ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

RESERVING ROOM BEFORE ENCRYPTION USING REVERSIBLE DATA HIDING TECHNIQUE

Adlin Shibi P[1], R.Ablin[2]
[1]PGStudent,DepartmentofECE,ArunachalacollegeofEngineeringforWomen
[2] AssistantProfessor,DepartmentofECE,ArunachalacollegeofEngineeringforWomen

Abstract -Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may subject to some errors on data extraction and/or image restoration. Here, a novel method is proposed so as to reserve room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, i.e.,data extraction and image recovery are free of any error.

Keywords: Reversible Data Hiding, image encryption, PSNR.

I. INTRODUCTION

ReversibleDataHidinginimagesisatechnique,bywhichtheoriginalcovercanbelosslesslyrecoveredaftertheembeddedmessageis extracted.This important techniqueiswidelyusedinmedicalimagery,militaryimagery andlawforensics,civilconstructionswherenodistortionoftheoriginal cover is allowed.*A.Forhiding data inan image*

Segmentstheencryptedimageintoanumberofnon-overlappingblocks;eachblockisusedtocarryoneadditionalbit.Theerrorrateisreducedbyfullyexploitingthepixelsincalculatingthesmoothnessofeachblockandusingsidematch.Here,anovelmethodisproposedsoastoencryptimagesusingRDH,forwhich"vacateroomafterencryption"isnotdonebut"reserveroombeforeencryption"where,firstemptyoutroombyembeddingLSBsofsomepixelsintootherpixelswithatraditionalRDHmethodandthenencrypttheimage,sothepositions ofthese LSBsin the encrypted.

II. PREVIOUSMETHODS

ThePreviousmethodcanbesummarizedastheframework,"vacatingroomafterencryption(VRAE)",asillustratedinFigure.(a).Inthisframework,acontentownerencryptstheoriginalimageusingastandardcipherwithanencryption key.Afterproducingtheencryptedimage,thecontentownerhandsoverittoadatahiderandthedatahidercanembedsomeauxiliarydataintotheencryptedimagebylosslesslyvacatingsomeroomaccordingtoadatahidingkey.Thenareceiver,maybethecontentownerhimselforanauthorizedthirdpartycanextracttheembeddeddatawith the data hiding encrypted version according to the encryption key.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

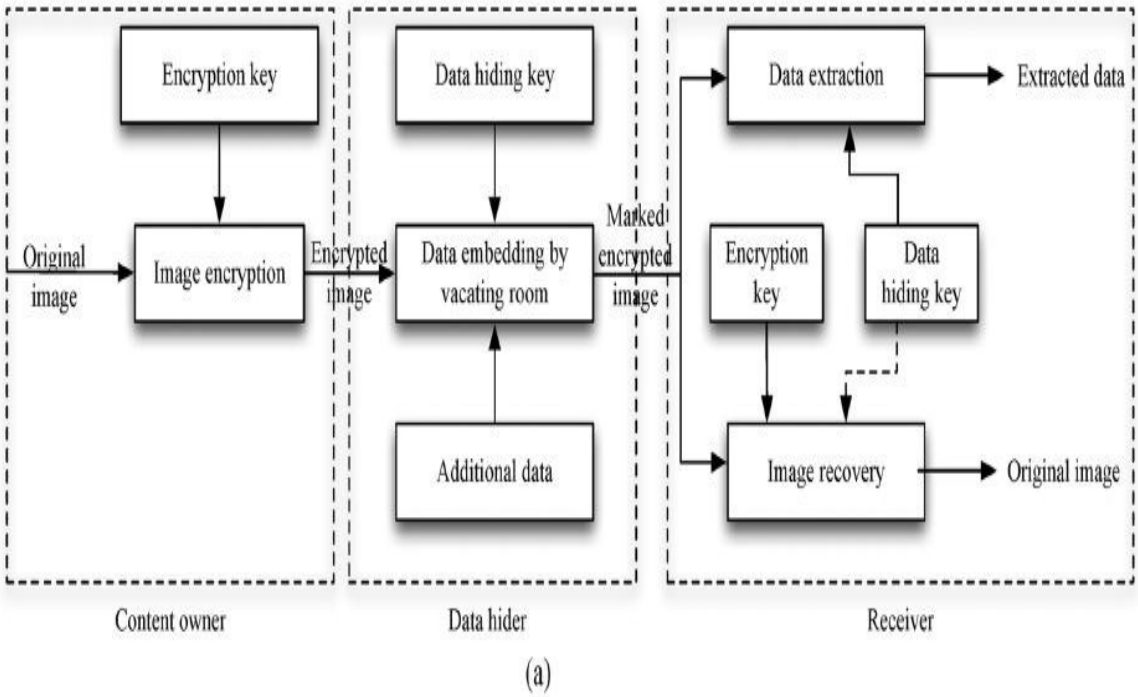


Figure .1 FrameworkVRAE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

Thismethodsegmentstheencryptedimageintoanumberofnon-overlappingblockssizedbya×a,eachblockisusedtocarryoneadditionalbit.Todothis,pixelsineachblockarepseudo-randomlydividedinto two sets.

S1andS2accordingtoadatahidingkey.Iftheadditionalbittobeembeddedis0,flipthe3LSBsofeachencryptedpixelinS1,otherwiseflipthe3encryptedLSBsofpixelsinS2.Fordataextractionandimagerecovery,thereceiverflips.allthethreeLSBsofpixelsinS1toformanewdecryptedblock,andflipsallthethreeLSBsofpixelsinS2toformanothernewblock;oneofthemwillbedecryptedtotheoriginalblock.Duetospatialcorrelationinnaturalimages,originalblockispresumedtobemuchsmootherthaninterferedblockandembeddedbitcanbeextractedcorrespondingly.However,thereisariskofdefeatofbitextractionandimagerecoverywhendividedblockisrelativelysmallor hasmuch fine-detailed textures.

III. PROPOSEDMETHOD

Sincelosslesslyvacatingroomfromtheencryptedimagesisrelativelydifficultandsometimesinefficientandreversingtheorderofencryptionandvacatingroom,i.e.,reservingroompriortoimageencryptionatcontentownerside,theRDHtasksinencrypted images wouldbemorenatural andmucheasierwhichleadstothenovelframework,"ReservingRoomBeforeEncryption(RRBE)".AsshowninFigure.(b),thecontentownerfirstreserveenoughspaceonoriginalimageandthenconvertstheimageintoitsencryptedversionwiththeencryptionkey

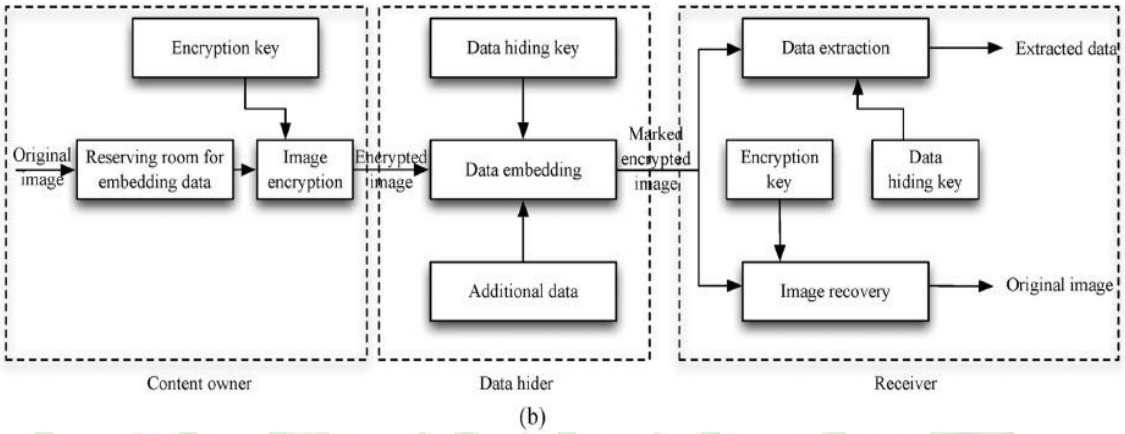


Figure 2.FrameworkRRBE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

Now,thedataembeddingprocessinencryptedimagesisinherentlyreversibleforthedatahiderwhichneedstoaccommodatedataintothesparespacepreviousemptiedout.Thedataextractionandimagerecoveryareidenticaltothatof FrameworkVRAE.Obviously,standardRDHalgorithmsaretheidealoperatorforreservingroombeforeencryptionandcanbeeasilyappliedtoFrameworkRRBEtoachievebetterperformancecompared with techniquesfromFrameworkVRAE.Thisisbecauseinthisnewframework,thecustomaryideaisfollowedi.e.,firstlosslesslycompressestheredundantimagecontent(e.g.,usingexcellentRDHtechniques)andthenencryptsitwithrespecttoprotectingprivacy.Next,elaborateapracticalmethodbasedontheFramework“RRBE”,whichprimarilyconsistsoffourstages:generationofencryptedimage,datahidinginencryptedimage,dataextractionandimagerecovery,dataextractiona nd image restoration.

A. GenerationofEncryptedImage

Actually,toconstructtheencryptedimage,thefirst stagecanbedividedintothreesteps:imagepartition,self-reversibleembeddingfollowedbyimageencryption.At the beginning,imagepartitionstep dividesoriginalimageintotwopartsAandB; then,theLSBsofAarereversiblyembeddedi

therefore,selectstheparticularblockwiththe highest to beA, andputs it to the front oftheimageconcatenatedbytherestpartwithfewer texturedareas.

C.Self-ReversibleEmbedding

Thegoalofself-reversibleembeddingistoembedtheLSB-planesofAintoBbyemployingtraditionalRDHalgorithms.Notethatthisstepdoesnotrelyonan ntoBwithastandardRDHalgorithmsothatLSBsofAcanbeusedforaccommodatingmessages;atlast,encrypttherearrangedimagetogenerateitsfinalversion.

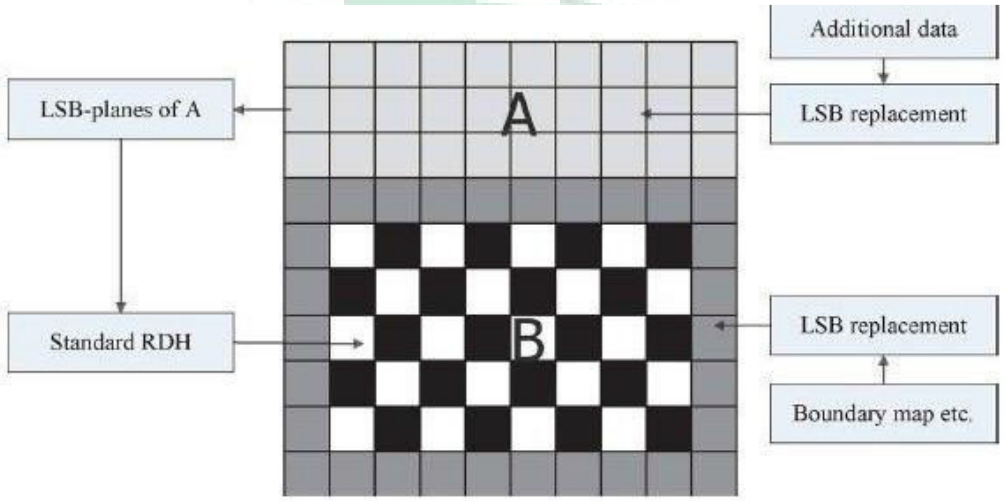
B.ImagePartition

The reserving room beforeencryptionisastandardRDHtechnique,sothegoalofimagepartitionistoconstructasmoother area,on which standard RDHalgorithmscanachievebetterperformance.To do that, without loss of generality,assumetheoriginalimageisan8bitsgray-scaleimagewithitssizeM×NandpixelsCi,j∈[0,255],1≤i≤M≤j≤N.First,thecontentowner extractsfromthe originalimage,alongtherows,severaloverlappingblockswhosenumberisdeterminedbythesizeoftobeembeddedmessages,denotedbyl.In detail, everyblock consists of mrows,where,m=[l/N]andthenumberofblockscanbecomputedthroughn=M-m+1.Animportantpointhereisthateachblockisoverlapped by pervious and/or subsequentialblocksalongtherows. Foreachblock,defineafunctiontomeasureitsfirst-order smoothness. The content owner, yspecificRDHalgorithm.Pixelsintherestofima geBarefirstcategorizedintotwosets:whitepixelswithitsindicesiandjsatisfying(i+j)mod2=0andblackpixels whoseindicesmeet(i+j)mod2=1,asshown in Figure(C).

Furthercalculatethe estimatingerrorsofblackpixelswiththehelpofsurroundingwhitepixels thatmayhavebeenmodified.Thenanotherestimatingerrorsequenceis

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

generatedwhichcanaccommodatemessagesa ndcanalsoimplementmultilayerembeddingsc hemebyconsidering themodifiedB as“original”onewhenneeded.Insummary,toe xploitallpixelsofB,twoestimatingerrorsequen cesareconstructedforembeddingmessagesine verysingle-layerembeddingprocess



(3)

Figure 3.Illustration ofimagepartition and embeddingprocess

C)Image Encryption

Afterrearrangedself-embeddedimage,denotedbyX,isgenerated.Th enencryptXtoconstructtheencryptedimage,de notedbyE.Withastreamcipher,theencryptionv ersionofXiseasilyobtained.

B.DataHidinginEncryptedImageOncethedata hideracquirestheencryptedimage, hecanembedsomedataintoit,althoughhedoesn otgetaccesstotheoriginalimage.Theembeddin gprocessstartswithlocatingthe encrypted version ofA, denotedbyS.

SinceShasbeenrearrangedtothetopof E,itiseffortlessforthedatahidertoread10bitsinf ormationinLSBsoffirst10encryptedpixels.Aft erknowinghowmany

bit-planesandrowsofpixelshecanmodify,thedatahidersimplyadoptsLSBreplacementtosubstitutetheavailablebit-planeswithadditionaldatam.Finally,thedatahidersetsalabelfollowingmtopointouttheendpositionofembeddingprocessandfurtherencryptsmaccordingtothedatahidingkeytoformulatemarkedencryptedimagedenotedbyS.Anyonewhodoesnotpossessthedatahidingkeycouldnotextractthe additionaldata.

D.Data Extraction and Image Recovery

Sincedataextractioniscompletelyindependentfromimagedecryption,theorderofthemimpliestwodifferentpracticalapplications.

Case1:ExtractingDatafromEncryptedImages

Tomanageandupdatepersonalinformationofimageswhichareencryptedforprotecting clients'privacy,aninferiordatabasemanager mayonlygetaccesstothedatahidingkeyandhavetomanipulatedatainencrypteddomain.Theorderofdataextractionbeforeimagedecryptionguaranteesthefeasibilityofourworkinthiscase.Whenthedatabasemanagergetsthedatahidingkey,hecandecrypttheLSB-planesofSandextracttheadditionaldatambydirectlyreadingthedecryptedversion.Whenrequestingfor updatinginformationofencryptedimages,thedatabasemanager,then,updatesinformationthroughLSBreplacementandencryptsupdatedinformationaccordingtothedatahidingkeyallovera gain.Asthewholeprocessisentirelyoperatedonencrypteddomain,itavoids the leakage of original content.

Case2: Extracting Data fromDecryptedImages

InCase1,bothembeddingandextractionofthedataaremanipulatedinencrypteddomain.Ontheotherhand,thereisadifferentsituationthattheuserwantstodecrypttheimagefirstandextractsthedatafromthedecryptedimagewhenitisneeded.Thefollowingexampleisanapplicationforsuchscenario.AssumeAliceoutsourcedherimagestoacloudserver,andtheimagesare encryptedtoprotecttheircontents.Inthatencryptedimages,thecloudservermarkstheimagesby embeddingsomenotation,includingtheidentityoftheimageowner,theidentityofthecloudserverandtimestamps, to manage the encryptedimages.

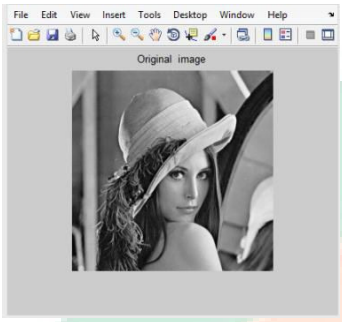
Notethatthecloudserverhasnorighttodoanypermanentdamagetotheimages.Nowanauthorizeduser,Bobwhohasbeensharedtheencryptionkeyandthedatahidingkey,downloadedanddecryptedtheimages.Bobhopedtogetmarkeddecryptedimages,i.e.,decryptedimagesstillincludingthenotation,whichcanbeusedtotracethesourceandhistoryofthedata.Theorderofimagedecryptionbefore/withoutdataextractionisperfectlysuitablefor this case.

IV. EXPERIMENTALRESULTSANDCOMPARISON

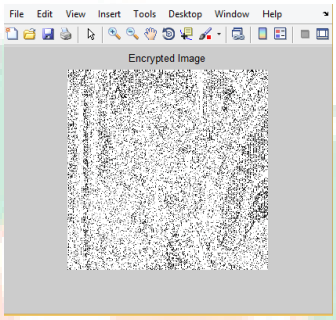
WetakestandardimageLena, showninFigure(D),todemonstratethefeasibilityofproposedmethod.Figure(E)is theencryptedimagecontainingembeddedmessagesandthedecryptedversionwithmessagesisillustratedinFigure(G).Figure (H)depicts therecoveryversionwhichisidenticaltooriginal image.TheReversibleDataHidingwillbetested onpublicavailablestandardimages,whichincludeLena,Airplane,Barbara,Baboon,PeppersandBoat.Thesizeofallimagesis512×512 ×8.

Theoriginalimageusedhereisababc 78
mage.Thisimageisencryptedandthensome ionaldataareembeddedintoit.Figure(5)isadıgıtalwatermarkaddedtoaimage,isamoreorlessvisibleinformationintheformofatextorsomeotherimagethathasbeenaddedtotheoriginalimage.Thea

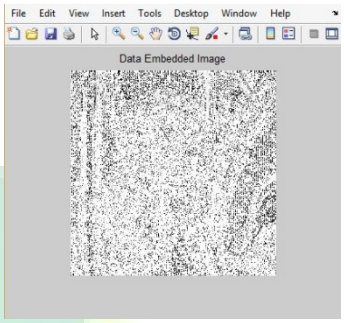
ddedinformationcan bemoreorlesstransparenttomakeiteithereasyorhardtonoticethewatermark.Therearevarioustechniquesforhidingtheinformationintheformofdigitalcontentslikeimage,text,audioandvideo.Basicallydigitalwatermarkingisamethodforembeddingsomesecretinformationandadditionalinformationinthecoverimagewhichcanlaterbeextractedordetectedforvariouspurposeslikeauthentication.



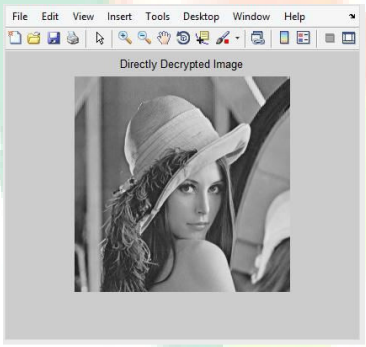
(4)



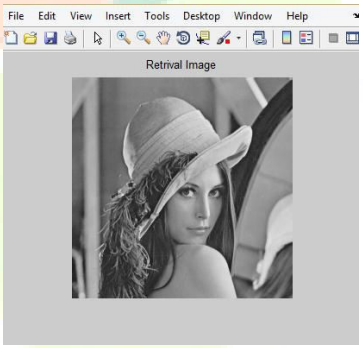
(5)



(6)



(7)



(8)

Figure(4)Original image,(5)Encryptedimage,(6) Image containing messages, (7)decryptedimage,(8)Recoveryversion

TableIshowsthecomparisonresultsmeasuredbyPSNRfordifferentimages,wherethee mbeddingrateismeasuredby bitsperpixel(bpp).ThechoiceofsingleLSB-planeoutperformstheothertwoatlowembeddingratelevels(lessthan0.2bpp).It

isconsistentwithourintuitiveunderstanding,whenembeddingrateissmall,hasthecapacitytoembedLSBsofinasingleroundwithoutsizeenlargement.Furthermore,wepreferusingtwoLSB-planestosingleonewhentheirperformancearecompetitiveinembeddingraterangefrom0.2to0.3bpp.Thisisbecausebyallocatingpartdistortionofinto,the"cut"artifactcanbereducedto certaindegree.ThePeakSignaltoNoiseRatio (PSNR)whichistheratioofmaximumsignalpowertothatofthepowerofnoiseiscalculatedfortheepurposeofreconstructionoftheoriginalimage. Inpractice,weutilizesingleLSB-planetoembedmessageswhenembeddingrateislessthan0.25bpp,andswitchtotwoLSB-planeswithembeddingratelargerthan0.25 bpp.

Input image	Embedding Rate (bpp)	PSNR values (dB)
Baboon	0.1	46.26
Barbara	0.1	51.46
Boat	0.1	52.62
Leena	0.1	52.33
Peppers	0.1	51.02
Airplane	0.1	54.21

Table I PSNR comparison with Embedding Rate

(Ctrl)

V. CONCLUSION

VI.

Reversibledatahidinginencryptedimagesisanewtopicdrawingattentionbecauseoftheprivacypreservingrequirementsfromclouddatamanagement.PreviousmethodsimplementRDHinencryptedimagesbyvacatingroomafterencryption,asopposedtowhichreservingroombeforeencryptionis proposed.Thusthedatahidercanbenefitfromtheextraspaceemptiedoutinpreviousstagetomakedatahidingprocesseffortless.Theproposedmethodcantakeadvantageofalltraditional RDH techniquesfor plain imagesandachieveexcellentperformancewithoutlossofperfectsecrecy.Furthermore,thisnovelmethodcanachieverealreversibility,separatedataextractionandgreatly improvementonthequalityofmarkeddecrypted images.

REFERENCES

[1] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding" in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS6958, 2011, pp. 255–269, Springer- Verlag.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

80

[4] 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.

[5] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst.VideoTechnol., vol.13, no.8, pp.890–896, Aug. 2003.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans.CircuitsSyst.VideoTechnol.,vol.16,no. 3,pp.354–362,Mar. 2006.

[7] D.M. Thodiand, J.J. Rodriguez, “Expansion embedding techniques for reversible watermarking, ”IEEE Trans.Image Process.,vol.16,no.3, pp. 721–730, Mar. 2007.

[8] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533,
Dec. 2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143,
2009.

[10] L. Luoetal, “Reversible image watermarking using interpolation technique,”IEEE Trans. Inf. Forensics Security, vol.5, no.1, pp.187–193, Mar. 2010.

[11] 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., vol.19, no.7, pp. 989–999, Jul.2009.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[13] K. Hwangand, D.Li,“Trusted cloud computing with securer sources and data coloring, ” IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.562

[15] W.Liu, W.Zeng, L.Dong, and Q.Yao, “Efficient compression of encrypted grayscale images, ”IEEE Trans. ImageProcess., vol.19,no.4, pp. 1097–1102, Apr. 2010.

[16] X. Zhang, “Reversible data hiding in encrypted images, ”IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[17] W.Hong, T.Chen, 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.

[18] X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol.7, no.2, pp. 826– 832, Apr.2012.