International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, 2020 pp.965-971

An Improved Reversible Data Hiding In Encrypted Images By Pre Encryption Room Reservation Policy (PERRP)

P.Anitha[1], Dr.V.Vallinayagi[2]
[1]*Assistant Professor & Research Scholar,Department Of Computer Science, Sri Sarada College For Women, Tirunelveli-627011*
[2]*Head & Associate Professor, Department Of Computer Science, Sri Sarada College For Women, Tirunelveli-627011*
Manonmaniam Sundaranar University,Abishekapatti,Tirunelveli-627012

Abstract

The Innovative Technique Is Pre Encryption Room Reservation Policy; It Is Reserving Room Earlier To Image Encryption. The Reversible Data Hiding Method On Encrypted Images Is More Expected And A Great Deal Easier. It Also Achieves The Entrenched Data Are Radically Improved. The Encrypted Image, Which Consisting Of Two Stages: Image Partition And Self-Reversible Embedding. In Image Partition The Encrypted Image Is Partitioned Into Two Parts, The First-Order Smoothness Function For Each Block To Find The Smoother Area. Then Calculate The Estimation Error Value And Then A Few Data Can Be Entrenched Into The Estimating Error Progression With Histogram Shift.

The Narrative Technique Is To Bring To The Values Of Peak Signal Noise Ratio And Entropy. Both The Values Of Peak Signal Noise Ratio And Entropy Is Reached The Elevated Values Compare Than The Existing Method. The Key Image And Original Image Are Recovered Without Affecting The Accuracy. In This Article, The Original And Key Images Are Also Applied In Various Resolutions. Each And Every Resolution Of Imagery Gives The High Peak Signal Noise Ratio Rate. The Novel Method Achieves The Admirable Performance Of Ideal Privacy For Plain Images Using The Above Techniques.

Index Terms: *Encryption, Image Embedding, Image Recovery, Privacy, Reversible Data Hiding*

1.0. Introduction

Data Hiding Is Referred To As A Procedure To Hide The Data Into A Cover Image. That Is, The Data Hiding Process Associates Two Sets Of Data, The First One Is Embedded Data And The Second One Is Cover Medium Data. Such As, The Hidden Data May Be A Lot Irrelevant To The Envelop Image. In Substantiation, On The Other Hand, The Envelope Image Data Is Related To The Embedded Data. The Two Applications, Are Invisibility Of Unknown Data Is An Necessary Obligation. In Majority Cases Of Hiding Technique, The Cover Image Will Occurrence Some Distortion Due To Data Hiding And Cannot Be Upturned To The Original Image. The Hidden Data Is To Be Extracted Away, But The Number Of Everlasting Distortions Has Visible In The Original Image.

In Various Applications, For Example, A Law Enforcement And Medical Analysis, It Is Important To Render Null And Void The Secret Messages Or Images Back To The Original Cover Image, After The Surreptitious Data Are Retrieved For Some Authorized Consideration. In Extra Application, Such As High-Energy Atom And Remote Sensing Physical Tentative Exploration, It Is Preferred That The Original Media To Be Improved. Reversible Data Hiding Facilitates Enormous Prospect Of Applications To Relate The Data Of Two Sets. Such An Approach That The Cover Image Can Be Lossless Recovered After The Secret Data Is To Be Extracted From The Original Media, Hence Given That An Extra Path Of Organize The Data Of Two Different Sets.

In Cryptography Method, Encryption Is The Progression Of Encoding Information In An Approach That Arbitrator Cannot Read It, But No More Than Approved Parties Can Convert The Encoded Information. Encryption Scheme Doesn't Use To Avoid The Tracing, But It Intercepts The Third Parties From The Original Data That Is Encrypted. In An Encryption Method, The Information Or Messages Referred To As Plaintext Is Encrypted Using A Different Encryption Algorithm,

ISSN: 2233-7857 IJFGCN

Revolving It Into An Illegible Cipher Text. The Important Use An Encryption Key, It Specifies The Steps Of Message Encoding. Each Opponent Can Observe The Unreadable Message Or Encoded Message. The Unreadable Or Encoded Message Is Called The Cipher Text. The Encoded Message Can't Be Viewed To Anybody. An Approved Person, On The Other Hand, The Encoded Message Is To Be Decoded By Using The Different Decryption Algorithms. The Decryption Algorithm Need A Furtive Decryption Key. An Encryption And Decryption System Commonly Requires A Key-Generation Algorithm. The Key Generation Algorithm Only Produce A Random Keys To Make Data More Secure.

Encryption Algorithm Also Used By Governments And Militaries To Facilitate Top Secret Communication. At This Moment Frequently Used In Protecting Information Contained By A Lot Of Civilian Systems[18].

Encryption Algorithm May Use To Guard The Data To Transport Via Networks Such As The Wireless Microphones, Internet, Wireless Intercom Systems E-Commerce, E-Mails, Files, And Folders, Bank ATM (Automatic Teller Machine), Mobiles And Bluetooth Devices. There Comprise Be Frequent Data Reports In Transfer Individual Intercept During Modern Years. The Data Is Encrypting In Transfer Moreover Help To Protect It As It Is A Lot Complicated To Actually Secure All Admittance To The Network.

2.0. Previous Arts

Zhang[10] The Encrypted Image Divided Into Many Blocks. Moving The Three Least Significant Bits, Half Of The Pixels In Each And Every Block. Finally, The Embedded Bit Room Is Vacated. Hong [9] , Zhang's Process Error Rate Is Concerted By Entirely Exploit The Pixels In Manipulative , Smoothness Of Every Block By Match Of The Surfaces.Afterwards, The Extraction Of Block And Recovery Of Each Blocks Are Observed The Consonance With The Downward Order Of The Complete Ease Dissimilarity At Intervals Of Diploid Candidate Section Or Blocks And Enhanced Blocks Be Able To Worn To Estimate The Efficiency Of The Remaining Blocks, It Is Assigned To As Match Of Surfaces.

Kede Ma[13], Weiming Zhang, Xianfeng Zhao [13], The Owner First Reserving The Room For The Embedding Data .Then, The Embedded Data Using The Encryption Key, Subsequently The Image Is To Be Encrypted. Now The Key Image Is Ready To Be Embedded Into The Encrypted Image Using Data Hiding Key. This Method Is Called The Reserving Room Before Encryption. Finally The Secret Image Is Extracted Using Secret Keys, Then Decrypted Image Is Extracted Accepting Encryption Keys, Atlast, Recover The Original Image With High Error Rate And High Distortion.

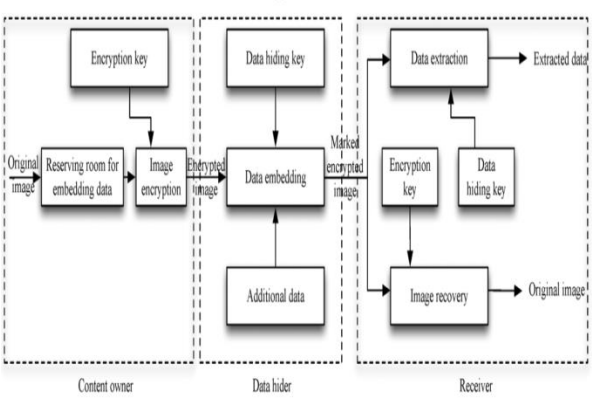

Fig1.Reserving Room Before Encryption(RRBE)

3.0. Proposed Method

Propose A Narrative Technique For Data Hiding In Encrypted Images, Not To Vacated The Room After The Encryption, This Method Has Been Done In The Previous Articles. Here, The Imperative Process Is To Reserving The Room Before The Encryption, This System Is Called As 'RRBE'. In The

ISSN: 2233-7857 IJFGCN

Novel Technique, Using A Conventional Data Hiding Method, Vacate The Room By Enclosing Least Significant Bits Of Various Pixels Into Supplementary Pixels. Then Image Is To Be Encrypted, So That Arrange The Least Significant Bits In The Uncorrupted Or Encrypted Image Can Be Worn To Implant Data.

It Reverses The Order Of Encryption And Vacating Room. It Is Reserving Room Earlier To Image Encryption. The Data Hiding Tasks On Encrypted Images Would Be Alive More Natural And Much Easier. It Also Achieves Outstanding Routine In Two Special Scenarios, Actual Feasibility Is Accomplished, So That Error Is Free For Both The Data Extraction And Recovery Of Image Also. Forgiven Peak Signal Noise Ratio Of The Decoded Image, The Embedding Values Containing The Entrenched Data Are Radically Enhanced.

The Innovative Method Is Also Concludes Outstanding Achievement In Two Dissimilar Projections. They Are,

• The Free Of Error In Data Extraction And Recovery Of Image Are Free Of Any Error. So The Actual Feasibility Is Realized.

• For Certain Embedding Values, The Peak Signal Noise Ratio Of The Decoded Or Decrypted Image Includes Embedded Data Are Extensively Enhanced And Value Of Acceptable Peak Signal Noise Ratio, The Embedding Values Are Deeply Engorged.

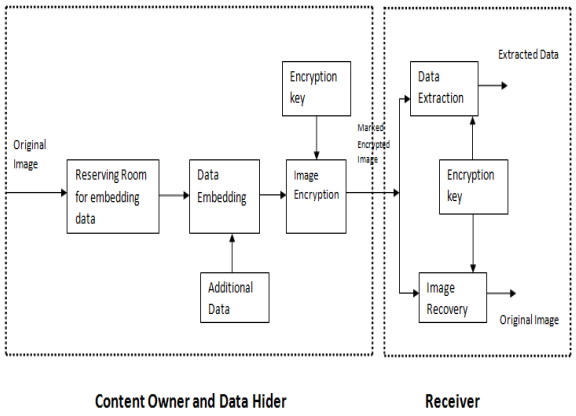

Fig2.Pre Encryption Room Reservation Policy (PERRP)

3.1. Generation Of Encrypted Image

Infact, The Encrypted Image Construction Divided Into Two Stages. The First Stage Includes The Three Steps. They Are I) Partition Of Images Ii) The Self-Reversible Embedding Iii) Encryption Of Image And To Hide The Data. At The Beginning, The First Step Image Partition Segregates The Unique Image Into Binal Parts, That Is A And B. Additional Data Are Hidden Into The Part A. Standard RDH Algorithm Applied To B. LSB Replacement Is Done For Both A And B Part. Then, The Lsbs Of Are Reversibly Entrenched Into With A Regular Data Hiding Algorithm . The Least Significant Bits Be Able To Obliging The Messages; At Most Recent Encrypt The Reorganize The Picture To Produce Its Concluding Edition.

3.1.1 Partition Of Images*:*

Conventional Data Hiding Technique Is The Main Process For Reserving The Room Before The Encryption, The Goal Of Image Partition Is To Create A Tranquil Area[16],[17] Be Capable Of Reach Enhanced Routine. To Perform With No Loss Of Simplification, Predicate The Cover Figure Is An Eight Bits Of Grayscale Figure By Way Of Its Range Of M Rows And N Columns (M X N) And Pixels, It Belongs To 1 And 255. The Value Of I And J Between The Range From 1 And I Is Greater Than M And J Is Greater Than N. The First Step Is The Gratify Owner Extract From The Novel Image, Alongside The Rows, Quite A Lot Of Coincidental Segments Whose Quantity Is Indomitable Through The Volume Of Embedded Messages , Symbolize As L.

The Superior Segments Or Blocks Contains A Complicated Characters. The Gratify Owner, For That Reason, Selects The Maximum F Toward A Particular Blocks Or Segments. Then Focus It Just Before The Image Link Together With The Remaining Position Of B With Smaller Amount Of

ISSN: 2233-7857 IJFGCN

Character Field. This Absolutely Depends Going On The Actuality, So That Particular Least Significant Bit Level Surface A Be Certified. It Is Straightforward That The Gratify Owner Be Capable Of Embed More Than Two Of Least Significant Bit Level Surfaces Of A Toward B, It Pass To Partially, The Diminution In Amount Of A. On The Other Hand, The Enforcement Of A, In Peak Signal Noise Ratio, Subsequent To Data Embedding In The Next Phase Decreases Broadly With Mounting Bit-Surfaces Subjugated.

3.1.2 Self-Reversible Embedding:

Self Reversible Embedding Main Objective Is To Entrench The Least Significant Bit Surfaces Of A Within B By Conventional Hiding Techniques. So That Make Simpler Technique To Exhibit The Procedure Of Self Reversible Embedding. Remind This Stride Do Not Await On Some Data Hiding Mthods. The Remaining Part Of Figure B Pixels Are Classified In Two Heads: Indices Of White Pixels With I And J Gratifying $(i + j) mod\ 2\ is\ equal\ to\ 0$ .The Black Pixels Indexes Meet $(i + j) mod\ 2\ is\ equal\ to\ 1$. Each White Pixel Is Anticipated Through The Interpolation Rates Procured By Means Of 4 Black Pixels[13].

The Weight, The Value Of I Is Between The Range From 1 And 4. It Is Resolved Via The Proposed Method. Using The Below Equation To Calculate Estimation Error Is ,

$$\mathbf{E_{i,J} = B_{i,J} - B'_{i,J}}$$

The Estimation Error Sequence Of Black Pixels Of Neighboring White Pixels. The White Pixels Can Be Modified At Any Time. To Accommodate The Messages, An Additional Estimation Error Progression Is Developed. Many Messages Know How To Be Embedded On Each One Estimation Error Progression By Bidirectional Histogram Shift. The Aim Of Bidirectional Histogram Shift Is To Divide The Estimating Errors Considered As Two Parts, Such That Right And Left Sections.

To Find The Maximum Point In Both Left And Right Parts, It Can Be Denoted As LM And RM. In The Original Image, The Default Value Of Left Part Is Equal To 1. The Right Part Value Is Equal To 0.At The Same Time The Minimum Value Is Also Search For Both Left And Right Part, It Can Be Denoted As RN And LN. To Embed The Communication Keen On The Location Is Equal To RM, With An Estimating Error. Then Shift All The Error Ranges From Adding 1 To The Right Part Maximum Value (RM+1) And Subtracting The Value 1 From The Minimum Value Of Right Part (RN-1).

With One Step Towards Right Part, Represent The Bit Value Is 0 With Right Part Maximum Value And The Bit Value Is 1 With To Adding 1 To The Right Part Maximum Value. The Embedding Procedure Is Same As The Left Part, Except The Direction Of Shifting Position And In Left, Then Shift Is Visualized By Decrease The Value Of 1 As Of The Pixel.

3.1.3 Data Hiding In Encrypted Image

Now, The Encrypted Image Can Embed The Secret Image Into The Original Image By Data Hider, And Even Though Does Not Get Right To Use The Novel Image. The Embedding Procedure Initiates The Encrypted Version Of A, Which Is Denoted As $A_{E.}$ The Encrypted Version Have Been Relocated To The Peak, The Data Hider Read The Ten Bits Of Data In Least Significant Bits Of First Ten Encrypted Pixels. At Last, The Data Hider Assigns A Label To Consequence Of Me, To Identify The End Position Of Embedding Images. The Data Hiding Or Secret Key Is To Create An Obvious Encrypted Image As E'. Somebody, Does Not Attain, The Data Hiding Key Might Not Take Out The Secret Information.

3.1.4 Encryption Of Image:

Subsequent To That**,** The Repositioned Self- Entrenched Image As X. Even Now The Encoded Image Is Denoted To E'. The Encryption Stage Follows The Stream Cipher Mechanism [13].

3.1.5 Data Extraction

ISSN: 2233-7857 IJFGCN

The Next Step Of Image Encryption Is Data Extraction. It Considers The Two Cases. The First Case Is Data Be Able To Extricated From The Encoded Figure And Second Stage Is Data Can Be Extricated Beginning The Decoded Image.

3.1.5.1 Data Extraction From The Encrypted Images:

To Modernize Individual Information Of Images Are Encrypted. The Aim Of Encrypted Images Is To Protect The Clients Confidentiality. A Database Administrator May Be Getting The Right Entry To Control The Data In Encrypted Sphere. In This Case, The Extraction Of Data Can Be Done Before The Decryption Of Image Is Used To Guarantee The Possibility Of Work.

The Database Administrator Only Knows The Secret Key Can Decrypt The Least Significant Bit And Extract Out The Additional Data By Directly Reading The Decrypted Image. If To Update Any Information Throughout The Least Significant Bit Substitution And Encrypts, The Updated Data To The Secret Key. The Entire Procedure Is Operated Only The Encrypted Area, Because It Abstains Trickle Of Cover Media.

3.1.5.2 Data Extraction From The Decrypted Images*:*

During The Preceding Stage, Mutually Extraction And Embedding Can Be Done In The Encrypted Area. At This Stage, The User First Needs To Decrypt The Image. Then The User Extricates The Secret Data From The Decrypted Image. The Image Alone, Encrypted To Retain The Information Into The Encrypted Image. The Order Of Image Extraction Is Apt For This Examine.

1.6 Image Restoration:

The Last Phase Is The Image Restoration, Exclusive Of Original Image Is To Be Improved. The Process Is Fundamentally Similar To The Conventional Reversible Data Hiding Method. The First Step Is Decrypt The Least Significant Bit Planes Of The Secret Key, Extract The Secret Data Until The Process Level Is Stretched At The End.

The Second Step Is To Extract The Image Left And Right Parts, Maximum, Minimum And Pixel Values That Is The LM, RM, LN, RN, X, And R_b Used The Boundary Map As Of The Least Significant Bit Of Region Of B". If The Value Of R_b=0, There Is No Black Pixel In The Embedding Procedure, Compute The Estimating Errors Of The White Pixels.

Otherwise, Calculate The Estimating Error Value For The Black Pixels [13]. Implement All The Exceeding Periods To Recuperate The Original Cover Image.

4.0. Experiments And Comparisons

Fig3. (I) Original Image (Ii) Encrypted Image
(Iii) Decrypted Image (Iv) Recovery Image

TABLE I
List Of Cover And Key Image Resolution

Images	Type Of Image	Resolution
Cover Image	**.JPG (GRAY SCALE IMAGE)**	**512 X 512,256 X256, 128X128**
Key Image	**.JPG (GRAY SCALE IMAGE)**	**64 X 64, 128 X 128, 32 X 32**

ISSN: 2233-7857 IJFGCN

TABLE II

Embedding Strategies Analysis Under Various

Images	PSNR VALUES	
	Existing(RRBE)	Proposed(PERRP)
IMG_1 : Lena	**36.2247**	**60.9234**
IMG_2 : Barbara	**36.9027**	**58.1234**
IMG_3: House	**36.9027**	**61.2045**
IMG_4: Cameron	**42.5544**	**57.5264**
IMG_5: Boat	**42.2114**	**55.8249**

PSNR Values

5.0 Conclusion

The Original Image Is Encrypted Before The Data Embedding Process And Using The Same Secret Key For Both The Data Extraction And Image Recovery. In This Way, The Secret Image Was Not Secured And The Original Image Also Blemished After The Image Extraction. The Most Attractive Features Of The Poroposed Scheme, The Image Is Encrypted After The Embedding Process. So That The Data Hider Can Promote From The Additional Block Emptied Out In The Preceding Stage To Compose Data Hiding Progression Effortless. The Traditional Data Hiding Technique Achieves The Admirable Performance. It Can Accomplish The Real Reversibility, Separate Data Extraction And Enhancement On The Excellence Of Decrypted Images.

6.0 Future Scope

In Future, This Method Can Be Implementing On Color Images, The Protection Is More Growing Of The Data Hiding In The Image And Also It Can Be Implementing In Video Files.

7.0. References

1. Macq, B., “Lossless Multi Resolution Transform For Image Authenticating Watermarking”, Proc. Of EUSIPCO, Tampere, Finland, September, 2000.
2. J. Fridrich And M. Goljan, “Lossless Data Embedding For All Image Formats,” In Proc. SPIE Proc. Photonics West, Electronic Imaging, Security And Watermarking Of Multimedia Contents, San Jose, CA, USA, Jan. 2002, Vol. 4675, Pp. 572–583.
3. W. Zeng, “Digital Watermarking And Data Hiding: Technologies And Applications,” In Proc. Int. Conf. Inf. Syst., Anal. Synth., Vol. 3, 1998, Pp. 223–229.
4. Z. Tirkel, C. F. Osborne, And R. G. Van Schyndel, “Image Watermarking- A Spread Spectrum Application,” In Proc. IEEE 4th Int. Symp. Spread Spectrum Techn. Applicat., Vol. 2, Sep. 1996, Pp. 785–789.
5. M. M. Yeung And F. C. Mintzer, “Invisible Watermarking For Image Verification,” Electron. Imag., Vol. 7, No. 3, Pp. 578–591, Jul. 1998.
6. B. Chen And G. W. Wornell, “Quantization Index Modulation: A Class Of Provably Good Methods For Digital Watermarking And Information Embedding,” IEEE Trans. Inf. Theory, Vol. 47, No. 4, Pp. 1423–1443, May 2001.
7. F. Perez-Gonzlez And F. Balado, “Quantized Projection Data Hiding,” In Proc. IEEE Int. Conf. Image Process., Vol. 2, Sep. 2002, Pp. 889–892.
8. Z. Ni, Y. Shi, N. Ansari, And S. Wei, “Reversible Data Hiding,” IEEE Trans. Circuits Syst. Video Technol., Vol. 16, No. 3, Pp. 354–362, Mar. 2006.
9. W.Hong And H.Wu,”An Improved Reversible Data Hiding In Encrypted Images Using Side Match,”IEEE Signal Process,Lett,Vol 19,No.4, Pp 199-202,Apr 2012.

ISSN: 2233-7857 IJFGCN

10. X. Zhang, “Seperable Reversible Data Hiding In Encrypted Image,” IEEE Trans. Inf. Forensics Security, Vol. 7, No. 2, Pp. 826–832, Apr. 2012.
11. Anatol.Z.Tirkel Et Al,”Image Watermarking-A Spread Spectrum Application”,September 2006.
12. A.C.Yao,”Protocols For Secure Computations,” In Proc,23rd IEEE Symp.Foundations Of Computer Science,Nov1982,Pp 160-164.
13. Kede Ma, Weiming Zhang And Xianfengzao, “Reversible Data Hiding In Encrypted Images By Reserving Room Before Encyption” IEEE Trans. Information Forensics And Security., Vol. 8, No. 3, Pp., Mar. 2013.
14. J.Tian,”Reversible Data Embedding Using A Difference Expansion,IEEE Trans.,Vol.13,No 8,Pp 890-896, Aug2003.
15. D.M.Thodi And J.J.Rodriguez, ”Expansion Embedding Techniques For Eversible Watermarking”,IEEE Trans, Image Process,Vol-16,No.3,Pp721-730,Mar 2007.
16. L.Luo Et Al., “Reversible Image Watermarking Using Interpolation Technique,” IEEE Trans,Inf,Forensics Security, Vol 5, No.1,Pp, 187-193, March 2010.
17. V.Sachnev, H.J.Kim, J.Nam, S,Suresh, And Y-Q.Shi, “Reversible Watermarking Algorithm Using Sorting And Prediction,” IEEE Trans.Circuits Syst.Video Technol., Vol1+, No.7, Pp 989-999, Jul 2009
18. Sudha Rani.K, "Text File Encryption Using FFT Technique In Lab View 8.6",International
19. Journal Of Research In Engineering And Technology, 2012

ISSN: 2233-7857 IJFGCN