International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

A Novel High Capacity Reversible Data Hiding in Encrypted Domain using Robust MSB Prediction Technique

N. Sindhura[1], M. Gnana Priya[2]

[1]PG Scholar, Gokula Krishna College of Engineering and Technology, Nellore, A.P., INDIA.
[2]Professor & HOD, Dept. of ECE, Gokula Krishna College of Engineering and Technology, Nellore, A.P., INDIA.

Abstract - In recent days the data security in communication has became a challenging task due to increased cyber attacks. The information in even most of the confidential communications is being hacked and intercepted by intruders which may lead to the major threat to the privacy in personal communication. These cyber attacks by intruders not only steal the customer's valuable personal information but also cause a huge loss to them by impacting their financial and property transactions. Invertible Cryptography in digital images has become most efficient technique for hiding and extraction of data in encrypted domain. Hence as a solution to the aforementioned problems and to strengthen the information security we proposed and developed a pair of novel slightly altering algorithms for high capacity reversible data hiding using an efficient MSB Prediction method in encrypted domain. The proposed approaches encrypt the data image with a confidential key and while or after its transmission additional information may be embedded into the encrypted image. The proposed algorithm pair consists of VRAE (Vacating Room After Encryption) and RRBE (Reserving Room Before Encryption) algorithms. The Former algorithm embeds the data into the image after encryption with a secrete key, where as the later algorithm hides the data into the image before encryption. The proposed reversible data hiding algorithms are designed, developed, implemented and tested in the Matlab Environment. The simulation results adjudged that the proposed approaches are best in all aspects and outperforms all the existing approaches.

Key Words: Reversible Data hiding, Digital Images, Encryption, Embedding, Retrieval and Data security.

1. INTRODUCTION

Data hiding are a gathering of strategies used to put a safe data in a host media (like images) with little weakening in host and the way to extricate the protected data a short time later. For instance, steganography can be named [1]. Steganography is one such genius security advancement in which mystery data is installed in a spread [2]. However, this paper will get into reversible data hiding. Reversible data hidings embed data bits by changing the host signal, however empower the accurate (lossless) rebuilding of the first host signal in the wake of removing the inserted data. Now and again, articulations like bending free, invertible, lossless or erasable watermarking are utilized as equivalent words for reversible watermarking [3].

Advanced image security assumes a critical job in all fields, particularly in profoundly private zones like the military and restorative universes. With the advancement of distributed computing, the development in data innovation has prompted genuine security issues where classification, confirmation and uprightness are always undermined, by illicit exercises like hacking, duplicating or malignant utilization of data. The point of encryption strategies is to ensure Data security by completely or somewhat randomizing the substance of unique images [25].

During the transmission or the filing of scrambled images, it is regularly important to examine or to process them without knowing the first substance, or the mystery key utilized during the encryption stage [4]. In many applications, the little bending because of the Data installing is normally passable. Be that as it may, the likelihood of recouping the precise unique image is an attractive property in numerous fields, as lawful, medicinal and military imaging. Give us a chance to think about that touchy reports (like bank checks) are examined, ensured with a validation plan dependent on a reversible Data stowing away, and sent through the Internet. Much of the time, the watermarked reports will be adequate to recognize unambiguously the substance of the records. Be that as it may, if any vulnerability emerges, the likelihood of recouping the first plain record is fascinating [3].

Specifically, strategies for reversible Data hiding in the encoded space (RDHEI) have been intended for Data enhancement and confirmation in the scrambled area, when the encryption stage is fundamentally done in any case as, in a distributed computing situation. Without knowing the first substance of the image or the mystery key used to scramble the image, it is then conceivable to insert a mystery message in the encoded image. During the deciphering [9] stage, the first image must be consummately recoverable and the mystery message must be removed without mistake. In this manner, there exists an exchange off between the inserting limit and the nature of the recreated image. As of late, numerous strategies have been planned. The space to implant the message might be emptied after or before the encryption stage and, during the translating stage, image remaking and Data extraction can be handled in the meantime [16] or independently [12].

Data security techniques are grouped into three noteworthy classifications. These are cryptography,

watermarking and steganography. In cryptography the Data is scrambled into incoherent structure. In this way, that it winds up mixed [3] - [5]. Since figure content has useless structure and in this manner effectively animates the interest of pitiless aggressors who are happy to recoup or demolish Data. Be that as it may, it doesn't energize the presence of the message [2]. A copyright is ensured through watermarking which is characterized as a procedure of embeddings data a image [6], [7]. The vital point steganography is to cover the data and utilized it for secure correspondence in a totally imperceptible way. Additionally the procedure counteracts creating doubt to the transmission of a concealed Data [8] - [11]. This transmission procedure empowers change in the structure by evading recognizable proof of human eye. Spread or bearers is utilized to conceal the mystery data that is accessible as Digital images, sound and video documents, and different records of PC. Stego image is gotten by implanting a message into spread image. Quantum of data that can be covered up in the spread medium is characterized as limit. Strength is the capacity of stego medium to endure an assault by foe and keeping the concealed data from being wrecked. For recent decades Data stowing away has developed as intriguing territory of research [12]-[14]. In this technique, mystery Data can be encoded into a spread medium, and in this manner encourages the client to take out the inserted Data from the stego mode for different applications. In numerous Data hiding techniques, the Data is twisted during the task and keep the collector from recovering unique type of Data. In urgent zones of medicinal conclusion and law requirement, it is imperative to turn around the checked media back to the first spread media subsequent to recovering the concealed Data.

Lossless Data implanting methods might be arranged into one of the accompanying two classifications: Type I calculations [4] utilize added substance spread range procedures, where a spread range sign comparing to the data payload is superimposed on the host in the installing stage. At the decoder, recognition of the implanted data is trailed by a reclamation step where watermark sign is evacuated, for example subtracted, to reestablish the first host signal. Potential issues related with the constrained scope of qualities in the advanced portrayal of the host signal, for example floods and sub-currents during expansion and subtraction, are forestalled by embracing modulo number juggling. Payload extraction in Type-I calculations is powerful. Then again, modulo math may cause irritating salt-and-pepper ancient rarities. In Type II calculations [5][6], data bits are installed by adjusting, for example overwriting, chose highlights (parcels) of the host signal - for example least critical bits or high recurrence wavelet coefficients-.

In all cases, the displayed strategies are not ready to propose a high installing rate together with a generally excellent recreated image quality. In [12], the payload can be high (0:5 bpp), however the remade image is changed when contrasted with the first (PSNR 40 dB). Also, different techniques, for example, Wu and Sun's form, propose a "high" implanting limit, yet it is just conceivable to install roughly 0:1 piece per pixel at generally [15]. Moreover, in a considerable lot of the current strategies, Data stowing away is made by LSB (least huge piece) substitution. Be that as it may, in the encoded space, it is hard to recognize whether a image contains a shrouded message or not on the grounds that pixels have pseudorandom esteems. Consequently, we propose to substitute the MSB (most huge piece) values rather than the LSB esteems. Actually, free space, MSB prediction is simpler than LSB expectation and in the scrambled area, classification continues as before. In addition, we don't have to save the high caliber of the scrambled image contrasted with the unmistakable area.

2. LITERATURE SURVEY

In[2] a technique which utilization of an astounding reversible data hiding plan with high limit dependent on contrast extension. Here data inserting is finished utilizing pixel contrasts; this is a direct result of the likelihood of high redundancies among the neighboring pixel esteems in common images. During installing process, contrasts of neighboring pixel esteems are determined. In that distinctions the variable bits are resolved and a few contrasts are chosen to be expandable by 1-bit, along these lines the alterable bits increments. At that point connected piece stream of packed unique alterable bits. The area of expanded contrast numbers and the hash of unique image is implanted into the alterable bits of distinction numbers in an irregular request.

The watermarked pixels are accomplished by utilizing opposite change to from resultant contrasts . During watermark extraction, contrasts of neighboring pixel esteems are estimated. At that point decide variable bits in that determined contrasts. Concentrate the alterable bitstream requested by a similar pseudo irregular request as inserting and separate the compacted unique variable bitstream. Decompress the compacted isolated piece streams and recreate the first image supplanting the alterable bits and figure the hash of reproduced image and contrast and removed hash. The procedure contains the accompanying points of interest. There is no loss of data because of pressure decompression, this is additionally appropriate to sound and video data. The encryption of packed area guide and variable piece stream of various numbers expands the security.

The impediments incorporated into contrast development are there might be some round off blunders. The strategy to a great extent delicate to the smoothness of the image. So this technique can't be connected to finished images, whose limit will be low or even zero. There is huge corruption of visual quality because of substitutions of bits of dim scale pixels. In [3] propose an examination of the neighborhood standard deviation of the stamped encoded

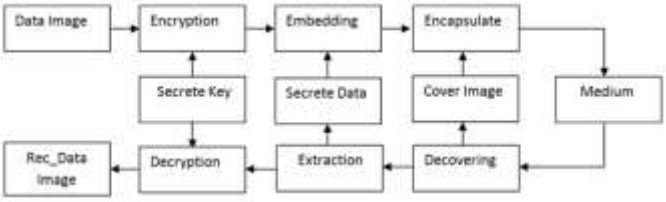
images so as to expel the inserted data during the decoding step. The quantity of computerized images has expanded quickly on the Internet. Image security has high effect on a few applications, e.g., video reconnaissance, military and medicinal applications. The need of quick and secure analysis is fundamental in the restorative world. The transmission of images is an every day schedule and it is important to locate a productive method to transmit them over systems. The data pressure is important to diminish the transmission time.

Two principle gatherings of advancements have been produced for this reason. First gathering dependent on substance insurance through encryption. There exist numerous techniques to scramble double images or dim dimension images. In this, legitimate decoding of data requires a key. The second gathering dependent on the assurance on computerized data hiding or data stowing away, went for furtively hiding a message into the spread data. These two innovations can be utilized integral and commonly commutative. .

In [4] proposes Data hiding Based On Search Order Coding for Vector Quantization Compressed Images. Vector Quantization is a prevalent and usually utilized computerized image pressure system. Since VQ fundamentally diminishes the size of a image to an extraordinary expand, the strategy can spare the expenses of extra room just as image conveyance. This technique uses Search-Order Coding (SOC) to control the arbitrarily disseminated histogram of a VQ-packed image into areas near zero. At that point utilizes the encoding procedures to perform encoding and data hiding all the while. During encoding process, pointer isn't required for records to distinguish list types, which thusly improves pressure execution. This strategy can totally reestablish the VQ-compacted image after mystery data extraction. The connection between's the neighboring pixels in each sub square is all around safeguarded in the encoded area. The primary favorable position of the proposed structure is that the RDH plan is free of the image encryption calculation. That is, the server director does not have to structure another RDH plan as indicated by the encryption calculation that has been led by the substance proprietor, as it is finished by inserting the data by utilizing different RDH calculations recently proposed to the scrambled area legitimately.

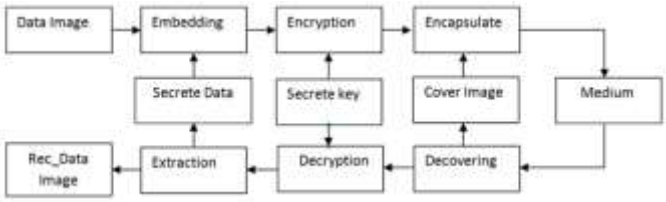
3. PROPOSED WORK

In this paper we proposed and developed a pair of novel slightly altering algorithms for high capacity reversible data hiding using an efficient MSB Prediction method in encrypted domain. The Proposed High Capacity Reversible Image Data Hiding and Extraction scheme implements two process correlative slightly altering algorithms named as VRAE and RRBE algorithms. In both algorithms the key objective process is to hide the secrete data in an image called data image and then embed it into a cover image. Now encrypt the cover image and transmit it to the destination. At the destination, first we perform decryption and then separate the data image from the cover image. Now from the data image, extract the secrete data using data retrieving process. The same procedure with slightly shuffled steps will be followed by the two proposed reversible image data hiding algorithms. First we discuss in detail about Vacating Room After Encryption (VRAE) algorithm in detail.



Fig(1): Schematic block diagram of the proposed VRAE reversible data hiding technique.

The proposed VRAE algorithm first considers the data image and encrypts it with a secrete key. After performing encryption now it is passed through a data embedding[16] room where the confidential information will be embedded into the encrypted data image. The data hided encrypted data image is now encapsulated in a cover object image which then encrypted and transmitted to the destination. At the destination the received cover object is decrypted to extract the encrypted data image from it. Next the confidential information is retrieved from the data image using the same key. After retrieving the confidential information from the data image, now data image is decrypted with the same key used for encryption to recover it into normal form. The second reversible data hiding technique proposed in this paper is Reserving Room before Encryption (RRBE) technique, which is shown in fig(2)



Fig(2): Schematic block diagram of the proposed RRBE reversible data hiding technique.

The RRBE technique first reserves the room for embedding the confidential data into the data image using some data embedding key. After embedding the confidential data into the data image, the data image is encrypted with some encryption key. Next the data image is hided in a cover image and then the cover image is encrypted and transmitted to the destination. At the destination the received cover image is decrypted first and the data image is separated from the cover image. Now the data image is also decrypted first and then it is subjected to retrieve the confidential information from it. During the data extraction operation the confidential information is extracted from the data image and the separated confidential information and

data image are sent to the destination separately. Thus the proposed reversible data hiding techniques enable a high capacity data hiding and extraction in encrypted images.

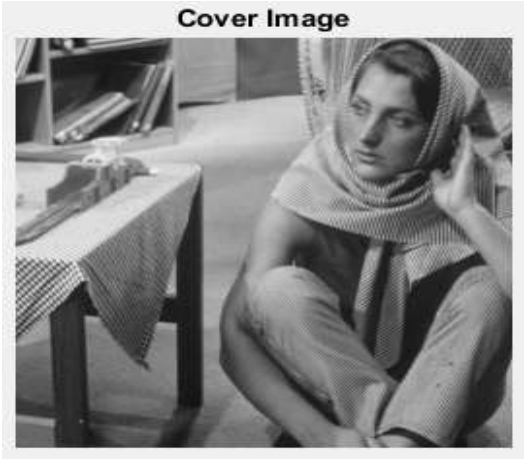
4. RESULTS AND DISCUSSION

In order to verify the operational effectiveness of the proposed reversible image data hiding system, the proposed system is designed, coded, implemented and tested in the Matlab environment and the simulation results are presented as follows

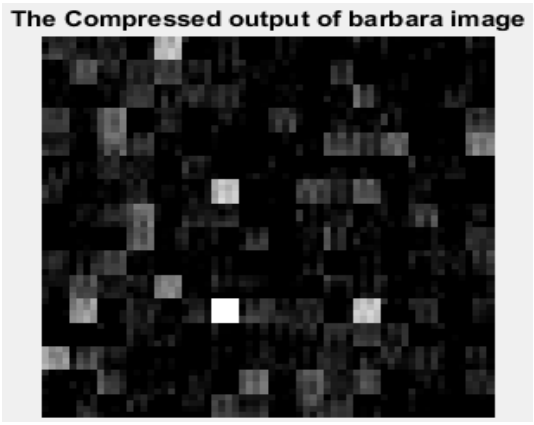
Fig (3): Data Image before data hiding.

Fig (4): Data Image after data hiding.

The data image into which the confidential information is going to be embedded is shown in fig(3) and after hiding the confidential information into the data image, the resultant image is shown in shown in Fig(4) .



Fig(5);Cover Image for Embedding.



Fig(6):VRAE encrypted Data embedded image.

The cover image for hiding the confidential information embedded data image is shown in Fig(5) and its VRAE encrypted version is shown in Fig(6).

Fig(7):Compressed Random encrypted image.

Fig(8):Extracted Data image.

```
retrievedBits =
  1×105 uint8 row vector
  Columns 1 through 30
   0   1   1   0   0   0   0   0   1   1   0   0   0   0   0
  Columns 31 through 60
   0   1   0   0   0   1   1   0   0   1   0   1   1   1   0
  Columns 61 through 90
   1   1   1   0   1   0   0   0   0   0   1   1   1   0   1
  Columns 91 through 105
   0   1   1   0   1   1   0   0   1   1   0   0   1   0   0
retrievedAsciiTable =
  7×15 uint8 matrix
   0   0   0   0   1   1   1   1   1   0   1   1   1   1   1
   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
   1   1   1   1   0   0   0   0   0   0   1   0   1   0   0
   0   0   0   0   1   0   1   1   1   0   0   1   0   1   0
   0   0   0   0   0   1   1   1   1   0   1   1   0   1   1
   0   0   0   0   0   0   0   0   1   0   1   1   1   0   0
   0   0   1   1   0   1   0   0   1   0   1   1   0   0   0
The recovered string =
hello world
```

Fig(9):Reconstructed Data

5. CONCLUSION

In this paper, we proposed an effective strategy for reversible data hiding in encrypted images dependent on MSB expectation with a high implanting limit, which beats the last best in class strategies. From our insight this is one of the principal techniques which proposes to utilize MSB rather than LSB for a RDHEI. Because of the way that MSB forecast is simpler than LSB expectation in unique space and in light of the fact that image quality disintegration isn't an issue in the scrambled area, we are then ready to have a high limit. Note that utilizing overhead such an extra guide isn't vital for this proposed methodology. As opposed to that, we utilized some MSB esteems as opposed to installing bits from the shrouded message. Also, we have seen that the proposed plan gives a decent security level and can be utilized to safeguard the first image classification, while offering in the meantime credibility or respectability check. In future work, we are keen on concealing more than one piece for every pixel. Truth be told, we imagine that it is conceivable to use, for instance, the second MSB of every pixel to broaden the measure of inserted data. The simulation results declared that the proposed methodologies are best in all aspects and outperforms all the current methodologies.

6. FUTURE WORK

Further research bearings incorporate testing other blunder indicators so as to diminish the quantity of forecast mistakes and, in this equivalent way, improve the recreated image quality (for the proposed Reversible Image Data Hiding Schemes) or the payload. Surely, with the proposed methodology, the more the payload is expanded, the more the quantity of forecast blunders is significant thus in this way, more the recuperated image is modified. In addition, with the proposed methodology, we are likewise engaged with the quest for another expectation mistake featuring component which will enable us to improve the implanting limit. Also there is a huge scope to extend this work by employing a video sequence as the data container for hiding and embedding the data and also there is a possibility to implement the proposed Reversible Data Hiding and Extraction techniques on a reconfigurable hardware using the robust VLSI architectures

REFERENCES

[1] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding new paradigm in digital watermarking,” EURASIP Journal. Appl. Sig. Proc., vol. 2002, no. 02, pp. 185–196, Feb 2002.

[2] Yaw-Hwang Chiou, Jiann-Der Lee, (2011)Reversible Data Hiding Based on Search-order Coding for VQ-compressed, JCIT), Vol. 6.

[3] X. Zhang, G. Feng, Y. Ren and Z. Qian. 2012. Scalable coding of encrypted images. IEEE Trans. Image Process. 21(6):3108-3114.

[4] W. Puech, M. Chaumont and O. Strauss (2008)A reversible data hiding method for encrypted images Proc. SPIE, vol. 6819,pp.68191E-1-68191E-9.

[5] Mohammad Awrangjeb, An Overview of Reversible Data Hiding, ICCIT 2003, 19-21 Dec, Jahangirnagar University, Bangladesh, pp 75-79.

[6] J. Fridrich, M. Goljan, and D. Rui, “'Invertible Authentication”, In Proc. of SPIE Photonics West, Security and Watermarking of Multimedia Contents III, San Jose, California, USA, Vol. 3971,pp. 197-208, January 2001.

[7] R. Rivest, “The MD5 Message-Digest Algorithm”, In DDN Network Information Center, http://www.ietf.org/rfc/rfc1321.txt, April 1992.

[8] K. Sayood, “Introduction to Data Compression”, Morgan Kaufmann, 1996, pp. 87-94.

[9] J. Fridrich, “Symmetric Ciphers Based on Two-Dimensional Chaotic Maps”, On Int. Journal of Bifurcation and Chaos, 8(6), pp. 1259-1284, June 1998.

[10] Fangjun Huang and Jiwu Huang (2016) New Framework For Reversible Data Hiding In Encrypted Domain, IEEE Transactions on Information Forensics and Security.

[11] Kede Ma ,Xianfeng ZhaoandWeiming Zhang 2016)Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, IEEE Transactions on Information Forensics and Security.vol 8, No 3,553-562.

[12] P. Bas and T. Furon, "Image database of BOWS-2," http://bows2.eclille.fr/.

[13] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation,"IEEE Transactions on Cybernetics, vol. 46, no. 5, pp. 1132–1143, 2016.

[14] T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693–1703, 2011.

[15] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP Journal on Information Security, vol. 2007, p. 17, 2007.

[16] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, pp. 1061–1070, 2011..

BIOGRAPHIES

N. SINDHURA received her B.Tech Degree in Electronics and Communication Engineering from Rajiv Gandhi University of Knowledge Technologies (APIIIT, RK VALLEY), Andhra Pradesh. Persuing M.Tech Degree in Digital Electronics and Communication Systems from Gokula Krishna College of Engineering, Sullurpet, and Andhra Pradesh.

M. Gnanapriya received her B.E degree in the field of Electronics and Communication Engineering from Madurai Kamaraj University and completed her M.E in the field of Computer science from AnnaUniversity, Tamilnadu. She is currently working as Associate professor & Head of ECE Dept, Gokula Krishna College of Engineering. Her areas of interest are Digital Signal Processing, Digital Image processing and Embedded Systems.