HIGHLY REVERSIBLE DATA HIDING FOR SOCIAL NETWORKS

Manoranjithan.D[1],Keerthana.M[1], Priyanka.C[1], Karpagavalli.V[1] ,Srividhya.S M.E[2]
[1]Final year B.E , Department of Computer Science and Engineering
Cheran College of Engineering, Karur
[2]AP/Department of Computer Science and Engineering
Cheran College of Engineering, Karur

***Abstract*—Thispaperproposesalossless,areversible,and acombineddatahidingschemes for ciphertext images encrypted by public key cryptosystems with probabilistic andhomomorphicproperties.Inthe losslessscheme,the ciphertextpixelsarereplacedwithnewvaluestoembedthe additionaldataintoseveralLSB-planesofciphertextpixels by multi-layer wet paper coding. Then,theembeddeddata canbe directlyextractedfrom the encrypteddomain, and thedataembeddingoperation does not affect the decryption of original plaintextimage.Inthe reversible scheme, a preprocessingisemployedtoshrinktheimage histogram beforeimage encryption, so that the modification onencryptedimagesfor dataembeddingwill notcause anypixel oversaturationin plaintextdomain. Althoughaslightdistortionis introduced,theembedded datacanbeextracted andthe original imagecanbe recoveredfrom the directlydecryptedimage.Due tothe compatibilitybetween the lossless and reversible schemes, the dataembedding operationsinthetwomannerscanbe simultaneouslyperformed inanencrypted image.Withthe combined technique, areceiver mayextractapart of embeddeddatabeforedecryption,andextractanotherpart of embedded data and recover the originalplaintextimage after decryption.**

***IndexTerms*—reversibledatahiding,losslessdatahiding, image encryption**

I. INTRODUCTION

Encryptionanddatahidingaretwoeffectivemeansofdata protection. While the encryption techniques convert plaintext contentinto unreadable ciphertext, the data hidingtechniquesembedadditionaldataintocovermediaby introducing slight modifications. In some distortion-unacceptable scenarios, data hiding may be performedwithalosslessorreversiblemanner.Althoughthe terms"lossless"and"reversible" haveasamemeaninginaset ofpreviousreferences,wewoulddistinguishtheminthiswork. Mostimagesteganographic algorithmsadoptanexisting imageasacovermedium. Theexpenseofembedding secret messagesintothiscoverimageistheimagedistortionencoun- teredinthe stegoimage. This leadsto two drawbacks.First,sincethe sizeofthecoverimageisfixed,themoresecret messageswhichareembedded allowformoreimagedistor- tion. Wesay a data hidingmethodislosslessifthedisplayofcover signal containingembeddeddataissameasthat of original covereventhoughthe cover data havebeenmodifiedfordata embedding. For example, in [1],the pixels withthe most used colorina palette image are assignedtosome unusedcolor indices forcarryingtheadditional data,andtheseindicesare redirected tothe most used color. This way, although the indicesofthesepixelsarealtered,theactualcolorsofthepixels are kept unchanged. Onthe otherhand,wesaya data hiding methodisreversibleifthe original covercontent can be perfectlyrecoveredfrom thecoverversioncontaining embeddeddataeventhoughaslight distortion has been introducedindataembeddingprocedure. A number of mechanisms,suchas difference expansion[2],histogram shift [3] and lossless compression [4], have been employed to developthereversibledatahidingtechniquesfordigitalimages. Recently,several good predictionapproaches[5]andoptimal transition probability under payload-distortioncriterion[6, 7] havebeenintroducedto improvetheperformanceofreversible data hiding.

Combinationofdatahidingandencryptionhasbeenstudied inrecent years.Insomeworks,datahidingandencryptionare jointedwithasimplemanner.Forexample,apartofcoverdata is usedforcarryingadditional data andthe rest data are encryptedforprivacy protection[8,9]. Alternatively, the additionaldataareembeddedintoadataspacethatisinvariable toencryptionoperations[10].Inanothertypeoftheworks,data embeddingis performedinencrypted domain, andan authorizedreceivercanrecoverthe original plaintext cover imageand extracttheembedded data.This technique is termed asreversible data hidinginencryptedimages(RDHEI). In somescenarios,forsecurely sharingsecret images,acontent ownermay encrypt the images before transmission,and an inferiorassistant ora channel administrator hopestoappend someadditional messages,suchasthe origininformation, image notations or authentication data, within the encrypted imagesthoughhe doesnot knowthe image content.For example, whenmedical images have been encrypted for protectingthe patient privacy, a database administratormay aim toembedthepersonalinformationintothecorresponding encryptedimages. Here, it may be hopeful that the original contentcanberecoveredwithoutanyerrorafterdecryptionand retrieve ofadditional message at receiverside. In[11], the original imageisencryptedbyanexclusive-oroperationwith pseudo-randombits,andthentheadditionaldataareembedded by flippinga part ofleast significant bits (LSB) ofencrypted image. By exploitingthe spatial correlationinnaturalimages, the embedded data andthe original content can be retrievedat receiver side. The performanceof RDHEI can be further

improvedbyintroducinganimplementationorder[12] ora flippingratio[13].In[14],eachadditionalbitisembeddedinto ablockofdataencryptedby theAdvancedEncryption Standard(AES).Whenareceiverdecryptstheencryptedimage containingadditional data, however,the quality ofdecrypted imageissignificantly degradeddue tothe disturbance of additional data.In[15],the data-hidercompressestheLSB of encryptedimageto generateasparsespacefor carrying the additionaldata.Sinceonly theLSBischangedinthe data embeddingphase,the quality ofdirectly decryptedimage is satisfactory.Reversible data hidingschemes forencrypted JPEGimagesisalsopresented[16].In[17],asparsedataspace foraccommodatingadditional datais directly created by compresstheencrypteddata.Ifthe creation ofsparse data space or the compressionis implementedbeforeencryption,a better performance can be achieved[18, 19].

While the additional data are embeddedintoencrypted imageswithsymmetriccryptosystem intheabove-mentioned RDHEImethods,aRDHEImethodwith public key cryptosystem isproposedin[20].Althoughthecomputational complexity is higher,theestablishment ofsecret keythrougha securechannelbetweenthesenderandthereceiverisneedless. Withthemethodin[20],eachpixelisdividedintotwoparts:an evenintegeranda bit,andthe two partsare encrypted using Pailliermechanism [21],respectively.Then,theciphertext values ofthe second partsoftwoadjacent pixelsaremodified toaccommodateanadditional bit.Duetothehomomorphicproperty ofthe cryptosystem,the embedded bit can be extracted bycomparing thecorresponding decrypted values on receiverside.Infact,thehomomorphicpropertymaybefurther exploited to implement signal processinginencrypted domain [22, 23, 24]. Forrecoveringthe original plaintextimage,an inverse operationtoretrieve thesecondpart ofeachpixelin plaintext domainisrequired,andthentwodecryptedpartsof each pixel should be reorganizedas a pixel.

Thispaperproposesalossless,areversible,andacombined data hidingschemes for public-key-encryptedimages by exploiting theprobabilistic and homomorphicpropertiesof cryptosystems. Withtheseschemes, the pixel division/reorganization is avoided and the encryption/decryptionisperformedonthecoverpixelsdirectly, sothattheamount ofencrypteddataandthe computational complexityarelowered.Inthelosslessscheme,duetothe probabilisticproperty,althoughthedataofencryptedimageare modifiedfordataembedding,adirectdecryptioncanstillresult inthe original plaintextimage whiletheembeddeddatacanbe extractedinthe encrypted domain.Inthereversiblescheme,a histogram shrinkisrealizedbeforeencryptionsothatthe modification onencryptedimage for data embeddingdoesnot cause any pixel oversaturationin plaintext domain.Although thedataembedding onencrypted domainmay result ina slight distortioninplaintextdomainduetothehomomorphicproperty, theembeddeddatacanbeextractedandtheoriginalcontentcan berecoveredfrom thedirectlydecryptedimage.Furthermore, thedataembeddingoperationsofthelosslessandthereversible schemescanbesimultaneously performedinan encrypted image.Withthe combinedtechnique,areceivermayextracta part ofembedded data before decryption,andextractanother part ofembedded data andrecoverthe original plaintext image after decryption.

II. LOSSLESSDATAHIDINGSCHEME

In this section, a lossless data hiding scheme for public-key-encryptedimagesis proposed. There are three partiesinthescheme: animage provider,a data-hider,anda receiver.Withacryptosystempossessingprobabilisticproperty, theimageproviderencryptseach pixelof theoriginalplaintext imageusingthepublickeyofthereceiver,andadata-hider who does not know the original image can modify the ciphertextpixel-values toembedsomeadditional dataintothe encryptedimage by multi-layer wet papercodingundera condition that the decrypted values of new and original cipher-text pixel valuesmust besame.When having the encryptedimagecontainingtheadditional data,areceiver knowingthe data hiding key may extract the embedded data, whileareceiverwiththe private key ofthecryptosystem may perform decryptiontoretrievetheoriginalplaintextimage.In other words, the embedded data can be extractedinthe encrypteddomain,andcannot beextractedafter decryption sincethe decryptedimage wouldbesame as the original plaintextimage duetothe probabilisticproperty.That also meansthedataembeddingdoesnotaffectthedecryptionofthe plaintext image.The sketch oflossless data hidingschemeis showninFigure 1.

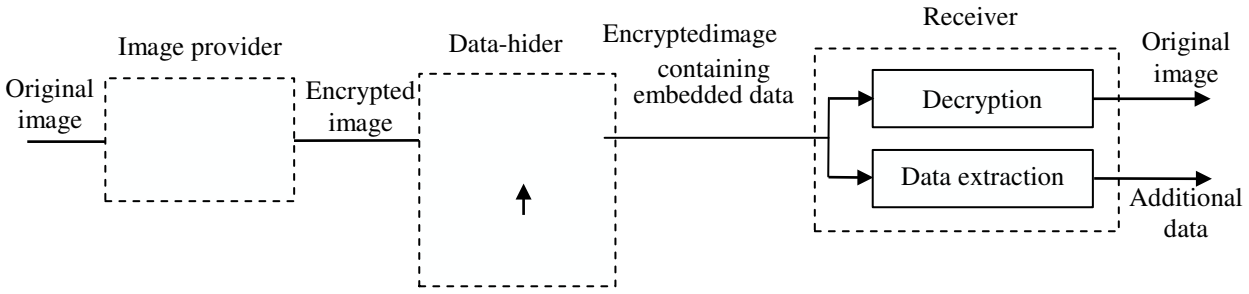


Figure 1. Sketch oflossless data hidingscheme for public-key-encryptedimages

A.Image encryption

Inthisphase,theimageproviderencryptsaplaintextimage usingthepublickeyofprobabilisticcryptosystemp_k.Foreach pixelvalue$m(i,j)$where(i,j)indicatesthepixelposition,the imageprovidercalculatesits ciphertextvalue,

$$c(i,j)=E[p_k,m(i,j),r(i,j)] \quad (1)$$

where$E$istheencryptionoperationand$r(i,j)$isarandomvalue. Then,theimageprovidercollectstheciphertextvaluesofall pixels toformanencryptedimage.

Actually,theproposedschemeiscapitablewithvarious probabilisticpublic-keycryptosystems,suchasPaillier[18] andDamgard-Jurikcryptosystems [25]. With Paillier cryptosystem[18],fortwolargeprimes$p$and$q$,calculate$n=pq$,$\lambda=\mathrm{lcm}(p-1,q-1)$,wherelcmmeanstheleastcommon multiple.Here,itshouldmeetthatgcd$(n,(p-1)(q-1))=1$, wheregcdmeansthegreatestcommondivisor.Thepublickey iscomposedof$n$andarandomlyselectedinteger$g$in$Z^*_{n^2}$, while the private key is composed of$\lambda$and

$$\mu=\left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n \quad (2)$$

where

$$L(x)=\frac{(x-1)}{n} \quad (3)$$

Inthis case,(1)implies

$$c(i,j)=g^{m(i,j)}\cdot(r(i,j))^n \bmod n^2 \quad (4)$$

where$r(i,j)$isarandomintegerinZ^*_n.Theplaintextpixelvalue can be obtained usingthe private key,

$$m(i,j)=L\left((c(i,j))^{\lambda} \bmod n^2\right)\cdot\mu \bmod n \quad (5)$$

As a generalizationofPailliercryptosystem, Damgard-Jurik cryptosystem [25]canbealsousedtoencrypttheplaintext image.Here, thepublickey is composed of$n$andanelement g in $Z^*_{n^{s+1}}$ such that $g=(1+n)^j x \bmod n^{s+1}$ for a known j relativelyprimeto$n$and$x$belongstoagroupisomorphictoZ^*_n, andwemaychoose$d$astheprivatekeywhen meeting$d \bmod n$ $\in Z^*_n$ and$d=0 \bmod \lambda$.Then,theencryptionin(1)can berewrittenas

$$c(i,j)=g^{m(i,j)}\cdot(r(i,j))^n \bmod n^{s+1} \quad (6)$$

where$r(i,j)$isarandomintegerin $Z^*_{n^{s+1}}$.Byapplyinga recursiveversion ofPaillier decryption,the plaintext value can beobtainedfrom theciphertextvalueusingtheprivatekey. Notethat,because ofthe probabilistic property ofthetwo cryptosystems, thesame gray valuesat different positionsmay correspondto different ciphertextvalues.

B.Dataembedding

When havingthe encrypted image, the data-hider may embedsomeadditional dataintoit inalosslessmanner.The pixels in the encryptedimagearerеorganizedasasequence according tothe data hiding key.Foreachencrypted pixel,the data-hiderselectsa randomintegerr′(i,j)inZ^*_nandcalculates

$$c'(i,j)=c(i,j)\cdot(r'(i,j))^n \bmod n^2 \quad (7)$$

ifPailliercryptosystemis usedforimage encryption, while the data-hider selectsa random integer $r'(i,j)$ in $Z^*_{n^{s+1}}$ and calculates

$$c'(i,j)=c(i,j)\cdot(r'(i,j))^{n^s} \bmod n^{s+1} \quad (8)$$

ifDamgard-Jurikcryptosystemisusedforimageencryption. Wedenotethebinaryrepresentationsof$c(i,j)$and$c'(i,j)$as$b_k(i,j)$and$b'_k(i,j)$,respectively,

$$b_k(i,j)=\left\lfloor \frac{|c(i,j)|}{2^{k-1}} \right\rfloor \bmod 2, \quad k=1,2,... \quad (9)$$

$$b'_k(i,j)=\left\lfloor \frac{|c'(i,j)|}{2^{k-1}} \right\rfloor \bmod 2, \quad k=1,2,... \quad (10)$$

Clearly,the probability of$b_k(i,j)=b'_k(i,j)$($k=1,2,\ldots$)is1/2. We also define the sets

$$S_1=\{(i,j)\,|\,b_1(i,j)\neq b'_1(i,j)\}$$
$$S_2=\{(i,j)\,|\,b_2(i,j)\neq b'_2(i,j), b_1(i,j)=b'_1(i,j)\}$$
$$\vdots$$
$$S_K=\{(i,j)\,|\,b_K(i,j)\neq b'_K(i,j), b_k(i,j)=b'_k(i,j), k=1,2,\ldots,K-1\} \quad (11)$$

By viewingthe k-thLSB ofencrypted pixels as awet paper channel(WPC)[26]andthe$k$-thLSBin$S_k$as“dry”elementsof thewetpaperchannel,thedata-hidermayemploythewetpaper coding[26]toembedtheadditional databyreplacingapartof $c(i,j)$ with$c'(i,j)$.The details will be giveninthe following.

ConsideringthefirstLSB,if $c(i,j)$arereplacedwith$c'(i,j)$, thefirstLSBinS_1 wouldbeflippedandtherestfirstLSB wouldbeunchanged.So,thefirstLSBoftheencryptedpixels canberegardedasaWPC,whichincludeschangeable(dry) elementsandunchangeable(wet)elements.Inotherwords, the first LSB in$S_1$are dryelementsandtherestfirstLSBarewet positions.By usingthe wet papercoding[26], one can representonaverageN_d bitsbyonlyflippingapartofdry elements whereN_d is thenumber of dryelements. In this scenario, the data-hidermay flipthe dry elements by replacing $c(i,j)$with$c'(i,j)$.Denotingthenumberofpixelsintheimageas N,the data-hidermay embedonaverage$N/2$bitsinthefirst LSB-layer usingwet papercoding.

ConsideringthesecondLSB(SLSB)layer,wecallthe SLSBinS_2asdryelementsandtherestSLSBaswetelements. NotethatthefirstLSBofciphertextpixelsinS_1 havebeen determinedbyreplacing$c(i,j)$with$c'(i,j)$orkeeping$c(i,j)$ unchangedinthefirst LSB-layerembedding,meaningthatthe SLSBinS_1 areunchangeableinthesecondlayer.Then,the data-hidermayflipapartofSLSBinS_2byreplacing$c(i,j)$with $c'(i,j)$toembed onaverage$N/4$ bits using wet papercoding.

Similarly,inthe$k$-thLSBlayer,thedata-hidermayflipa partof k-th LSB in $S_k$to embed on average $N/2^k$ bits.When the dataembeddingisimplementedin$K$layers,thetotal$N(1-1/2^K)$ bits,onaverage,areembedded.Thatimpliesthe embeddingrate,aratiobetweenthenumberofembedded bitsandthe numberofpixelsincoverimage,isapproximately$(1-1/2^K)$. Thatimpliestheupperboundoftheembeddingrateis1bit per pixel.Thenextsubsectionwillshowthat,althoughapartof$c(i,j)$isreplacedwith$c'(i,j)$,the original plaintext imagecanstill be obtained by decryption.

C.Dataextraction andimage decryption

Afterreceivinganencryptedimage containingthe additional data,ifthe receiver knowsthe data-hiding key,he may calculate the *k*-thLSB ofencrypted pixels,andthen extracttheembeddeddatafrom the*K*LSB-layersusingwet papercoding.Onthe other hand,ifthe receiver knows the private key ofthe usedcryptosystem, he may perform decryptiontoobtaintheoriginalplaintextimage.WhenPaillier cryptosystemis used,Equation(4)implies

$$c(i,j)=g^{m(i,j)}\oplus(r(i,j))^n+\pm\oplus n^2 \quad (12)$$

where±is aninteger.By substituting(12)into(7),there is

$$c'(i,j)=g^{m(i,j)}\oplus(r(i,j)\oplus r'(i,j))^n \bmod n^2 \quad (13)$$

Since$r(i,j)\oplus r'(i,j)$canbeviewedasanotherrandomintegerin Z^*_n, the decryption on$c'(i,j)$ will result inthe plaintext value,

$$m(i,j)=L\left((c'(i,j))^{\tilde{}}\bmod n^2\right)\oplus\propto\bmod n \quad (14)$$

Similarly,whenDamgard-Jurikcryptosystemis used,

$$c'(i,j)=g^{m(i,j)}\oplus(r(i,j)\oplus r'(i,j))^n \quad {}^{s} \bmod n^{s+1} \quad (15)$$

The decryption on$c'(i,j)$ willalsoresultintheplaintext value. In otherwords,the replacement ofciphertext pixel valuesfor data embedding does not affect the decryptionresult.

III. REVERSIBLEDATAHIDINGSCHEME

This sectionproposesareversible data hidingschemefor public-key-encryptedimages.Inthe reversible scheme, a preprocessing is employed to shrink the image histogram, and theneachpixel is encrypted withadditive homomorphic cryptosystem bytheimage provider. Whenhavingthe encryptedimage, the data-hider modifies theciphertext pixel valuestoembeda bit-sequence generatedfrom theadditional data anderror-correction codes. Due tothe homomorphic property,themodificationinencrypteddomainwillresultin slightincrease/decreaseonplaintextpixelvalues,implyingthat adecryptioncanbeimplementedtoobtainanimagesimilarto theoriginalplaintextimageonreceiverside.Becauseofthe histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directlydecryptedimage.Then,theoriginalplaintextimage canberecoveredandtheembeddedadditional data can be extracted fromthedirectlydecrypted image. Notethatthe data-extractionandcontent-recoveryofthereversiblescheme areperformedin plaintext domain,whilethe dataextractionof thepreviouslosslessschemeisperformedinencrypteddomain andthe content recovery is needless.Thesketchofreversible data hidingscheme is giveninFigure 2.

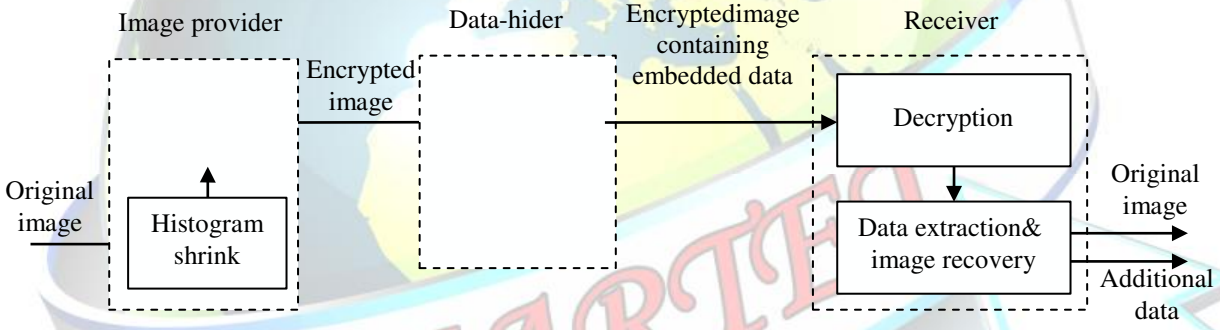


Figure 2.Sketch ofreversible data hidingscheme for public-key-encryptedimages

A.Histogramshrinkandimage encryption

Inthereversiblescheme,asmallintegerxsharedby theimageprovider,thedata-hiderandthereceiverwillbeused, anditsvaluewillbediscussedlater.Denotethenumberof pixelsintheoriginalplaintextimagewithgrayvalue*v*ash_v, implying

$$\sum_{v=0}^{255} h_v = N \quad (16)$$

where*N*isthenumberofallpixelsintheimage.Theimage providercollectsthepixelswithgrayvaluesin[0,x+1],and representtheirvaluesasabinarystreamBS_1.Whenanefficient lossless source codingis used,the length ofBS_1

$$l_1 \approx \sum_{v=0}^{x+1} h_v \oplus H\left(\frac{h_0}{\sum_{v=0}^{x+1} h_v}, \frac{h_1}{\sum_{v=0}^{x+1} h_v}, \cdots, \frac{h_{x+1}}{\sum_{v=0}^{x+1} h_v}\right) \quad (17)$$

where$H(\oplus)$istheentropy function.Theimageprovideralso collects thepixels with gray values in [255↕x, 255], and representtheirvaluesasabinarystreamBS_2withalengthl_2.Similarly ,

$$l_2 \approx \sum_{v=255\updownarrow x}^{255} h_v \oplus H\left(\frac{h_{255\updownarrow x}}{\sum_{v=255\updownarrow x}^{255} h_v}, \frac{h_{255\updownarrow x+1}}{\sum_{v=255\updownarrow x}^{255} h_v}, \cdots, \frac{h_{255}}{\sum_{v=255\updownarrow x}^{255} h_v}\right) \quad (18)$$

Then,thegrayvaluesofallpixelsareenforcedinto[x+1, 255↕x],

$$m'(i,j)=\begin{cases} 255\updownarrow x, & \text{if } m(i,j)\varepsilon 255\updownarrow x \\ m(i,j), & \text{if } x+1<m(i,j)<255\updownarrow x \\ x+1, & \text{if } m(i,j)\delta x+1 \end{cases} \quad (19)$$

Denotingthe new histogramash'_v, there must be

$$h'_v=\begin{cases}0, & v\le\lambda\\ \sum_{v=0}^{\lambda+1} h_v, & v=\lambda+1\\ h_v, & \lambda+1<v<255-\lambda\\ \sum_{v=255-\lambda}^{255} h_v, & v=255-\lambda\\ 0, & v>255-\lambda\end{cases} \quad (20)$$

The image providerfinds the peak ofthe new histogram,

$$V=\arg\max_{\lambda+1\le v\le 255-\lambda} h'_v \quad (21)$$

Theimageprovideralsodividesallpixelsintotwosets:thefirst setincluding ($N/8$)pixelsand thesecond setincludingthe rest 8pixels,andmapseachbitofBS_1,BS_2andtheLSBofpixelsin thesecondsettoapixelinthefirstsetwithgrayvalue V.Since thegray values closetoextreme black/white are rare,there is

$$h'_V<l_1+l_2+16 \quad (22)$$

whenλisnottoolarge.Inthiscase,themappingoperationis feasible.Here,8pixelsinthesecondsetcannotbeusedtocarry BS_1/BS_2sincetheirLSBshouldbeusedtocarrythevalueof$V$, while8pixelsinthefirstsetcannotbeusedtocarryBS_1/BS_2 sincetheirLSBshouldbeusedto carrytheoriginalLSBof the secondset.So,atotalof16pixelscannotbeusedforcarrying BS_1/BS_2.Thatisthereasonthatthere isavalue16 in (22).The experimental result on 1000 natural imagesshows (22) is alwaysrightwhenλislessthan15.So,werecommend the parameterλ<15.Then,a histogramshift operationis made,

$$m'(i,j)=\begin{cases}m_s(i,j), & \text{if } m_s(i,j)>V\\ V, & \text{if } m_s(i,j)=V \text{ and the corresponding bit is 0}\\ V+1, & \text{if } m_s(i,j)=V \text{ and the corresponding bit is 1}\\ m_s(i,j)+1, & \text{if } m_s(i,j)<V\end{cases} \quad (23)$$

Inotherword,BS_1,BS_2andtheLSBofpixelsinthesecondset are carried by the pixels inthe first set. Afterthis,theimage providerrepresentsthe value of$V$as8bitsandmapsthem to the pixelsinthesecondset ina one-to-onemanner.Then,the values of pixels inthe secondset are modifiedas follows,

$$m_k(i,j)=\begin{cases}m_s(i,j), & \text{if LSB of } m_s(i,j) \text{ is same as the corresponding bit}\\ m_s(i,j)+1, & \text{if LSB of } m_s(i,j) \text{ differs from the corresponding bit}\end{cases} \quad (24)$$

Thatmeansthevalueof$V$isembeddedintotheLSBofthe second set.Thisway,allpixelvalues must fall into[λ, 255$-\lambda$].

At last,theimage providerencryptsall pixelsusinga public keycryptosystemwithadditivehomomorphicproperty,suchas PaillierandDamgard-Jurikcryptosystems. When Paillier cryptosystemis used,the ciphertextpixel is

$$c(i,j)=g^{m_T(i,j)}\cdot(r(i,j))^n \bmod n^2 \quad (25)$$

And,whenDamgard-Jurikcryptosystemisused,theciphertext pixelis

$$c(i,j)=g^{m_T(i,j)}\cdot(r(i,j))^{n^s} \bmod n^{s+1} \quad (26)$$

Then,theciphertextvaluesofallpixelsarecollectedtoforman encryptedimage.

B.Dataembedding

Withtheencryptedimage,the data-hiderdivides the ciphertextpixelsintotwoset: SetAincluding$c(i,j)$withodd value of $(i+j)$,andSet Bincluding$c(i,j)$withevenvalueof $(i+j)$. Without loss of generality,wesupposethe pixel number inSetAis$N/2$.Then,thedata-hideremployserror-correction codesexpandtheadditionaldataasabit-sequencewithlength $N/2$,andmapsthe bitsinthe coded bit-sequence tothe ciphertext pixelsinSetAina one-to-one manner, whichis determinedbythedata-hidingkey.WhenPailliercryptosystem isused,ifthebitis0,thecorrespondingciphertextpixelis modifiedas

$$c'(i,j)=c(i,j)\cdot g^{n^{\lambda}}\cdot(r'(i,j))^n \bmod n^2 \quad (27)$$

where$r'(i,j)$isaintegerrandomlyselectedinZ^*_n.Ifthebitis1, the correspondingciphertextpixel is modifiedas

$$c'(i,j)=c(i,j)\cdot g^{\lambda}\cdot(r'(i,j))^n \bmod n^2 \quad (28)$$

WhenDamgard-Jurikcryptosystemisused,ifthebitis0,the correspondingciphertextpixel is modifiedas

$$c'(i,j)=c(i,j)\cdot g^{n^{s+1}-\lambda}\cdot(r'(i,j))^{n^s} \bmod n^{s+1} \quad (29)$$

where$r'(i,j)$isaintegerrandomlyselected in$Z^*_{n^{s+1}}$.If thebit is 1,the correspondingciphertextpixel is modifiedas

$$c'(i,j)=c(i,j)\cdot g^{\lambda}\cdot(r'(i,j))^{n^s} \bmod n^{s+1} \quad (30)$$

Thisway,anencryptedimagecontainingadditional datais produced. Notethat theadditionaldataareembeddedintoSet A.Althoughthe pixelsinSet B may providesideinformation ofthepixel-valuesinSet A, whichwill be usedfor data extraction,thepixel-valuesinSetAaredifficulttobeprecisely obtainedonreceiverside,leadingtopossibleerrorsindirectly extracteddata.So,theerror-correctioncodingmechanismis employedheretoensuresuccessfuldataextractionandperfect image recovery.

C.Image decryption, dataextraction andcontent recovery

After receivinganencryptedimage containingadditional data,thereceiverfirstly performs decryptionusinghis private key.We denotethe decryptedpixelsas$m'(i,j)$. Due tothe homomorphicproperty,thedecryptedpixelvaluesinSet Ameet

$$m'(i,j)=\begin{cases}m_T(i,j)+\lambda, & \text{if the corresponding bit is 1}\\ m_T(i,j)-\lambda, & \text{if the corresponding bit is 0}\end{cases} \quad (31)$$

Ontheotherhand,thedecryptedpixelvaluesinSetBarejust $m_T(i,j)$since theirciphertextvalues are unchangedin data embeddingphase.Whenλissmall,thedecryptedimage is perceptually similartothe original plaintext image.

Then,thereceiverwiththedata-hidingkeycanextractthe embeddeddatafromthedirectlydecryptedimage.Heestimates thepixel values inSet A usingtheir neighbors,

$$\bar{m}_T(i,j)=\frac{m_T(i-1,j)+m_T(i,j-1)+m_T(i+1,j)+m_T(i,j+1)}{4} \quad (32)$$

andobtainanestimatedversionofthecodedbit-sequenceby comparingthedecryptedandestimatedpixelvaluesinSetA. Thatmeansthecodedbitisestimatedas0if$m_T(i,j)>\bar{m}'(i,j)$ or as1 if $\bar{m}_T(i,j)\le m'(i,j)$. With theestimate of coded

bit-sequence,the receivermay employ the error-correction methodtoretrievethe originalcoded bit-sequence andthe embeddedadditionaldata.Notethat,withalarger×,theerror rateintheestimateofcodedbitswouldbelower,sothatmore additionaldatacanbeembeddedwhenensuring successfulerrorcorrectionanddataextraction.Inotherwords,asma ller ×would resultin ahighererrorrate in theestimateofcoded bits, so thatthe error correction may be unsuccessful when excessivepayloadisembedded.That meanstheembedding capacityofthereversibledatahidingschemeisdependedon the value of×.

Afterretrievingthe original coded bit-sequence and the embeddedadditional data, the original plaintext image may be furtherrecovered.Forthe pixelsinSet A,$m_T(i,j)$areretrieved accordingtothe coded bit-sequence,

$$m_T(i,j)=\begin{cases} m'(i,j)\updownarrow\times, & \text{ifthecorrespondingbitis1} \\ m'(i,j)+\times, & \text{ifthecorrespondingbitis0} \end{cases} \quad (33)$$

ForthepixelsinSetB,asmentionedabove,$m_T(i,j)$arejust$m'(i,j)$.Then,dividesall$m_T(i,j)$intotwosets:thefirstoneincluding $(N\updownarrow 8)$pixelsandthesecondoneincludingtherest8pixels.The receivermay obtainthe value of$V$from theLSBinthesecond set,andretrieve$m_S(i,j)$ ofthe first set,

$$m_S(i,j)=\begin{cases} m_T(i,j), & \text{if}\ m_T(i,j)>V \\ V, & \text{if}\ m_T(i,j)=V\ \text{or}\ V\updownarrow 1 \\ m_T(i,j)+1, & \text{if}\ m_T(i,j)<V\updownarrow 1 \end{cases} \quad (34)$$

Meanwhile, the receiverextractsabit0 fromapixelwith$m_T(i,j)=V$andabit1fromapixelwith$m_T(i,j)=V\updownarrow 1$. After decomposingthe extracted data intoBS_1, BS_2andtheLSB of $m_S(i,j)$inthesecondset,thereceiverretrieves$m_S(i,j)$ofthe secondset,

$$m_S(i,j)=\begin{cases} m_T(i,j), & \text{ifLSBof}\ m_S(i,j)\ \text{and}\ m_T(i,j)\ \text{aresame} \\ m_T(i,j)+1, & \text{ifLSBof}\ m_S(i,j)\ \text{and}\ m_T(i,j)\ \text{aredifferent} \end{cases} \quad (35)$$

Collectallpixelswith$m_S(i,j)=\times+1$,and,accordingtoBS_1, recovertheiroriginalvalueswithin$[0,\times+1]$. Similarly, theoriginalvaluesofpixelswith$m_S(i,j)=255\updownarrow\times$arerecovered within$[255\updownarrow\times,255]$accordingto$BS_2$.Thisway,theoriginal plaintext image is recovered.

IV. COMBINEDDATAHIDINGSCHEME

AsdescribedinSections3and4,alosslessandareversible data hidingschemesfor public-key-encryptedimages are proposed.Inbothofthetwoschemes,thedataembedding operations are performedinencrypteddomain.Onthe other hand, the dataextractionprocedures ofthetwoschemesare very different. Withthe lossless scheme, data embedding does notaffectthe plaintext content and dataextractionisalso performedinencrypted domain.Withthe reversible scheme, there is slight distortionin directly decryptedimagecausedby data embedding, and data extraction and imagerecovery must beperformedinplaintext domain.That implies, onreceiver side,theadditional dataembedded by thelosslessscheme cannot beextractedafter decryption, whiletheadditional data embeddedbythe reversible scheme cannot extracted before decryption.Inthissection,wecombinethe lossless and reversible schemestoconstruct a newscheme,in whichdata extraction ineither ofthe two domains is feasible. That means theadditionaldata for various purposes may be embeddedinto anencryptedimage,andapartoftheadditionaldatacanbe extractedbeforedecryptionandanotherpartcanbeextracted after decryption.

Inthecombinedscheme, the image provider performs histogram shrinkandimageencryptionas describedin Subsection 3.A. When having the encrypted image, the data-hider mayembedthefirstpartofadditionaldatausing the method describedinSubsection 3.B. Denotingtheciphertext pixelvaluescontainingthefirstpartofadditionaldataas$c'(i,j)$, thedata-hidercalculates

$$c''(i,j)=c'(i,j)\oplus(r''(i,j))^n \bmod n^2 \quad (36)$$

or

$$c''(i,j)=c'(i,j)\oplus(r''(i,j))^n \bmod n^{s+1} \quad (37)$$

where$r''(i,j)$arerandomlyselectedinZ^*_nor$Z^*_{n^{s+1}}$ forPaillier andDamgard-Jurik cryptosystems, respectively. Then, he may employ wet papercodinginseveral LSB-planes ofciphertext pixelvaluestoembedthesecondpartofadditionaldataby replacinga part of$c'(i,j)$ with$c''(i,j)$.In other words, the methoddescribedinSubsection2.Bis used to embed the secondpartofadditionaldata.Onreceiverside,thereceiver firstlyextracts thesecondpartofadditionaldatafromthe LSB-planes ofencrypted domain.Then,afterdecryptionwith his private key, he extracts the first part ofadditional dataand recoverstheoriginalplaintextimagefrom thedirectly decryptedimage asdescribedinSubsection3.C.Thesketchof thecombinedschemeisshowninFigure3.Notethat,sincethe reversibly embedded datashould beextractedintheplaintext domainandthe lossless embedding does not affect the decrypted result, the losslessembeddingshouldimplemented afterthe reversible embeddinginthe combinedscheme.

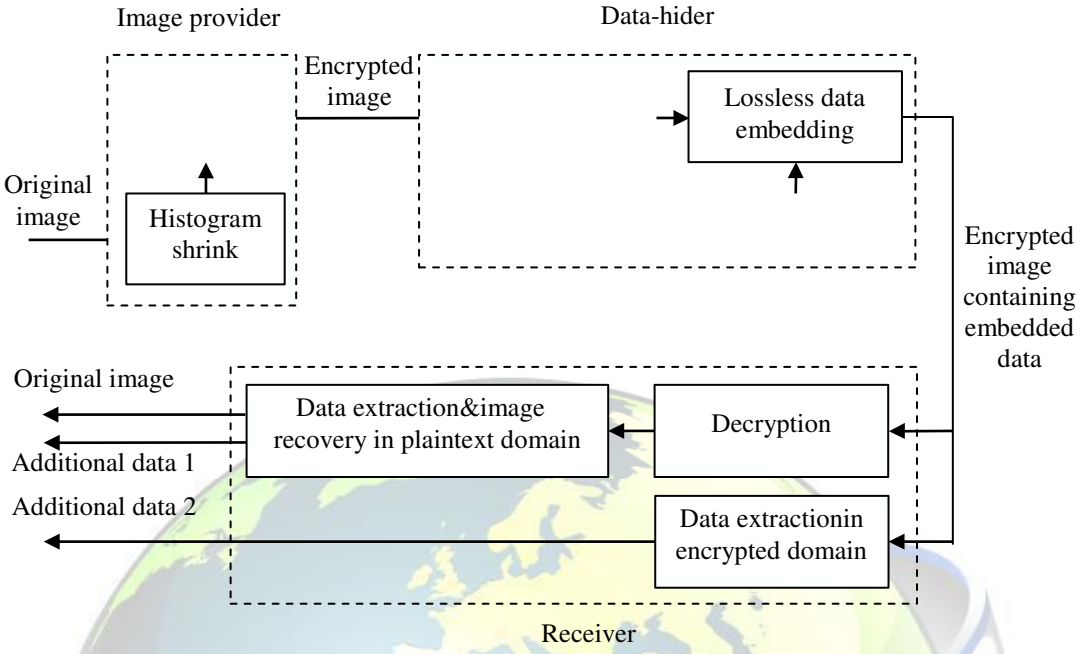


Figure 3.Sketch ofcombinedscheme

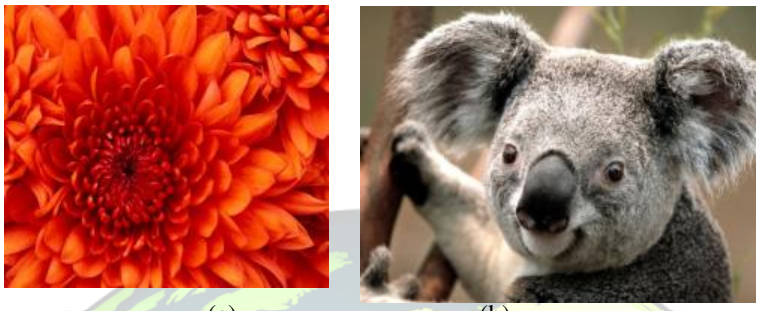
V. EXPERIMENTALRESULTS

Fourgrayimagessized512 - 512, Lena,Man,Planeand Crowd,shoninFigure4,and50naturalgrayimagessized 1920 - 2560,which contain landscape and people, were usedas the original plaintext coversintheexperiment.With the lossless scheme, all pixels inthe coverimages were firstly encrypted using Paillier cryptosystem, and then the additional data wereembedded into the LSB-planes of ciphertext pixel-values usingmulti-layer wet papercoding as in Subsection 2.B. Table 1 lists the average value ofembedding rateswhen$K$LSB-planeswereused forcarrying theadditional datainthe54encryptedimages.Infact,theaverageembedding rateisverycloseto($1\updownarrow 1/2^{K}$).Onreceiverside,theembedded datacanbeextractedfromtheencrypteddomain. Also,the original plaintext images can be retrieved by direct decryption. Inotherword,whenthedecryptionwas performedonthe encrypted images containing additional data, the original plaintext images were obtained.

Withthe reversible scheme, all pixels were encryptedafter histogram shrinkasinSubsection3.A.Then,ahalfof ciphertextpixels weremodifiedtocarry theadditional dataas inSubsection 3.B, andafterdecryption,weimplementedthe dataextractionandimagerecovery inthe plaintext domain. Here,thelow-densityparity-check(LDPC)codingwasusedto expandtheadditionaldataasabit-sequenceindataembedding phase,andtoretrievethecodedbit-sequenceandtheembedded additional data onreceiverside.Althoughtheerror-correction mechanismwasemployed,anexcessivepayloadmaycausethe failure of data extractionandimage recovery.Witha larger valueofχ, ahigherembeddingcapacitycouldbe ensured, whileahigherdistortionwouldbeintroducedintothedirectly decryptedimage.Forinstance,whenusingLenaasthecover andχ= 4,atotal of$4.6 - 10^{4}$bitswereembeddedandthevalue ofPSNRindirectlydecryptedimagewas40.3dB.Whenusing χ=7,atotalof$7.7 - 10^{4}$ bitswereembeddedandthevalueof PSNRindirectlydecryptedimagewas36.3dB.Inbothofthe twocases,theembeddedadditional dataandthe original plaintextimagewereextractedandrecoveredwithoutanyerror. Figure5givesthetwo directly decryptedimages.Figure6 showstherate-distortioncurvesgeneratedfromdifferentcover imagesandvarious values ofχunder the condition of successful data-extraction/image-recovery.The abscissa representsthe pure embeddingrate, andthe ordinateis the PSNR value indirectly decryptedimage.Therate-distortion curves onfourtest images,Lena,Man,Plane andCrowd,are giveninFigures 6,respectively.We alsoused50natural gray images sized 1920 - 2560asthe original plaintextcovers,and calculated the average values ofembeddingratesandPSNR values,which arealso shown asacurvemarked byasterisks in the figure. Furthermore, Figure 7 compares the average rate-PSNRperformancebetweenthe proposedreversible schemewith public-key cryptosystemsandseveral previous methods with symmetric cryptosystems underaconditionthat theoriginalplaintextimagecanberecoveredwithoutanyerror using the data-hidingandencryptionkeys.In[11] and[12], each block of encryptedimage with givensize is usedtocarry oneadditionalbit.So,theembeddingratesofthetwoworksare fixedandlow.With various parameters, we obtain the performancecurvesofthe methodin[15] andthe proposed reversiblescheme,whichareshowninthefigure.Itcanbeseen that the proposedreversibleschemesignificantly outperforms thepreviousmethodswhentheembeddingrateislargerthan 0.01bpp.

With thecombined scheme,we implementedthe histogram shrinkoperationwithavalueofparameterχ,andencryptedthe

pixelsusingPailliercryptosystem.Then,weembeddedthefirst part ofadditional dataintotheciphertextpixel values by the reversibleembeddingmethod,andembeddedthesecondpart ofadditionaldataintothe*K*LSB-planesof theciphertextpixel values by thelossless embedding method. When having the encryptedimage containingthe additional data,we firstly extracted the second part of additional data from the LSB-planes ofciphertext pixel values. After decryption, we further extractedthe first part ofadditional dataandrecovered the original plaintext imageintheplaintextdomain.Here,the payloads of the twoparts ofadditional dataaresameasthe payloads ofreversible andlossless schemes,respectively,and the qualityof directly decrypted image is same as thatof reversible scheme.



(a) (b)

Figure 4.Coverimage-a) Chrysanthemum,Secret image-b)Koala

(a) (b)

Figure5.Directlydecryptedofreversiblescheme(a)×=4,atotalof4.6 - 10^4bitsembeddedandPSNR=40.3dB,(b)×=7, a total of 7.7 - 10^4bits embeddedandPSNR = 36.3 dB

VI. CONCLUSION

Thisworkproposesalossless,areversible,andacombined datahidingschemesforcipher-textimagesencryptedbypublic key cryptography with probabilistic and homomorphicproperties.Inthelossless scheme,theciphertextpixel values arereplacedwithnewvaluesforembeddingtheadditionaldata intotheLSB-planes ofciphertextpixels. This way, the embeddeddatacanbedirectlyextractedfrom theencrypted domain, andthe data embeddingoperationdoes notaffectthe decryptionoforiginalplaintextimage.Inthereversiblescheme, apreprocessingofhistogramshrinkismadebefore encryption, anda halfofciphertext pixel values are modifiedfor data embedding.Onreceiverside,theadditional data can be extractedfrom theplaintext domain,and,althoughslight distortionis introducedin decryptedimage, the original plaintext image can berecoveredwithoutanyerror.Duetothe compatibility ofthetwoschemes,the data embedding operations of the lossless andthereversibleschemescanbe simultaneously performedinanencryptedimage. So, the receivermay extract a part ofembedded dataintheencrypted domain,andextractanotherpartofembeddeddataandrecover the original plaintext image inthe plaintext domain.

REFERENCES

[1] N.A.Saleh,H.N.Boghdad,S.I.Shaheen,A.M.Darwish,"High Capacity LosslessDataEmbedding Technique forPaletteImagesBased onHistogramAnalysis,"*DigitalSignalProcessing*, 20,pp.1629↕1636, 2010.

[2] J.Tian,"ReversibleDataEmbeddingUsingaDifferenceExpansion," *IEEETrans.onCircuitsandSystemsforVideoTechnology*,13(8),pp. 890↕896,2003.

[3] Z.Ni,Y.-Q.Shi, N.Ansari,andW.Su, "ReversibleDataHiding,"*IEEE Trans.onCircuitsandSystemsforVideoTechnology*,16(3),pp.354↕362, 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, andE. Saber, "Lossless Generalized-LSBDataEmbedding," *IEEETrans.onImageProcessing*, 14(2),pp.253–266,2005.

[5] X.Hu,W.Zhang,X.Li,andN.Yu,"MinimumRatePredictionand OptimizedHistogramsModification forReversibleDataHiding,"*IEEE Trans.onInformationForensicsandSecurity*,10(3),pp.653-664,2015.

[6] X.Zhang,"ReversibleData Hiding withOptimalValue Transfer,"*IEEE Trans.onMultimedia*,15(2),316↕325,2013.

[7] W.Zhang,X.Hu,X.Li,andN.Yu,"OptimalTransitionProbability of ReversibleDataHidingforGeneralDistortion MetricsandIts Applications,"*IEEETrans.onImageProcessing*,24(1),pp.294-304, 2015.

[8]S.Lian,Z.Liu,Z.Ren,andH.Wang,"CommutativeEncryptionand WatermarkinginVideoCompression,"*IEEETrans.onCircuitsand SystemsforVideoTechnology*,17(6),pp.774↕778,2007.
[9] M.Cancellaro,F.Battisti,M.Carli,G.Boato,F.G.B.Natale,andA.Neri, "ACommutativeDigitalImageWatermarkingandEncryptionMethodin theTree StructuredHaarTransformDomain,"*Signal Processing:Image Communication*,26(1),pp.1↕12,2011.
[10] X. Zhang, "Commutative Reversible Data Hiding and Encryption," *SecurityandCommunicationNetworks*,6,pp.1396↕1403,2013.
[11] X.Zhang,"ReversibleDataHidinginEncryptedImage,"*IEEESignal ProcessingLetters*,18(4),pp.255↕258,2011.
[12] W.Hong,T.-S.Chen,andH.-Y.Wu,"AnImprovedReversibleData HidinginEncryptedImagesUsingSideMatch,"*IEEESignalProcessing Letters*,19(4),pp.199↕202,2012.
[13] J.Yu,G.Zhu,X.Li,andJ.Yang,"AnImprovedAlgorithmforReversible DataHidinginEncryptedImage,"*Proceeding ofthe11thInternational WorkshoponDigital-Forensics Watermark(IWDW2012)*,Shanghai, China,Oct.31-Nov.02,2012,LectureNotesinComputerScience,7809, pp.358-367,2013.
[14] W.Puech,M.Chaumont,andO.Strauss,"AReversibleDataHiding MethodforEncryptedImages,"*Security,Forensics,Steganography,and WatermarkingofMultimediaContentsX*,*Proc.SPIE*,6819,2008.
[15] X.Zhang,"SeparableReversibleDataHidinginEncryptedImage,"*IEEE Trans.InformationForensics&Security*,7(2),pp.526↕532,2012.
[16] Z.Qian,X.Zhang,andS.Wang,"ReversibleDataHidinginEncrypted JPEGBitstream,"*IEEETrans.onMultimedia*,16(5),pp.1486↕1491, 2014.
[17] M.S.A.Karim,andK. Wong,"UniversalData Embeddingin Encrypted Domain,"*SignalProcessing*,94,pp.174-182,2014.
[18] K.Ma,W.Zhang,X.Zhao,N.Yu,andF.Li,"ReversibleDataHidingin EncryptedImagesbyReservingRoomBefore Encryption,"*IEEETrans. InformationForensics&Security*,8(3),pp.553-562,2013.
[19] W.Zhang,K.Ma,andN.Yu,"ReversibilityImprovedDataHidingin EncryptedImages,"*SignalProcessing*,94,pp.118-127,2014.
[20] Y.-C.Chen,C.-W.Shiu,andG.Horng,"EncryptedSignal-Based Reversible DataHiding with Public Key Cryptosystem,"*Journal of VisualCommunicationandImageRepresentation*,25,pp.1164-1170, 2012