ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

Review on Reversible Data Hiding In Encrypted Images

Amit Kumar Goel

Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India

Email Id: drgoelkamit@gmail.com

ABSTRACT: Cryptic photos Reversible data (CRI) hides in the hashing algorithm with the capacity to listlessly retrieve the unique content. Strategy hides extra information into the hash algorithm. Several approaches have been recommended on this matter in recent years. In this paper propose an alternative RDH-EI method, which can produce a very broad embedding potential through the transformation of an efficient reversible integer. The top photo is separated first into sections that are not overlapped. We release the built-in room to accommodate the supplementary data and payload with a neural network of adaptive minimally invasive integer metamorphosis. The cloud service will cover many more details into the hashing algorithm through embedded support data after file authentication and upload. The method is versatile so as to be able to extract additional information accurately and restore the actual image without distortion. The proposed solution will achieve significantly higher watermarking efficiency and a far higher proportion of quality compared to state-of-the-art approaches.

KEYWORDS*:* Reversible data hiding Image encryption Integer transformation Adaptive embedding

I.INTRODUCTION

Hiding Reversible Information (RDH) is a picture reversible technique for adding additional data, ensuring that incorporated images and the initial image are retrieved slowly. In general, there are three types of HDR methods, namely, methodologies based on compression, methods premised on expansion, and methods based on waveform monitor modification. There seems to be a range of JPEG image RDH methods in which the constraint domain provides additional parts. RDH is implemented in the encrypted framework in recent decades. An image controller can periodically encrypt and transfer the photo to the remote server in cloud computing or the internet of things. The cloud provider will hope to add additional information to the authenticated picture for easy control, e.g. initial records, time-signs or notes. In the meantime, the processor should be able to obtain the encoded information correctly, and after decryption, the origination fee should be able to restore the quality content. The RDH technology in encoded pictures (RDH-EI) is tested in this case. As the chart revealed. 1, RDH-EI with two forms, E-mail: encryption vacant room, and encryption vacation room. The embedding of the encryption image is created by the secure server specifically with VRAE technologies. Three groups of VRAE approaches are available. Information in plaintext domain is taken in the first range. A researchers also suggest that the picture be encrypted utilizing AES and that one bit be inserted in a random location of each element. On the beneficiary dimension, the local defect of a block is examined to recreate the actual image and retrieve the unknown data. In Zhang recommends swapping several least significant bits (LSBs) inside each anti-overlapped section of the authenticated file[1]–[6]. The embedded data can be collected and the initial image collected together after the picture decryption, depending on the variability of the picture block.

Hong et al. in strengthen the algorithms. In, the integration efficiency is enhanced with a method for public-key synchronization. In addition, the first RED-EI approach for JPEG images was introduced by Qian et al. Due to the combination of batch processing and picture regeneration, these approaches are also named joint RDH-EI. The second category is the RDH-EI dividing data retrieval and object restoration. Zhang introduces the first form of separation in which LSBs are condensed to create opportunities for data decoding for the authenticated file. Several approaches

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

vacate integrating space by deforming encrypted bits[2]–[8]. For instance by compacting encrypted with low-density parity control (LDPC) codes and by measuring the difference between both the vector LSB source and supplementary channel Hamming that is planned to use Golomb-Rice codewords to use an arbitrary RDH for authenticated space, enhancing picture safety and quality in one of paper, alternate RDH-EIs for ciphertext dependent on block encryption. In comparison, several different JPEG image RDH-EI methods often unlock the room following encryption. Information extraction for both encrypted and decrypted domains is feasible in the third category VRAE. Or use a pseudo-random pattern modulation method, a code hider embeds additional information after picture encryption to safe removal of both domains. Most techniques derive data from the two realms by integrating data into non-encrypted areas. In one of the paper the public-key cryptosystems are introduced by RDH-EI. The receiver will remove part of both the concealed data until decryption, extract part of a concealed data and recapture the actual image after authentication by way of digital audio, irreversible variations[9]–[14]. By "Paillierhomomorphic cryptography the copyright holder preprocesses the actual image. In order to produce the given encoded image, a bit is placed from each pair of neighboring encrypted pixels. The recipient contrasts all pairs of decoded pixels to remove the built-on bit and retrieves the actual image predicated on the Paillier encryption property" as shown in Figure 1.

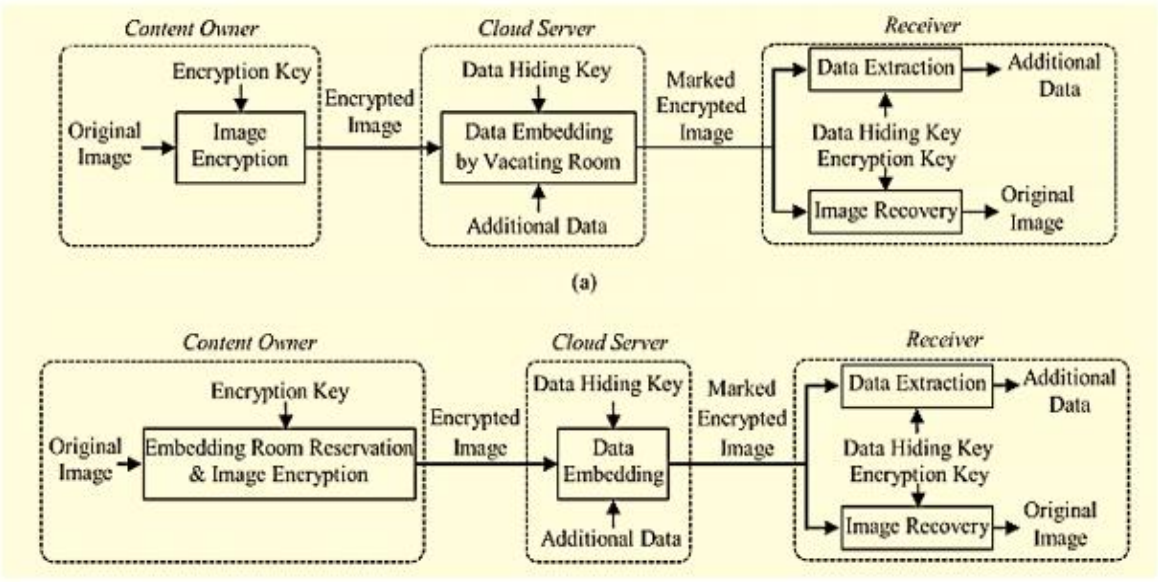

Fig.1: Two Kinds of RDH-EI, a) Vacating Room after Encryption (VRAE), b) Vacanting Room Before Encraption (VRBE)

II.PROPOSED METHOD

As Fig shows. 2, three separate phases are protected by the proposed RDH-EI system. In the first phase, the alleged infringer essentially turns the actual image I to vacate an incubator with an adaptive reversible integer transformation and encrypts the morphed image and embeds the additional information to produce the encoded image. The authenticated image would then be transferred to the remote server. The cloud server incorporates extra data in the encoded image and creates the marked encoded image. Receivers with specific permissions get separate details in the last process. The user may enter the deciphered labeled picture "Idm" with the "Ke" key of encryption by decrypting images. The receiver will retrieve hidden D data from the labeled "Iem" encryption picture with the "Kl" and "Kd" encrypted data. The receiver will retrieve the original picture lossless using the "Ke" and "Kl" credit card data. The processor can both retrieve data "D" with all key and restore the actual image "I" without failure.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

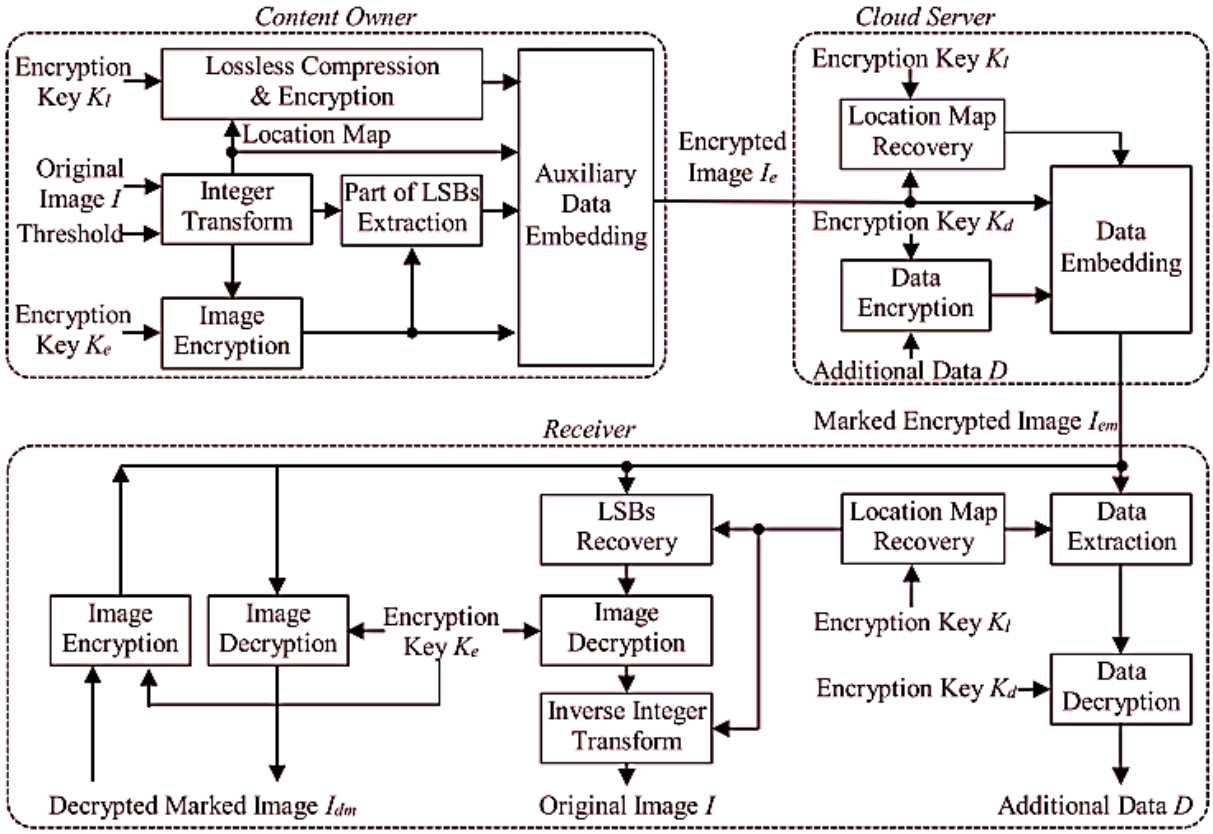

Fig.2: Framework Of The Proposed Method

To reach a higher RDH-EI modularizing efficiency, this paper suggest an improved method. This paper describe an integer conversion reversible (RIT) to convert the whole array. The algorithms and equation are as follows:

$$y_i = 2^m \cdot x_i - 2^m \cdot f(a(\mathbf{x}), 2^m), \quad (1)$$

where $m \in \mathbb{N}$. For $x \in \mathbb{N}$, the function $f(x, 2^m)$ is defined as

$$f(x, 2^m) = \lceil (2^m - 1) \cdot x / 2^m \rceil, \quad (2)$$

in which $\lceil \cdot \rceil$ is the ceil function, and $a(\mathbf{x})$ is the rounded average of $\mathbf{x}$ as

$$a(\mathbf{x}) = \begin{cases} \lfloor \bar{\mathbf{x}} \rfloor, & if\ \bar{\mathbf{x}} - \lfloor \bar{\mathbf{x}} \rfloor < 0.5 \\ \lceil \bar{\mathbf{x}} \rceil, & otherwise \end{cases}, \quad (3)$$

where $\bar{\mathbf{x}} = \frac{\sum_{i=1}^{n} x_i}{n}$, $\lfloor \cdot \rfloor$ is the floor function.

After integer transformation, each y_i $(1 \le i \le n)$ in $\mathbf{y}$ satisfies

$$y_i \bmod 2^m \equiv 0, \quad (4)$$

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

$$h(x, 2^m) = x - f(x, 2^m) = \lfloor x/2^m \rfloor. \quad (5)$$

Then, we calculate

$$h(y_i, 2^m) = x_i - f(a(\mathbf{x}), 2^m), \quad (6)$$

so,

$$\sum_{i=1}^{n} h(y_i, 2^m) = \sum_{i=1}^{n} x_i - n \cdot f(a(\mathbf{x}), 2^m). \quad (7)$$

The rounded average of (7) is

$$a(h(\mathbf{y}, 2^m)) = a(\mathbf{x}) - f(a(\mathbf{x}), 2^m), \quad (8)$$

where $h(\mathbf{y}, 2^m) = (h(y_1, 2^m), h(y_2, 2^m), \ldots, h(y_n, 2^m))$. Since $a(\mathbf{x}) = h(a(\mathbf{x}), 2^m) + f(a(\mathbf{x}), 2^m)$,

$$a(h(\mathbf{y}, 2^m)) = h(a(\mathbf{x}), 2^m). \quad (9)$$

Define $g(a(\mathbf{x}), 2^m)$, the m bits LSBs of $a(\mathbf{x})$ as

$$\begin{aligned} g(a(\mathbf{x}), 2^m) &= a(\mathbf{x}) - 2^m \cdot h(a(\mathbf{x}), 2^m) \\ &= f(a(\mathbf{x}), 2^m) - (2^m - 1) \cdot h(a(\mathbf{x}), 2^m), \end{aligned} \quad (10)$$

which is equal to

$$h(a(\mathbf{x}), 2^m) = (f(a(\mathbf{x}), 2^m) - g(a(\mathbf{x}), 2^m))/(2^m - 1). \quad (11)$$

$$f(a(\mathbf{x}), 2^m) = (2^m - 1) \cdot a(h(\mathbf{y}, 2^m)) + g(a(\mathbf{x}), 2^m). \quad (12)$$

From Eq. (6), we can get

$$x_i = h(y_i, 2^m) + f(a(\mathbf{x}), 2^m). \quad (13)$$

Subsequently, x_i can be calculated by substituting $f(a(\mathbf{x}), 2^m)$ with the right side of (12), the inverse form of RIT is therefore

$$x_i = h(y_i, 2^m) + (2^m - 1) \cdot a(h(\mathbf{y}, 2^m)) + g(a(\mathbf{x}), 2^m). \quad (14)$$

The cloud service must split the authenticated “Ie” image into overlapped blocks for the n-dimensional pixel ranges throughout data embedding.

$$\mathbf{Z} = \{\mathbf{z}^{(1)}, \mathbf{z}^{(2)}, \ldots, \mathbf{z}^{(N)}\}$$

Each z(j) I in z(j) must remove the LSB. The LSBs are decrypted by Kl for the compressed multilevel localization map to be reconstructed and the multilevel localization map is reconstructed. The cloud service identifies the properties with both the dual-level position chart.

$$L_{M'},\ L_{LSB1},\ L_{LSB2},\ \text{and}\ N' = \lceil L_{M'}/n \rceil$$
$$\mathbf{Z_1} = \{\mathbf{z}^{(1)}, \mathbf{z}^{(2)}, \ldots, \mathbf{z}^{(N')}\}$$
$$\mathbf{Z_2} = \{\mathbf{z}^{(N'+1)}, \mathbf{z}^{(N'+2)}, \ldots, \mathbf{z}^{(N)}\}$$

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

$(\mathbf{z}^{(j)} \in \mathbf{Z_2}$ and $m^{(j)} \neq 0)$

$(\mathbf{z}^{(j)} \in \mathbf{Z}$ and $m^{(j)} = 2)$

On the side of the receiver, it is possible to extract and recreate the original image. According to the separation of data collection from the authentication of files, several potential applications vary. The cases are listed below in table 1:

Table.1: The Table Portrayed The Various Cases As According To The Several Application

1.	Generating the Decrypted Marked Image. If the receiver only has the encryption key Ke, the decrypted marked image Idm can be obtained by direct decryption. The pixel value z (j) i in each z(j) also can be presented by 8 bits denoted as z (j) i (0), z (j) i (1), …, z (j) i (7). The decrypted marked bits x (j) i (k) can be calculated through the exclusive-or operation as follow x (j) i (k) = z (j) i (k) r (j) i (k).
2.	Marked Encrypted Executable code Extraction. The receiver can retrieve the encoded data from the specified encoded picture by using the K1 and Kd decryption key. The data extraction method is the reverse of data integration. The recipient divide this labelled encrypted picture into block Z= {z (1), z (2),..., z (N)} in non-overshadowed lines.
3.	Recovering the Original Image. As shown in case2, with encryption key K1, the receiver can recovery the multi-level location map. With the multi-level location map, the values of m(j) and N are determined, and the sequence SLSB1, SLSB2 can be extracted exactly
4.	Extracting Data and Recovering the Original Image. If with all of the encryption keys Ke, K1 and Kd, the receiver can extracting data from the marked encrypted image as case2, and recover the original image as case 3.

III.RESULTS

This paper carries out several tests utilizing various images to validate the proposed procedure. This paper uses these grayscale images for reference to demonstrate the works, as shown in figure 3. As payload rather than one of deciphered photo "PSNR" means that the success is not good because these techniques are reserved for embedding rooms in other papers with the modification of larger bit planes or Bit-planes by "MSB". Such approaches will achieve high throughput because they do not need to maintain the high performance of decrypted labelled photos. The proposed solution will achieve higher output and can achieve a large embedding potential only with the proposed solution. In fact, the approach suggested is reasonably secure. Because this paper uses the popular cryptographic algorithm, the picture controller is safe to prevent leakage of the image material. Fig. 4 showa the RDH-EI in lena and in airplane

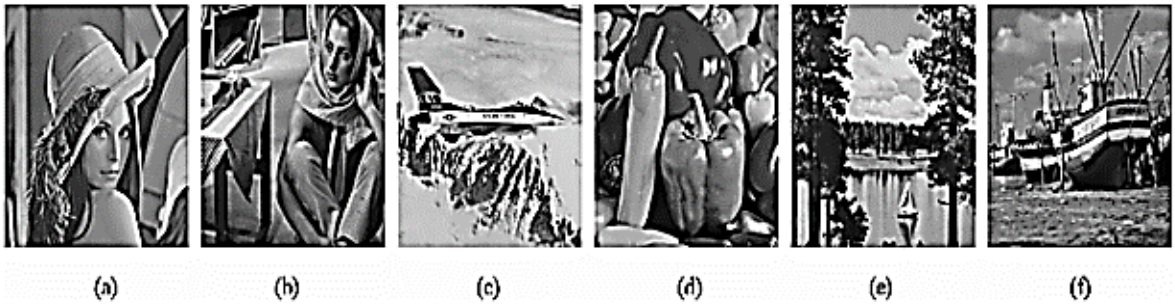

Fig.3: Six Test Images a) Lena; b) Barbara; c) Airplane; d) Peppers; e) Sailboat; f) Boat

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

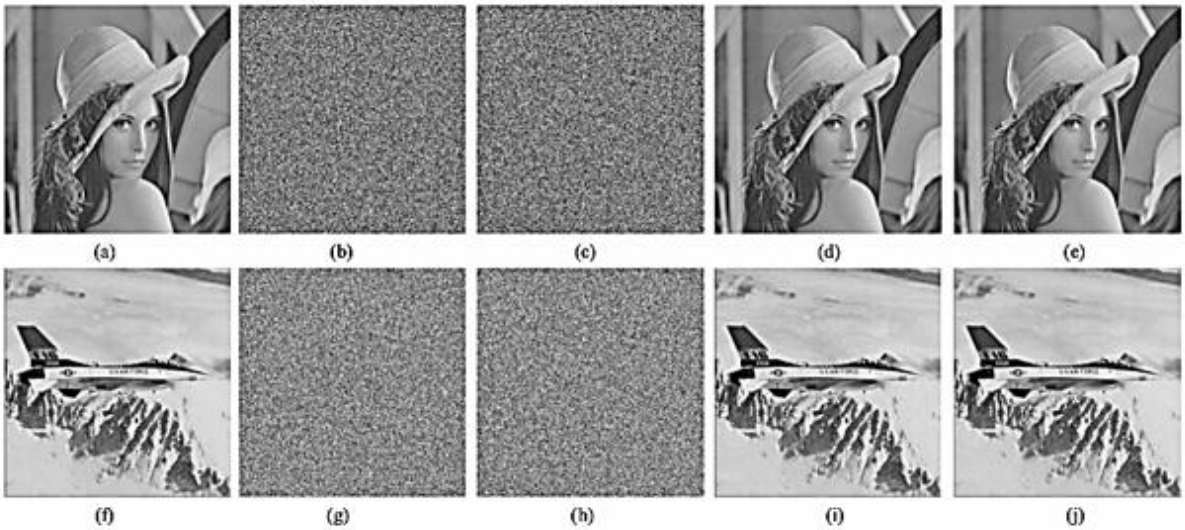

Fig.4: Examples of RDH-EI in Lena and in Airplane, (a) and (f) are the Orignal Images; (b) and (g) are the Encrypted Images with Reserved Embedding Room Generated by the Content Owner; (c) and (h) are the Encrypted Marked Images Embedded 0.6044bpp (158,451bits)

IV.CONCLUSION

This paper is proposing a new RDH-EI approach in this publication by setting aside a room before the encryption of the image. Each non-overlapping block in the final image is optimally incorporated with a specific m parameter (m / 0) using the adaptive minimally invasive integer transformation methodology. The auxiliary information collected is then inserted in converted blocks and the built-in room is processed. After the copyright holder has authenticated the image and submitted it is easy to incorporate vast volumes of data back into the cryptographically signed image with integrated ancillary data from the central server. The secret images can be essentially retrieved on the hand of the receiver and the initial file collected forward to decryption without failure. Both can be done separately. Observational findings show that the approach proposed is successful, allowing for greater development and improved quality of the identified picture that is directly decrypted relative to cutting edge approaches.

REFERENCES

[1] T. Jitha Raj and E. T. Sivadasan, "A survey paper on various reversible data hiding techniques in encrypted images," in Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 2015.
[2] A. Achuthshankar, A. Achuthshankar, K. P. Arjun, and N. M. Sreenarayanan, "Implementation of reversible Data Hiding in Encrypted Image using A-S Algorithm," in Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015, 2016.
[3] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," J. Vis. Commun. Image Represent., 2014.
[4] X. Zhang, "Separable reversible data hiding in encrypted image," in IEEE Transactions on Information Forensics and Security, 2012.
[5] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., 2011.
[6] 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 Secur., 2013.
[7] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," IEEE Access. 2016.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 4, April 2017

[8] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, 2014.
[9] A. Shaik, V. Thanikaiselvan, and R. Amitharajan, "Data security through data hiding in images: A review," Journal of Artificial Intelligence. 2017.
[10] H. T. Wu, J. L. Dugelay, and Y. Q. Shi, "Reversible image data hiding with contrast enhancement," IEEE Signal Process. Lett., 2015.
[11] F. Huang, J. Huang, and Y. Q. Shi, "New framework for reversible data hiding in encrypted domain," IEEE Trans. Inf. Forensics Secur., 2016.
[12] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," J. Vis. Commun. Image Represent., 2015.
[13] F. Khelifi, "On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain," Signal Processing, 2018.
[14] X. Liao, K. Li, and J. Yin, "Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform," Multimed. Tools Appl., 2017.

- P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
- P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
- S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014.
- RitikaWason, Vishal Jain, Gagandeep Singh Narula, AnupamBalyan and MandeepKaur, "Smart Robotics for Smart Healthcare", Advances in Robotics & Mechanical Engineering (ARME), Volume 1, Issue 5, January, 2019, DOI: ARME.MS.ID.000121.
- RitikaWason, Vishal Jain, Gagandeep Singh Narula, AnupamBalyan, "Deep Understanding of 3-D Multimedia Information Retrieval on Social Media: Implications and Challenges", Iran Journal of Computer Science, ISSN: 2520-8438 (Print) 2520-8446 (Online).

.