IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 9, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.122

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

|| Volume 9, Issue 11, November 2020 ||

Development of Reversible Data Hiding (RDH) Techniques for Image Transmission

Priyanka Varathe[1], Dr. Anil Khandelwal[2]

PG Student [Digital Communication], Dept. of ECE, VNS Group of Institutions, Bhopal, Madhya Pradesh, India[1]

Assistant Professor, Dept. of ECE, VNS Group of Institutions, Bhopal, Madhya Pradesh, India[2]

ABSTRACT: Reversible data hiding is a technique by using which we can embed essential data into images, audio, video and so on. As a result, the security of information transmitted over public channels is a fundamental problem, and as a result, the confidentiality and integrity of the data is essential to protect against unauthorized access and use. This caused the information concealment area to become unstable. Encryption and steganography are two of the most common methods you can use to ensure safety. With encryption, the data is converted to another form of gibberish and the encrypted data is transmitted. In Steganography, the image is transferred to the image, which is embedded in the image without affecting the quality of the image.This article suggests a new way to embed data into images and edit data using common virtual built-in technologies.

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

I.INTRODUCTION

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 ciphertext. 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.[1] 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 reestablish the picture for additional diagnosing by utilizing the cryptographic key.

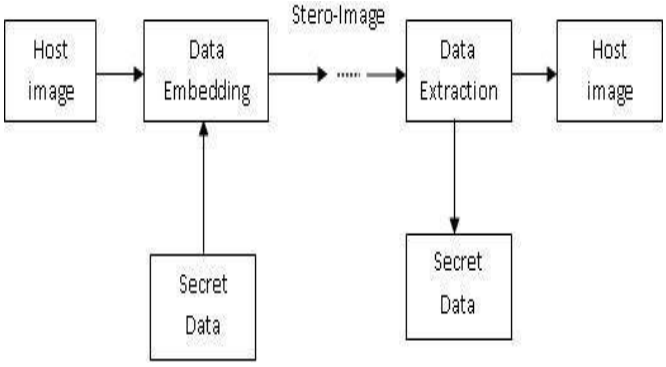


Figure 1: Block diagram of RDH

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

|| Volume 9, Issue 11, November 2020 ||

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 is conceivable 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, for example, 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.

Wei Liu et al. [4] 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. W.

Puech et al. [5] proposed an investigation of the nearby standard deviation of the checked scrambled 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.

Christophe Guyeux et al. [6] built up another system for data concealing security, called confusion security. Imprint Johnson et al. [7] proposed the oddity of switching the request for these means, i.e., first encoding and afterward compacting, without bargaining either the pressure proficiency or the data hypothetical security.

Jun Tian et al. [8] proposed reversible data installing which is likewise called lossless data inserting which implants imperceptible data into a computerized picture in a reversible style.

Patrizio Campisi et al. [9] present a novel strategy to indiscriminately assess the nature of a media correspondence interface by methods for an unusual utilization of advanced delicate watermarking. Stephane Bounkong et al. [10] 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.

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 un-readable 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-key cryptography*:

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. Itproduces fixed length signature for a message.

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

|| Volume 9, Issue 11, November 2020 ||

C. 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.

D. Data hidingtechniques:

Mainly the data hiding techniques are classified into two techniques:

1. Reversible data hidingtechnique:

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

2. Irreversible data hidingtechnique:

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.

a) 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).

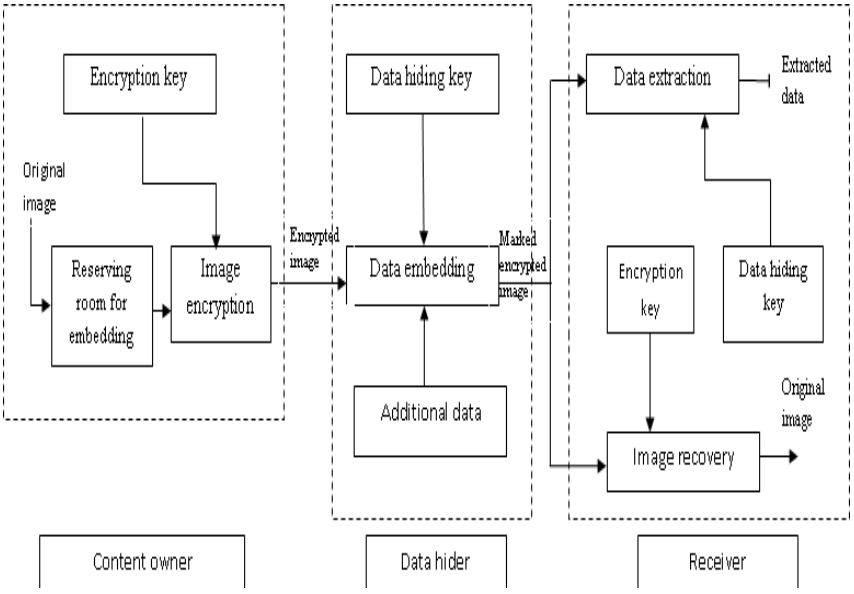


Figure 2: Vacating Room after the Encryption

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

|| Volume 9, Issue 11, November 2020 ||

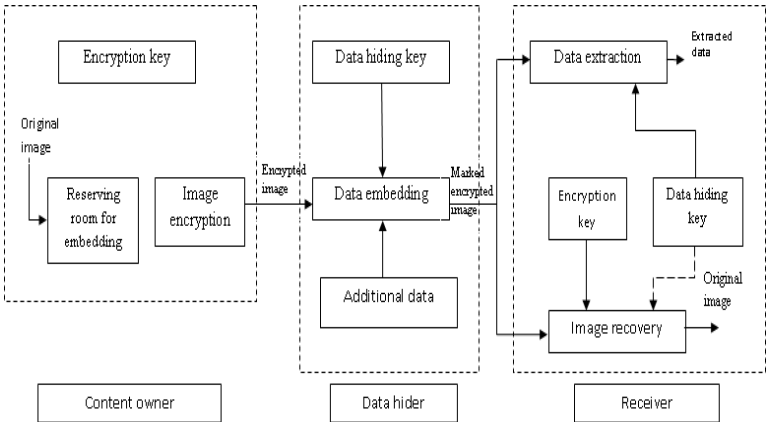


Figure 3: Vacating before the Encryption

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. [1] 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.METHODOLOGY

The proposed method consists of 4 steps. Image encryption, data modification, data integration, image search and data extraction. The content owner encrypts the cover image using an encryption key. The data owner uses the encrypted image to insert information (image or text). The encryption key is securely obtained by the recipient using an appropriate key exchange protocol based on the RSA algorithm. The virtual embedding of information extracts pixel indices corresponding to the bits of data and is performed by the data manager and generates a data extraction key. This extraction key is encrypted using the public key generated by RSA and sent to the recipient. If the recipient has a data extraction key, the original data can be retrieved. If the recipient has an encryption key, the original image can be recovered. If the receiver has two keys, you can get data and images. A block diagram of the transmitter side and the receiver side is shown in Figs.4 and 5, respectively

IMPLEMENTATIONMODULES

Encryption requires that you apply a special mathematical algorithm that uses a key to transform the data into encrypted code before passing it. Decryption is the reverse of the encryption to retrieve the original data from the encrypted code. In this document, the cover image is encrypted using modular additional encryption technology. The key sequence for encryption is generated using an annotation shift register (FSR).

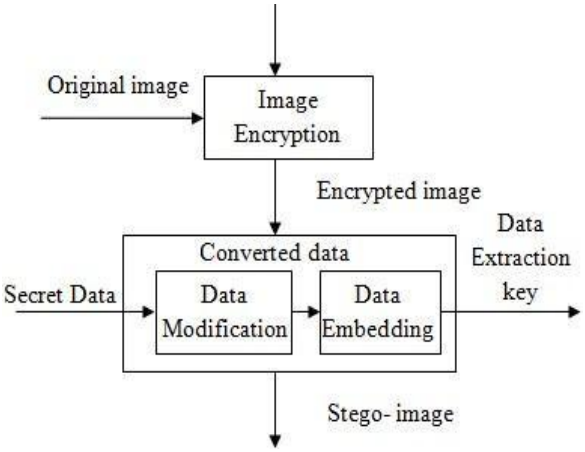


Fig 4: Architectural Diagram of the sender side

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

|| Volume 9, Issue 11, November 2020 ||

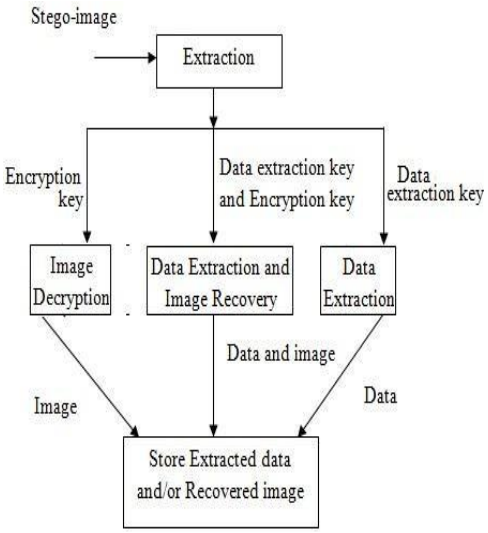


Fig 5: Architectural Diagram of the receiver side

Generators FSR uses the initial key called initial value / initial value (IV) to generate the key sequence. The generated initial value is shared between the sender and recipient. Each pixel in the image is encrypted using mod 256 additives to produce encrypted text. On the receiving side, a decryption algorithm is used in which the key sequence is generated by FSR, as mentioned above. The decryption method uses this key sequence as a backward key to recover the original image.

Consider a colour image of size M * N. Each pixel has red, green, and blue components with values between [0-256]. Each colour component consists of 8 bits and each pixel consists of 24 bits.

The initial start value is regarded as S1 S2 S3 ... Sn. The length varies from 8 to 12 digits. The seed's largest starting value is the encryption value and the new value is calculated. Then move the value to the left and place it on the right.

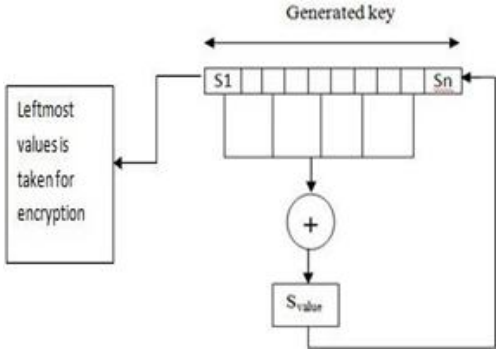


Fig 6: Key usage for encryption

The original image is encrypted using an encryption key. Encrypted data is used for data integration. In ordinal virtual integration, no actual embedding is performed. Where ordinal represents the position of the pixel that matches the data. At each pixel, the data is virtually integrated based on the bit values of the data and the LSB bits of the pixel. If the LSB bits of the pixel match the bit values of the data, it indicates that the data has been merged at this pixel in the cryptographic image. The display of the ordinal value of a pixel with virtually embedded data is recorded in a separate location and is considered the key to retrieve data from the receiver. For security reasons, it may be encrypted and sent to the recipient. For incompatibility, select the next pixel for virtual integration. Repeat until the end of the file. Eventually, a Stego image is created and sent to the recipient.

A. Image recovery

If the encryption key is available on the recipient side, the encryption key can be used to decrypt the original image. The sender sends the encryption key to the recipient. This key is used as the start value of the feedback shift register. This initial value is used to generate a pseudorandom number that is added to the pixel value of the image and performs the modular operation with 256. The generated value will be the new pixel value. The same procedure is performed for

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

|| Volume 9, Issue 11, November 2020 ||

all pixels in the cover image. Therefore, the image is decrypted. Pseudo-random numbers are generated by subtracting a random number from a starting value. The result is placed at the end of the starting value by moving the starting value to the left.

B. Data extraction

Data extraction is the reverse process of data integration. Initially, the key is included in the encrypted image where the data is displayed. Group LSB bits into 5 bits. Then check 5bits based on this control symbol with control symbols 1B, 1C, 1D and 1E. Finally, the original data is acquired.

IV. ALGORITHM

1. Read the input image and input from data modification stage.
2. Read the RGB values of the each pixel of the image.
3. Compare the LSB bit of the pixels with the bit value of the data. 0
4. If matched read the location where it is matched which will be the data extraction key Else Try to find the match of data bits with the LSB bits of the pixels.
5. Finally obtain data extraction key which will be locations of the pixel where the data bits are present.

V. RESULT AND PERFORMANCE ANALYSIS

Our proposed method is verified using standard gray image and color image with size (256 × 256). Fig 7(a) shows experimental results of a group of flower images. The original image of Fig. 7 (a) is encrypted using the encryption flow shown in Fig. 7 (a). Points to note, the encryption process is performed in two steps. Fig. 7(b)(1)shows the result of the encrypted operation 1, and Fig. 7 (b) (2) shows the result of the encryption operation 2. Fig. 7(c)shows a generated encrypted image containing secret bits, respectively and extracts hidden text (secret data) shown in Fig 7(d).
Like encryption, decryption is done in two steps. Operation and Operation the results of deference 1-2 are shown in Fig. 7 (d)(1) and Fig. 7(d)(2). Hidden text, hidden text length, the number of bits to use for data masking, the number of hidden ASCII characters is calculated. Since no operational image encryption is performed prior to the encryption key, the coarse image can be reconstructed with high quality. Two aspects of security are considered here. Security image content and supplemental security messages. The content owner does not allow access to the original image serving. The data manager cannot hack the system for messages that contain a partner. The original image is encrypted with the stream encryption using the encryption key.
For the data cache, extra bits are also protected by the establishment key. Data extraction and image reconstruction are separated in this method. There are three cases to be solved here at reception; just use two keys together to integrate and encrypt only the key and key.

Fig 7(a): Original image

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

|| Volume 9, Issue 11, November 2020 ||

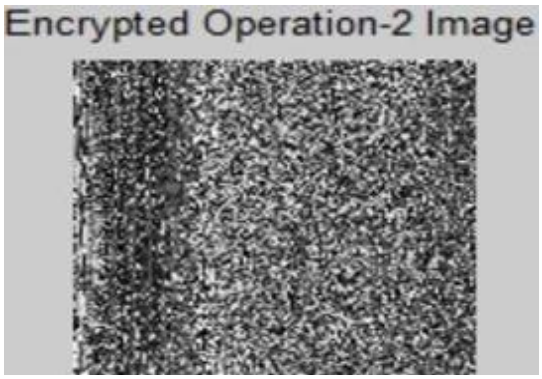


Fig 7(b) (1): Output of encryption opearation-1

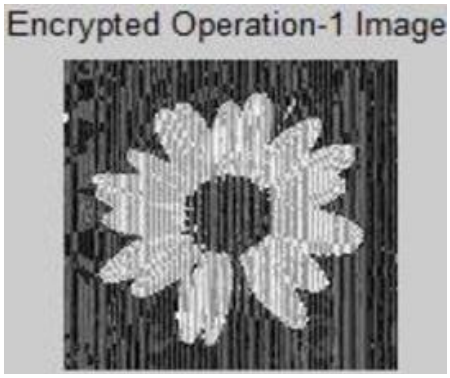


Fig 7(b) (2): Output of encryption operation-2

Fig 7(c): Encrypted image contains secret data

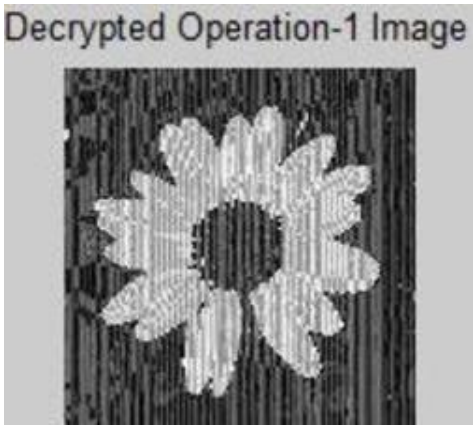


Fig 7(d)(1): Output of decryption-1

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

|| Volume 9, Issue 11, November 2020 ||

Fig 7(d)(2): Output of decryption

VI.CONCLUSION

In this paper, we propose a reversible and separable data masking method. That is, the virtual embedding is performed and the data bits are changed before embedding. In the first step, the content owner uses an encryption key to encrypt the cover image. Data Hider does not know the contents of the original image and embeds the data using this encrypted image. Selected data is converted using MLSB technology. The converted data is incorporated into the image using virtual integration technology. After insertion, a data extraction key is generated, encrypted, and sent to the recipient. Only the original image can be recovered if the receiver has only the encryption key and the stereo image. If you only have the data overwrite key and stego image, you can only import the original data from the stego image. If you have both data extraction and encryption keys and a stereo image, you can import both the original image and the data. Thus, there will be a separation at the receiver side, and based on the available keys, the receiver can obtain information. In this article, only the LSB of the pixel is considered in the virtual embedded. Future enhancements can take into account the LSB component of RGB components for the virtual embedding of data.

REFERENCES

[1] 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.

[2] 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.

[3] 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, July 2015.

[4] Wei Liu, WenjunZeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 – 1102.

[5] 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.

[6] Christophe Guyeux, Nicolas Friot, and Jacques M. Bahi, "Chaotic iterations versus Spread-spectrum: chaos and stego security", January 25-2011, IIHMSP,pp. 208-211.

[7] 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.

[8] 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.

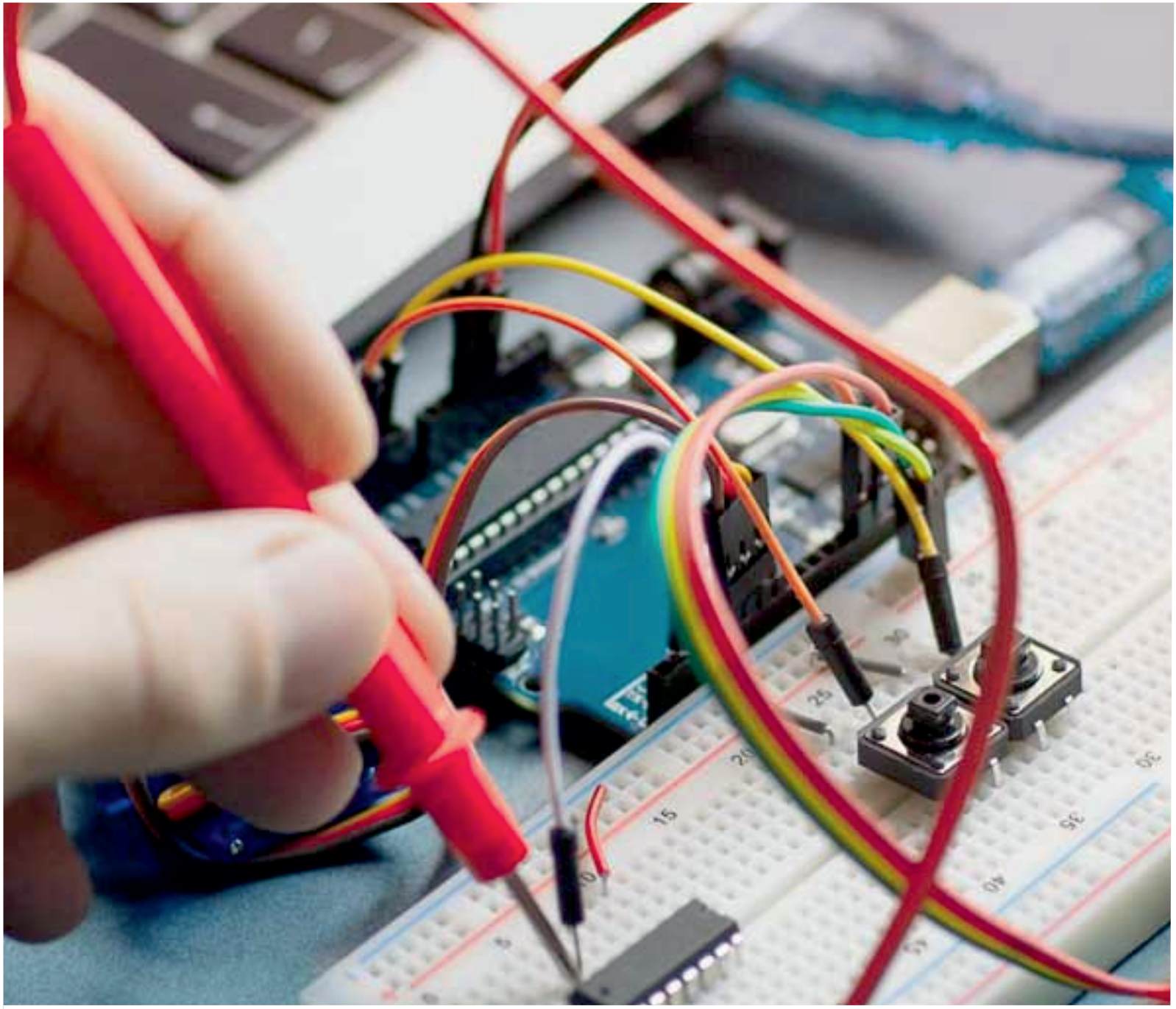
[9] PatrizioCampisi, Marco Carli, Gaeta no Giunta and Alessandro Neri, "Blind Quality Assessment System for Multimedia Communications using Tracing Watermarking" IEEE Transactions on Signal Processing, Vol 51, No 4, Apr 2003, pp. 996– 1002.

[10] 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 11, November 2020 ||

[11] 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.
[12] A.H. Ouda, M.R. El-Jakka, "A practical version of Wong's watermarking technique", Proc. ICIP (2004) 2615–2618.
[13] G. Boato, C. Fontanari, and F. Melgani "Hierarchical deterministic image watermarking via polynomial interpolation" Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept-2005,
[14] H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems 9 (3) (2003).
[15] Frederic Cerou, Pierre Del Moral, Teddy Furon and Arnaud Guyader, "Sequential Monte Carlo for rare event estimation" Statistics and Computing, pp. 1– 14, 2011.



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.122

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details