European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 08, Issue 04, 2021

Quantum Cryptography helps to enhance on security issues.

Mr.BGiridhar
Associate Professor, Computer Science and Engineering
Sri Venkateswara College of Engineering and Technology, Srikakulam, A.P., India

Abstract
Stegnography is the technique of hiding confidential information within anymedia.Inrecentyearsvarious stegnography methods have been proposed to makedatamoresecure.Atthesametimedifferentsteganalysismethods have also evolved. The number of attacks used by thesteganalyst has only multiplied over the years. Various toolsfor detecting hidden information's are easily available over theinternet, so securing data from steganalyst is still considered amajorchallenge.Whilevariousworkhavebeendonetoimprove the existing algorithms and also new algorithms havebeenproposedtomakedatabehindtheimagemoresecure.Wehave still been using the same public key cryptography likeDeffie-HellmanandRSAforkeynegotiationwhichisvulnerable to both technological progress of computing powerandevolutioninmathematics,sointhispaperwehaveproposeduseofquantumcryptographyalongwithstegnography.Theuseof this combination will createkeydistributionschemesthatareuninterceptable thusprovidingour dataaperfectsecurity.

Keywords-Stenography,Steganalysis,Steganalyst,Quantum Cryptography.

1. Introduction

Internet users frequently need to store, send and receiveprivate information. The most common way to do this isto transform the data into different forms. The resultingdata can be understood only by those who know how toreturn it to its original form. This method of protectinginformation is known as encryption. A major drawbackto encryption is that the existence of data is not hidden.Data that has been encrypted, although unreadable, stillexists as data.If given enoughtime,someone couldeventuallydecryptthedata.Asolutiontothisproblemisstegnography.Stenography isalsoaformofwritingnamely concealed writing.

The Greek word *staginess* means "unseen" or "hidden."Stegnographyisthusaformofcommunication,whichisdesigned to be hidden from general view. Stegnographyshould notbe seen as a replacementfor cryptographybutratherasa complement to it.. There has been a rapid growth ofinterest in this subject over the last two years, and fortwomainreasons.Firstly,thepublishingandbroadcastingindustrieshavebecomeinterestedintechniques for hiding encryptedcopyrightmarks andserialnumbersindigitalimages,audiorecordings,books and multimedia products; an appreciation of newmarket opportunities created by digital distribution iscoupled with a fear that digital works could be too easyto copy. Secondly, moves by various governments torestricttheavailabilityofencryptionserviceshavemotivated people to study methodsby

which privatemessagescanbeembeddedinseeminglyinnocuouscovermessages.Inmoderntermssteg nographyisusuallyimplementedcomputationally,wherecoverWorks such as text files, images, audio files, and videofilesaretweakedinsuchawaythatasecret messagecanbeembedded withinthem.

Thetechniquesareverysimilartothatofdigitalwatermarking;howeveronebigdistinctionmustb ehighlighted between the two. In digital watermarking,thefocusisonensuringthatnobodycanremoveoralterthecontentofthewatermar keddata,eventhoughitmightbeplainlyobviousthatitexists.Stegnography on the other hand, focuses on making itextremely difficult to tell that a secret message exists atall. Ifanunauthorizedthirdpartyisabletosaywithhighconfidence that a file contains a secret message, thenstegnography has failed. Stegnography also differs fromcryptography because the latter does not attempt to hidethe factthatamessageexists.Instead,cryptographymerelyobscurestheintegrityoftheinformations othatit does not make sense to anyone but the creator and therecipient.The artof detecting stegnography is referredto as steganalysis. With rapid advances in the field ofstegnographyandcryptography therehavealsobeenmajor advances made in the field of steganalysis andcryptanalysis.Typically,asteganalysisbeginsbyidentifyinganyartifactsthatexistsinthesus pectfileasa result of embedding a message. Electronically, each ofthe tool used for stegnography leaves a fingerprint orsignatureintheimagethatcanbeexploitedtofindthe message in the image. Steganalysis does not howeverconsider the successful extraction of the message, thereisusuallya requirementofcryptanalysis.

So, after performing cryptanalysis on the cipher text, theplain text can easily be obtained. Over the years ourfocushasbeenmainlyonsecurityofdatabutthesecurity of keys is as important as the security of data.Often this aspect is neglected. We have been using thesamepublickeycryptosystemfor manyyearsnow.

Since,uncertainlyloomsoverthesecurityofthesecryptosystems; we have used quantum cryptography forsecuring the key distribution. Quantum cryptography isthought to be secure for three main reasons. One, thequantum no-cloning theoremstatesthatanunknownquantum state cannot be cloned. Theoretically, messagessentusingquantumcryptographywouldbeinanunknownquantumstate,sotheycouldnot becopiedandsent on. Two, in a quantum system, which can be in oneof two states, any attempt to measure the quantum statewilldisturbthesystem.Aquantummessagethatisintercepted and read by an eavesdropper will becomegarbledanduselesstotheintendedrecipientofthemessage. Three, the effects produced by measuring aquantumpropertyareirreversible,whichmeansaneavesdropper cannot “put back” a quantum message toitsoriginalstate.Thesethreepropertiesprovidethepowerofquantumcryptography.

2. Related Work

S. K. Moon et al proposed an algorithm to hide data ofany format in an image and audio file (S.K Moon et al2007).For stegnography he used the least significant bit (4 LSB) substitution method. The 4LSB method wasimplemented for color bitmap images and wave files asthe carrier media.A new method of stegnography inMMS was proposed by Mohammad Shirali et al .Thispaper presented a new method of stegnography usingboth image and text stegnography methods. This projectwas written in J2ME (Java 2 Micro Edition) .In thismethod, data is broken into two parts with proper sizesand the parts were hidden in the image and text part ofMMS message (Mohammad Shirali et al 2007).In orderto further enhance the secrecy of stegnographyPiyushMarwaha and PraveshMarwaha (PiyushMarwaha et al2010) proposed an advanced system of encrypting datathatcombinesthefeaturesofcryptography,stegnography along with multi-media data hiding. Thispaper proposed the conceptof multiple cryptographywhere the data will be encrypted in a cipher and thecipher will be hidden into a multimedia image file inencryptedformat.Thissystemwasmoresecurethananyother these techniques alone and also as compared tostegnographyand cryptography combined systems

.MuhammadAsadetalproposedanenhancedleastsignificantbitforaudiostegnography(Muha mmadAsadetal2011hispaperproposestwowaystoimprove the conventional LSB modification technique. The firstway is to randomize bit number of host message used forembedding secret message while the second way is torandomizesamplenumbercontainingnextsecretmessage bit. The improvised proposed technique

worksagainststeganalysisanddecreasestheprobabilityofsecretmessagebeingextractedbyanin truder.Mohammad Hamdaqa used VoIP (Voice over IP) forrealtime network stegnography,which

utilizesVoIPprotocolsandtrafficasacovertchanneltoconcealsecretmessages.Thispapermodif iesthe(k,n)thresholdsecret sharing scheme, which is based on *Lagrange'sInterpolation*, and then applies a two phase approach ontheLACKstegnographymechanismtoprovidereliabilityandfaulttoleranceandtoincreaseste ganalysiscomplexity(MuhammadHamdaqaetal2011).A new perfect hashing based approach was givenbyImranSarwarBajwaetal.Ituseshashingbasedapproach for stegnography in grey scale images. Theproposed approach is more efficient and effective thatprovidesamoresecurewayofdatatransmissionathigher speed**.** The presented approach is implementedinto a prototype tool coded in VB**.**NET (Imran SarwarBajwaet al2011).

3. Proposed Work

Theproposedworkconsistsofthegivendiscussedphases.

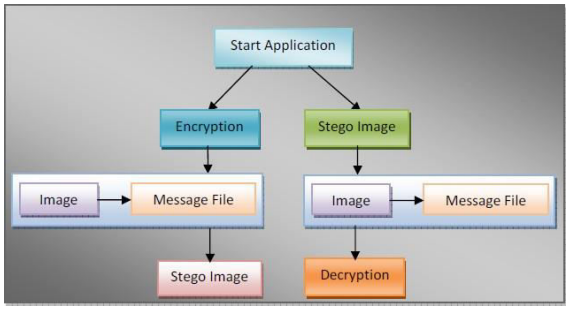
3.1 Stegnography

Steganography literally means covered writing. Its goalis to hide the fact that communication is taking place.Steganographyismainlyappliedtomediasuchasimages,text,videoclips,musicandsound s.Imagesteganographyisgenerallymorepreferredmediabecause of its harmlessness and attraction.The threebasictechniquesusedforsteganographyareclassifiedasfollows:

(A)-Injection-Hiding datainsectionsoffilethatareignored by the processing applications. Therefore avoidmodifying those file bits that are relevant to an end userleavingthecoverfileperfectlyusable.

(B)-Substitution-Replacement of least significant bits ofinformationthatdeterminethemeaningfulcontentoftheoriginal file with new data in a way that causes leastamountofdistortion.

(C)-Generation-Unlikeinjectionandsubstitution,thisdoes not require an existing cover file



but generates acover file for the sole purpose of hiding the message.Therearemanyalgorithmsthatcanbeusedforstegnography. The algorithm which we have used herefor stegnography is F5 which is much more secure thanall the other algorithms. The F5 algorithm provides highstenographiccapacityandcanprevent visual attacksand itisalsoresistanttostatisticalattacks.Eveniftheattacker is able to break this algorithm, he will get backonlytheciphertextandwillhavetoperformcryptanalysis on it to get back the original text. Fig 1showsthegraphicalrepresentationofstegnography.

Figure1.GraphicalRepresentationofStegnography

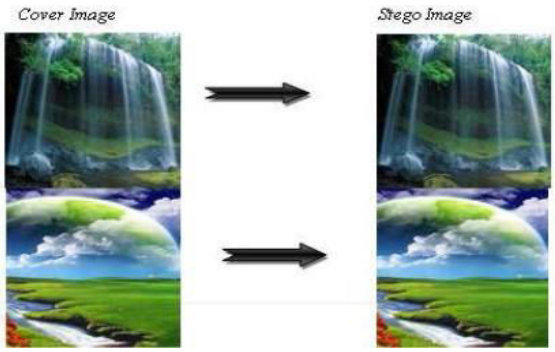


Figure 2. Results of Cover Image and Stego Image (after Hiding theDatabehindtheCoverImage

3.3 Stegnalysis

Stegnography basically exploits human perception, ashuman senses are not trained to look for files that haveinformationinsidethem.Theartofdetectingstegnographyisreferredtoassteganalysis.Stegn

ography have made rapid advances over the yearsandsohavesteganalysis.Stegnography(andSteganalysis)isneither inherentlygoodnorevil;it isthemannerinwhichitisusedwhichwilldeterminewhetherit is benefit or detriment to our society. The number ofattacksusedbythesteganalystfordetectinghiddeninformationshas been only multiplied over the years.Thetypesofattacksusedbythesteganalystsarefollowing.

1. Stegoonlyattack
2. Chosenstegoattack
3. Knowncoverattack
4. Knownstegoattack

Varioustoolsfordetectingstegnographyareeasilyavailable over the internet. Various tools like StegdetectandXstegarefreelyavailableovertheinternetfor detecting stegnography. By performing Steganalysis onthe image the attacker will only get the cipher text andhe will have to perform Cryptanalysis to get back theoriginaltext.

3.4 QuantumCryptography

Public key cryptosystems such as RSA and DEFFIE-HELMANarestillconsideredtobesecureforkeydistribution. They have undergone over lots of publicscrutiny over the years. The power of these algorithmsarebasedonthefactthatthereisnoknownmathematical operation for quickly factoring very largenumbers given today's computer processing power. Thepublic cryptosystem hasbeen workingvery welloverthe years but in the recent years it has been exposed to ahandfulofrisks.FirstlyacomputerscientistattheIndianInstituteofTechnology,ManindraAgarwalsolved aproblem, how to tell if a number isprime,without performing any factoring, solving this problemmay open the door for mathematician to figure out howto factor large numbers. Secondly, the advancements incomputerprocessingwillbeabletodefeatthesecryptosystems in timely fashion thus making the publickeycryptosystemsobsolescentinstantly.SoherewehaveusedquantumcryptographyforexchangingthekeysefficientIy.Atthistime,transmissionspeedandhardwareexpenseshavegenerallylimitedtheuseofquantumdevicestodistributethekeysratherthantheentiremessage.Classicalmethodsofinformationsecurityusingencryptiondecryptionorotherwiseareknowntobesecurebutnot100percent.Increasingcomputationpowers helps hackers to crack down the security cover.Quantumlevelisonewhichbehavessomewhatdifferently than classical ones. Classical methods cannevergive100%securityforexampleevenstrongencryption like DES, AES are prone to be broken asmucheffectiveworkhasbeendonetobreakthese.Dealingthingsatquantum levelwilldefinitelygiveperfect security because of the behavior of microscopicparticles.Assuming laws of Quantum mechanics is true, whichfollowHeisenberg's uncertainty principle andphotonpolarizationwe

canprovide100%security.

3.4.1 WhyQuantumCryptography

Ratherthandependingonthecomplexityoffactoringlargenumbers,quantumcryptographyisbased onthefundamentalandunchangingprinciplesofquantummechanics. In fact, quantum cryptography rests on twopillarsof20thcenturyquantummechanics– theHeisenbergUncertaintyprincipleandtheprincipleofphotonpolarization.Heisenberg'suncerta intyprinciplesaysthatifyoumeasure onething,you can notmeasureanotherthingaccurately.Forexample,ifyoumeasure the position of an electron flying around an atom, youcannotaccuratelymeasureitsvelocity.Itcanberepresentedusingthisequation.AccordingtheH eisenberg Uncertainty principle, it is not possible tomeasurethequantumstateofanysystemwithoutdisturbingthatsystem.Thus,thepolarizationofa photon or light particle can only be known at the pointwhen it is measured. This principle plays a critical roleinthwartingtheattemptsofeavesdroppersinacryptosystembasedonquantumcryptography.Se condly,thephotonpolarization principledescribeshowlightphotonscanbeorientedorpolarizedinspecific directions. Moreover, a polarized photon canonlybe detectedbyaphotonfilterwiththe correctpolarization or else the photon may be destroyed. It isHeisenberg's uncertainty principle that makes quantumcryptographyanattractiveoptionforensuringtheprivacyofdataanddefeatingeavesdropp ers.

3.5 KeyGeneration

Quantumpropertyoflightisusedtogeneratekey.Individualphotonsarecompletelypolarized.Their polarizationstatecanbelinearorcircular,oritcanbeelliptical, which is anywhere in between of linear andcircularpolarization

3.6 SecuringKeyDistribution

Itistheone–way-nessofphotonsalongwiththeHeisenberg uncertainty principle thatmakes quantumcryptographyanattractiveoptionforensuringtheprivacyofdataanddefeatingeavesdropp er.Therepresentation of bits through polarized photons is thefoundation of quantum cryptography that serves as theunderlying principle of quantum key distribution. Thus,whilethe strengthof moderndigitalcryptography isdependent on the computational difficulty of factoringlargenumbers,quantumcryptographyiscompletelydependentontherulesofphysicsandi salsoindependentoftheprocessingpowerofcurrentcomputing systems. Since the principle of physics willalways holdtrue,quantum cryptographyprovidesananswertotheuncertaintyproblemthatcurrentcryptography suffers from; it is no longer necessary tomakeassumptionsaboutthecomputingpowerofmalicious attackers or the development of a theorem toquicklysolvethelargeinteger

factorizationproblem.

Keys can be distributed using quantum cryptography inthe following manner. The sender will send the messagetothereceiverusingaphotongun.Thestreamofphotonswillbeinoneofthefourpolarizationthatcorrespondstovertical,horizontalordiagonalinoppositedirections(0,45,90.135degree). Atthereceiver's end the receiver will randomly choose a filterand count and measure the correct photon polarization.Now, receiver will communicate with sender (out-of-band)abouttheir correctmeasurement(without sending actualmeasurementvalues.Thephotonsthatwereincorrectly measured will be discarded and the correctlymeasured photons will be translated into bits based ontheirpolarization.Now,senderandreceiverwillgenerate one time pad combining their results. This one-time pad will be used in one time information exchangebetween them. None of them can know the actual key inadvance because the key is the product of both theirrandomchoices.

Now, if an attacker tries to eavesdrop, he must select thecorrect filter otherwise the photon will get destroyed.Even if attacker is able to successfully eavesdrop, theinformation which he will get will be of little use unlesshe has the knowledge of correct polarization of eachparticular photon. As a result attacker will not correctlyinterpret meaningful keys and thus be thwarted in hisendeavors.

3.7 Security

Thedatawhichhastobesecuredhereiswrappedaround number of security layers. If the attacker getsaccess to the stego image file in which the message isembedded. Atfirsthewillhavetoperformteganalysistofind out that this message contains a message or not.Even if after performing steganalysis he finds out thatimage contains some data, he will have to apply thesamealgorithmtoretrievetheembeddedfile.Unfortunately,ifhefindsoutthealgorithmbywhichthetextshavebeenembeddedintothemedium,hecouldgetback only the cipher text file. The encryption algorithmwhich we have used here is AES, which is one of themostsecureencryptionalgorithmusedtoday.Thisprovidesan extralayerofsecurity.

Now the hacker is left with only one choice to extracttheembeddedfileandthatistocompromisetheencryptionkeyusedsomehow.Sincemoderncryptographyisvulnerabletobothtechnologicalprogressofcomputingpowerandevolutionin mathematics,thereis uncertainty thatDeffie-Helmanand RSA will be secure for key distribution in future ornot. Here we would like to propose a new model. Thismodel could be easily applied on the web for makingdatamoresecure.

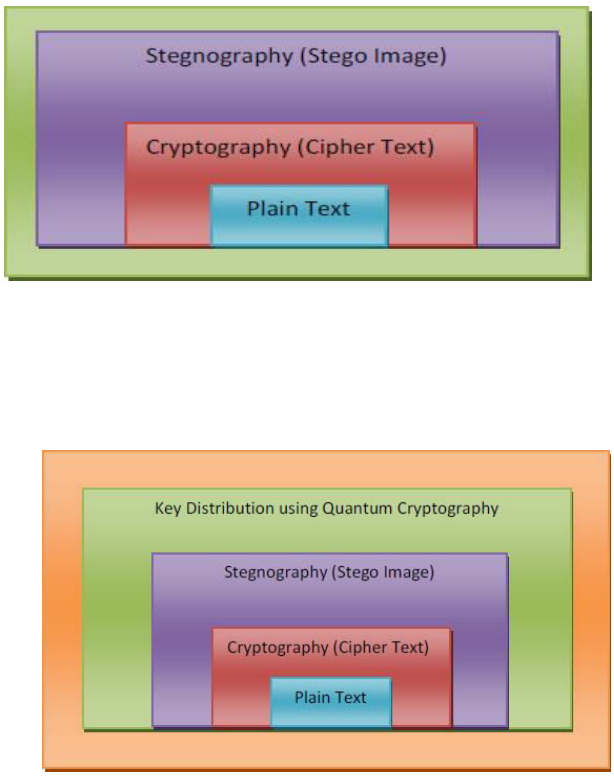


Figure 4. The proposed model of Stegnography with Key DistributionusingQuantumCryptography

Mainideabehindthismodelistousequantumcryptographyforsecuringkeydistributionthusproviding our data another layer of security. This waywecanprovide perfectsecuritytodataovertheinternet.

4. FutureWork

At present quantum cryptography is used in very smallarea,theuseofquantumcryptographyshouldbeencouragedanditshouldbeusedinwideareaofapplicationsbesidethat,maximumguaranteedtransmission distance between remote parties is very lessatpresent.As,opticalfibersarenotperfectlytransparent,a photonwillattimes getabsorbed andthereforenotreachtheendofthefiber.Although,quantumcryptographyissecurebutinformationretrievedisveryless(duetoloss).Itshouldbeimproved. Another problem that needs to be addressedinfutureisifanattackertriestotamperwiththemessagewholemessagegetsdestroyed.Itis anicefeature of quantum cryptography that no one can tamperwith the message but at the same time due to this thereceiver is also suffering because correct message wasnot delivered to the recipient, and now the sender willhave to resend the message either from the same path orhe willhavetochooseadifferentpath.

5. Conclusion

Securing the key distribution is as important as securingthedataitself.Inthispaperwehavemadeuseofquantum cryptography thusimproving

thesecurity ofthe keys and providing our data a perfect security. Theuse of quantum cryptography has added another layer ofdefensetoourdata.Evenifweusemostsecureencryption algorithm and best stego technique to hideour data, if the keys gets compromised these securitywillbeofnouse.Quantumcryptographyaddressescurrent as well as emerging threats and it definitely has“competitiveadvantage”overotherpublickeycryptosystems.Wehaveusedquantumcrypto graphyonly for key distribution rather than for entire messagesbecauseoflimitationsoftransmissionspeedsandhardware expenses. The representation of bits throughpolarizedphotonisthefoundationofquantum cryptography that serves as the underlying principle ofquantum key distribution. This paper concentrates ontheory of quantum cryptography and the use of quantumcryptography for key distribution and how the use ofquantumcryptographycontributestothefieldofstegnography. In this paper we have shown that usingquantummechanicsandphotonpolarizationwecanprovideperfectsecurity.

References

[1] Manindra Agrawal, NeerajKayal, and NitinSaxena(2004).PrimesisinP.AnnalsofMathematics,160,781-793.doi:10.4007/annals.2004.160.781

[2] Imran SarwarBajwa and RubataRaisat (2011). ANewPerfectHashingbasedApproach forSecureStegnograph.DigitalInformationManagement(ICDIM),174-178.doi:10.1109/ICDIM.2011.6093325

[3] Muhammad Asad, JunaidGilani and Adnan Khalid(2011).AnEnhancedLeastSignificantBitModificationTechniqueforAudioSteganographyComputerNetworksandInformationTechnology(ICCNIT), 143-147. doi:10.1109/ICCNIT.2011.6020921

[4] Mohammad Hamdaqa and LadanTahvildari (2011).ReLACK:AReliableVoIPSteganographyApproach.Fifth International Conference on Secure SoftwareIntegrationandReliabilityImprovement,189-197.doi: 10.1109/SSIRI.2011.24

[5] S. Changder, N.C. Debnath and D.Ghosh (2011). AGreedyApproachtoTextSteganographyusingPropertiesofSentences.EighthInternationalConferenceonInformationTechnology:NewGenerations, 30-35.doi:10.1109/ITNG.2011.13

[6] PiyushMarwahaandPareshMarwaha(2010).VISUAL CRYPTOGRAPHIC STEGANOGRAPHYINIMAGES.SecondInternationalconferenceonComputing,CommunicationandNetworkingTechnologies,1-6. doi:10.1109/ICCCNT.2010.5591730

[7] JinsukBaek, CheonshikKim,PaulS.Fisher andHongyangChao(2010).(N.1)SecretSharingApproachBasedonSteganographywithGrayDigitalImages.IEEEConferenceonWirelessCommunications,NetworkingandInformationSecurity (WCNIS) ,325-

329.doi:10.1109/WCINS.2010.5541793

[8] FerruccioPisanello, Luigi Martiradonna, PiernicolaSpinicelli,AngelaFioreandJean-PierreHermier(2009).PolarizedSinglePhotonEmissionforQuantumCryptographyBasedonColloidalNanocrystals.11th international conference on Transparent OpticalNetworks,1-4.doi:10.1109/ICTON.2009.5185131

[9] VladimirL.KurochkinandIgorG.Neizvestny(2009).QuantumCryptography.10thINTERNATIONALCONFERENCE AND SEMINAR EDM'2009, 166-170.doi: 10.1109/EDM.2009.5173960