurably autonomous sources. Installing data in one of these autonomous sources limits the developing crosschannel impedance. Actually, for an expansive class of assaults and fixed limit esteems, one can show that twisting is limited when the message is implanted in measurably autonomous sources, this very straightforward change encourages the utilization of Bayesian deciphering methods. As this strategy depends on inserting data utilizing factually free sources the equivalent watermarking technique can be effortlessly applied across various media however it needs extra security in the utilization of explicit blending/demising frameworks that are difficult to acquire.

Boato et al. [14] presents a novel strategy for the protected administration of advanced pictures detailed inside the numerical hypothesis of polynomial addition as fundamental spearheading highlights. This work depends on a various leveled joint responsibility for picture by a confided in layered power and on a deterministic watermarking methodology, implanting a short significant or arbitrary mark into the picture. To show the outcomes here the mark written in English letters in order is first converted into a succession of whole numbers by methods for a look-into table. Such an arrangement of numbers is utilized to set the coefficients of a geometrical polynomial from which a predefined number of tests is separated assessed at similarly divided focuses. At long last, the estimations of the examples are installed into the most minimal recurrence coefficients of the first picture changed into the DCT space barring the DC segment a superior is acquired as far as bogus identification even in basic circumstances or sensible measure of picture corruption because of the picture preparing administrators, for example, separating, mathematical distortion(s) and compressions however progressive plan isn't constrained by the sort of watermarking method embraced because of which it is inclined to the vindictive assaults. Henceforth need to have more valuable and hearty strategies to dodge such assaults.

Abd-el-Kader H. Ouda et al. [15] proposed the Work for security of Wong's procedure is defenseless against cryptographer's assaults. This is because of the utilization of short keys in the open key cryptosystem. Short keys are utilized in Wong's method to make the watermark sufficiently little to fit in a picture square. Another technique for applying the cryptographic hash work is used. This technique makes the picture squares ready to hold longer and secure watermarks while giving comparative degree of the confinement precision. Here they used MD5 calculation to accomplish a significant level of confinement precision however the security imperfections of MD5 are predefined henceforth known to all because of which it is inclined to the wear security assaults mulling over to the non-dependability.

G. Boato et al. [16] proposed a novel technique for steganography picture watermarking with two fundamental imaginative highlights i.e., it includes a progressive control, submitting the watermark reproduction to a believed layered position and it is deterministic, installing a short important mark into the spread picture. In this technique they took a mark written in English letters in order and made an interpretation of it into a succession of whole numbers with reasonable look into table. Next, they distinguished it with the coefficients of a geometrical polynomial and implant a repetitive number of tests of the polynomial assessed at similarly separated focuses into the most minimal recurrence coefficients of the DCT lattice barring the DC part. As a rule by utilizing this strategy it is conceivable that the installed mark can be precisely recouped even in nearness of a sensible measure of picture debasement because of picture handling administrators however it gets no opportunity to oppose against the assault by embeddings different watermarking.

HuipingGuo et al. [17] proposed a novel technique that utilizes a summed up mystery sharing plan in cryptography to address the issue of picture watermarking. In this plan, given that various proprietors make a picture mutually unmistakable keys are given to just an approved gathering of proprietors so just when all the individuals in the gathering present their key sweep the responsibility for picture be confirmed. This cycle depends on summed up mystery sharing plan, various watermarks, one for every proprietor's critical and one for the mystery key are inserted with the goal that both full possession and halfway possession can be confirmed. Spread range watermarking plans, quantization watermarking plans for the most part quantize the estimations of host pictures spatial area or in the range space to a pre determined arrangement of qualities as indicated by paired watermarking pieces. Hence, the watermark data is totally contained in the watermarked pictures and the watermarking locator can recognize the inserted watermark indiscriminately. By utilizing this plan they accomplished two significant results

1. Access structure is more adaptable under a mystery sharing plan. In the event that a mystery sharing plan isn't spatially multiplexed into the picture, we have no real way to control the approved set wherein members can mutually confirm proprietorship.

2. Secondly the protected mystery based watermark is inserted to build up a safe association between proprietors. However, because of different watermarking there is probability of loss of information because of which the watermarked picture might be mutilated influencing the first information.



| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 9, September 2020 ||

Cerou, et al. [18] examines a novel procedure for recreating uncommon occasions and a related Monte Carlo assessment of tail probabilities. This strategy utilizes an arrangement of interfacing particles and adventures a Feynman-Kac portrayal of that framework to investigate their changes. This exact examination of the change of a standard staggered parting calculation uncovers an open door for development. This work proposes a comparable calculation including the utilization of amounts of the irregular variable on the multitude of particles so as to appraise the following level. The fundamental distinction is their two phase strategy they previously run the calculation just to process the levels and afterward they restart from the earliest starting point with these proposed levels. Very this technique it is indicated thatby processing the levels on the fly inside a similar run as the one to register the uncommon occasion likelihood paid a little predisposition on the gauge. They fundamentally guarantee that from a down to earth perspective one should support the variations without predisposition in the ideal gauges however for security reason against plot codes presently can't seem to be utilized.

#### V. CONCLUSION

With the expanded utilization of web, proposed framework centres basically around RDH as the made sure about method of discussing over unreliable channels of web. Reversible information covering up in encoded pictures is another subject getting consideration due to the made sure about natural prerequisites. Information stowing away in reversible way in scrambled pictures is giving twofold security to the information, for example, picture encryption just as information covering up in encoded pictures both are done here. The current framework contains a few burdens so the future degree is to eliminate the detriments by including reversible way implies, information extraction and recuperation of picture are liberated from mistakes. The PSNR will be improved to get unique spread back. In future it might conceivable that memory space can be saved before encryption which requires less measure of time for information extraction and picture recuperation.

#### REFERENCES

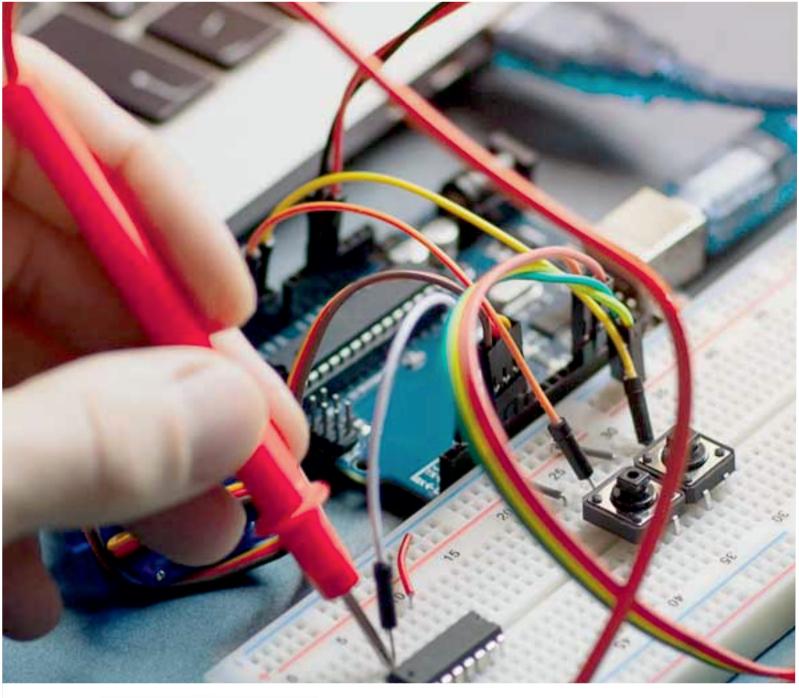
- Yin, Zhaoxia & Xiang, Youzhi & Zhang, Xinpeng. (2019). Reversible Data Hiding in Encrypted Images Based on Multi-MSB Prediction and Huffman Coding. IEEE Transactions on Multimedia. PP. 1-1. 10.1109/TMM.2019.2936314.
- [2] Dewang Wang, Xianquan Zhang \*, Chunqiang Yu \* and Zhenjun Tang (18 March 2020) Reversible Data Hiding in Encrypted Image Based on Multi-MSB Embedding Strategy.
- [3] Y. Puyang, Z. Yin, and Z. Qian, "Reversible Data Hiding in Encrypted Images with Two-MSB Prediction," IEEE International Workshop on Information Forensics and Security (WIFS), 2018.
- [4] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology,DOI 10.1109/TCSVT.2015.2433194.
- [5] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," IEEE Trans. Data Forensics & Security, 8(3), pp. 553- 562,2013.
- [6] Shweta Patil Student, Electronics Amrutvahini college of engineering, Sangamner Maharashtra, India," Data Hiding Techniques: A Review" International Journal of Computer Applications (0975 – 8887) Volume 122 – No.17, July2015.
- [7] Wei Liu, WenjunZeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted GrayscaleImages", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102.
- [8] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for EncryptedImages", SPIE, IS & T'08: SPIE Electronic Imaging, Security, Forensics, Steganography And Watermarking of Multimedia Contents, San Jose, CA,USA.
- [9] Christophe Guyeux, Nicolas Friot, and Jacques M. Bahi, "Chaotic iterations versus Spread-spectrum: chaos and stego security", January 25-2011, IIHMSP,pp.208-211.
- [10] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramchandran, "On compressing and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.
- [11] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 -896.
- [12] PatrizioCampisi, Marco Carli, Gaeta no Giunta and AlessandroNeri, "BlindQualityAssessmentSystem for Multimedia Communications using Tracing Watermarking" IEEE Transactions on Signal Processing, Vol 51, No 4, Apr 2003, pp. 996–1002.
- [13] S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images," Journal of Machine Learning Research, vol. 1, pp. 1–25,2002.



| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 9, Issue 9, September 2020 ||

- [14] G. Boatoa, F.G.B.DeNatalea, C. Fontana rib, F. Melgania "Hierarchical ownership and deterministic watermarking of digital images via polynomial interpolation", Signal Processing: Image Communication 21 (20 0 6), pp.573–585.
- [15] A.H. Ouda, M.R. El-Jakka, "A practical version of Wong's watermarking technique", Proc. ICIP (2004)2615– 2618.
- [16] G. Boato, C. Fontanari, and F. Melgani "Hierarchical deterministic image watermarking via polynomial interpolation" Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14Sept-2005.
- [17] H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems 9 (3) (2003).
- [18] Frederic Cerou, PierreDel Moral, Teddy Furon and Arnaud Guyader, "Sequential Monte Carlo for rare event estimation" Statistics and Computing, pp. 1–14, 2011.





Impact Factor: 7.122





## International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering





www.ijareeie.com