ROLE OF CRYPTOGRAPHY AND STEGANOGRAPHY IN SECURING DIGITAL INFORMATION: A REVIEW

Challa AksharaSree
MtechStudent,Dept. of IT
Sreenidhi Institute of Science and Technology

Dr. B. Indira Reddy
Professor,Dept. of IT
Sreenidhi Institute of Science and Technology

Abstract-Digital communication has lot of significance in human life now a days and it is important for communication to be made secret. Today, many applications are internet based and people are relying on social networking sites like facebook,twitter etc. The information is distributed through insecure channels and needs to be protected from unauthorised access and use. Cryptography and steganography are two popular methods used for data protection. The cryptography distorts the data and steganography hides the existence of data. Alone approach of any of these techniques may cause some vulnerabilities.But, cryptography combined with steganography has high standards of securing information. This paper focuses on combination of cryptography and steganography to provide high security for the communication through insecure channels.

Keywords: Cryptography, Steganography, hiding information,Security.

I. INTRODUCTION

The cryptography and steganography are two extensively used techniques for concealment of data exchange. Cryptography is used to cipher information and steganography is used to hide the reality of data communication. Cryptography scrambles the information by using a key so that a third party cannot access the information without the key.Cryptography is also called as the science of secret script. Steganography hides the information by using a cover medium so that a third person cannot identify the communicationSteganography is also called art and science of writing hidden messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message.[5]Consider any situation wherein a person A, has to send a secret message or some confidential information to another party C through unsecured channels. In this case, it becomes essential to realize the following for secure data transmission:

1. Data Integrity: C should receive the exact message sent by A, it should not be tampered or modified during the transmission.

2. Data Confidentiality: The message should only be received by C and interpretable by C.

3. Authentication: The receiver C should be able to authenticate the sender A and verify that the message has been sent by the desired source.

4. Non-repudiation: The source A should not be in a position to deny the sending of the message.

To satisfy the above security services various techniques have been implemented.

Cryptography is the study of mathematical techniques related to characteristics of information security such as confidentiality, authentication, integrity and non-repudiation. The aim of cryptography is to make data unreadable by a third party. Cryptography algorithms are divided into symmetric and asymmetric algorithms. Symmetric algorithms are used to encrypt and decrypt original messages by using the same key. Asymmetric algorithms use public-key cryptosystem to exchange key and then use secret key algorithms to ensure secrecy of data. In Public-key encryption algorithms, one key is known to the public, and is used to

encrypt information and is sent to receiver who owns the corresponding private key, which is used to decrypt information [5].

Steganography is the scientific approach of introducing the secret data within a cover media so that the unauthorized viewers do not have knowledge of any information hidden in it. Steganography is an alternative to cryptography in which the secret data is fixed into the carrier in such a way that only carrier is visible which is sent from sender to receiver without clambering. Individually cryptography and steganography offersprivacy to the data but they have some vulnerability. So we can go for a combination of cryptography and steganography. There are various kinds of cryptographic and steganography techniques offered thus we can have different combinations of cryptography and steganography [5].

The rest of this paper is organized as follows. Section **II** discussedCryptographic techniques. In section**III**, We statedSteganographic techniques. Combined cryptography and steganography techniquesin section **IV**.Related work in literature of combining Section **V**. We also present a conclusion of our work in Section **V**.

II. CRYPTOGRAPHIC TECHNIQUES

A. DES algorithm

Data Encryption Standard (DES) is a standard for the encryption of electronic data. It is a symmetrickey algorithm invented in the early 1970 at IBM. DES encrypts 64 bitplain text using a 56-bit key which is too small, and so considered to be insecure.[1,7,24]

B. RSA algorithm

RSA is one of the public-key cryptosystems and is widely used for securing data transmission. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. In this encryption key is public and decryption key is private, which is kept secret. RSA is based on factorizing two large prime numbers.[6,9,14,16]

C. AES algorithm

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. It was described by U.S. governmentin 1997. AES is a symmetric-key algorithm which means that the same key is used by sender and receiver. This AES standard specifies the Rijndaelalgorithm, a symmetric block cipher that can process data blocks of 128 bits, using key size of 128, 192, and 256 bits [8,12].

The other cryptographic techniques used areDiffie-Hellman, Elliptic curve cryptography, Digital signature standard and RC4 algorithm.

III.STEGANOGRAPHIC TECHNIQUES

The historical techniques include

- Character marking
- Invisible ink
- Pin punctures
- Typewriter correction ribbon

The recent techniques include

LSB –Steganography.

In Least Significant Bit (LSB) steganography text message is embedded in least significant bits of digital picture. Data is embedded by replacing the LSB of cover carrier with the data to be send.ie first read the cover image and text message which is to be hidden in the cover image, then convert text message in binary.

Calculate LSB of each pixels of cover image. Replace LSB of cover image with each bit of secret message so we get an image in which data is hidden.[4,6,15,19,20]

DCT - Steganography

The hidden message converted into binary stream of "1" and "0" are inserted the into the DCT domain of the cover image. The color-based transformation converts the cover image into 8x8 blocks of pixels. DCT can divide the image into high, middle and low frequency components. As the high frequency coefficients are vulnerable and less robust on the quality of image,the low and mid frequency coefficients are the most appropriate. Quantity K represents the persistence factor.Iftheith term of message bit is "1", the coefficient of the image is added with a quantity K, otherwise the same quantity is subtracted from it[2,19,20,22,24].

DWT-Steganography

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. This is one of the frequency domains in which steganography can be implemented. DWT splits component into numerous frequency bands called sub bands known as LL – Horizontally and vertically low pass, LH – Horizontally low pass and vertically high pass, HL - Horizontally high pass and vertically low pass, HH - Horizontally and vertically high pass. Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band [19,22,23].

IV.COMBINED CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

Basic combination

The information or data from the sender is taken as the plain text. Then the plain text is converted into cipher text using any encryption method. The transformed cipher text can be used as the input for steganography. The key of cryptography is kept secret. Then the cipher text is embedded into the cover medium using steganography techniques. The cover image is transmitted to the receiver. This is a direct approach in which both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography [5].

i. DES with LSB Steganography

DES algorithm is used to encrypt the data to be transferred then the encrypted information i.e. cipher text is hidden within a cover carrier. Here an image can be used as the cover carrier. The embedding process is performed using LSB steganography.[1]

ii. AES with LSB Steganography

AES algorithm is used to encrypt the data to be transferred then cipher text is embedded into a cover carrier. Here 24 bit image can be used as cover carrier. The embedding process is performed using LSB steganography. For each 8 bit data, the first three bits of the data are replaced by the three least significant bits of the red byte, the second three data bits are replaced by the three least significant bits of the green byte, the last two data bits are replaced by the two least significant bits of the blue byte. Then the image is transmitted to the receiver [13,18].

iii. AES with DCT-Steganography

AES algorithm is used to encrypt the data, the cipher text is generated from the plain text using AES encryption. The cipher text then embedded into the cover image using DCT based steganography in which a DCT transformation is applied on the cover image so the image get divided into high, middle and low frequency components. As the high frequency coefficients are vulnerable and less robust on the quality of image, we can use the low and mid frequency coefficients [2].

iv. AES with DWT-steganography

AES algorithm is used to encrypt the data, the cipher text is generated from the plain text using AES encryption. The cipher text then embedded into the cover image using DWT based steganography in which a DWT transformation is applied on the cover image so the image get divided into four sub bands, Since Human eyes are much more sensitive to the low frequency part we can hide secret message in high frequency part without making any alteration in low frequency sub band. DWT steganography can hold more data without distortion to the cover image [5].

V. Background work

R.Nivedhitha andDr.T.Meyyappan[1] introduced two new methods where cryptography and steganography are combined to encrypt the data as well as to hide the data in another medium through image processing. DES algorithm is used to encrypt secret image and LSB technique is used to hide the encrypted secret image into cover image. This proposed technique is effective for secret communication and it is hardly attracted from eavesdropper.DiptiKapoorSarmah and NehaBajpai[2] developed a system using AES algorithm to encrypt the message and the message is hidden in DCT of an image. When the combination is used, it enables the people to communicate without possible eavesdroppers even knowing that the communication is taking place.

Md. Khalid Imam Rahmani, KamiyaArora and Naina Pal[3]proposed that cryptography and steganography lacks security in some or the other way if they are used individually.so they have proposed a new method called crypto-steganography to increase security and fulfil the basic requirements of security like robustness, undetectability and capacity etc.Nikhil Pate and ShwetaMeena[4] proposed a system where least significant bits of carrier image are replaced by most significant bits of secret image. Security is provided by dynamic key cryptography. If any eavesdropper makes analysis only cipher text is obtained. Here 4 LSB of carrier image is replaced by 4 MSB of every pixels of secret image. LSB based steganography is a new method which is used for image hiding along with cryptography method.

Varsha and Dr.Rajendra Singh Chhillar[6] discussed a technique used on the advanced LSB and RSA algorithm .By matching data into the image, there is a less chance of an attacker being able to use steganalysis to recover data. An efficient steganographic method for embedding secret message into cover images has been accomplished through LSB method. It also applies a cryptographic method, RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key.DeepaliBhat, Krithi V, Manjunath KN, SrikanthPrabhu and RenukaA[7]proposed a method of dynamic text steganography with cryptography.The methodology was built on the result of DES-symmetric key algorithm and data hiding is done through text steganography. As more number of people are tending towards use of mobile applications, E-mail, utility of internet, the combination of both provides an efficient solution for information hiding through unsecured channels.

Marwa E. Saleh and Abdelmgeid A. AlyFatma A. Omara[8] proposed that if cryptography is used there is a chance for the attacker to interrupt the transmission and if steganography is used the message is become known once the presence of information is revealed.so here AES algorithm is used to encrypt the secret message and the message is hidden using image steganography.AnkitGambhir and SibaramKhara[9] proposed a technique that provides multilayer security by integrating cryptography and steganography. As people are committing e-transactions like online shopping,money transfer etc.These two methods are used for secure transmission.

M.Saritha,Sushravya and M,Vishwanath.M.Khadabadi[10] developed a high secured model. Sequential algorithm is used for steganography and symmetric XOR algorithm is used for cryptography. In this method, the software will help to reduce manual effort and time. It also provides security. It is user-friendly. It can also be applied to video or video files.Lipi Kothari, RikinThakkar and satvikkhara[11]gives correspondence through information hiding on internet.Web is not only space for information it is a tool to connect people. People share confidential data on web.so, steganography and cryptography can be used to

hide the data from unauthorised user.This proposed method has high security,larger embedding capacity and best imperceptibility than others.

Sajisha K S and Dr.SheenaMathew[12]proposed that DNA(deoxyribonucleicacid)is explored as new carrier for data security since it achieves maximum protection,powerful security with high capacity and low modification rate. Here the secret message is first encoded to DNA bases then DNA based AES algorithm is applied to it.Finally encrypted DNA will be concealed in another DNA sequence. DNA based encryption and steganography method is the recent technique embedded into cryptographic field. The proposed method can be modified by introducing various encryption techniques like Blowfish, Twofish, Triple DES etc.

SofyaneLadghamChikouche and NoureddineChikouche[13]proposed a LSB technique in which the bits of the message are put in LSB in each pixel of the image.The length of the hidden message is reduced by the deflate algorithm which is a lossless data compression algorithm that combines the LZ77 algorithm and Huffmannalgorithm.The reduced hidden data is protected by AES algorithm. Here AES algorithm with size key 256 which is the strongest symmetric algorithm and is very fast.Kripa N Bangera,YashikaPaddambail,Dr.N.V.Subbareddy and Shivaprasad G[14]proposed a technique by integrating RSA cryptographic algorithm with dual audio steganographic algorithm .This algorithm combines the features of RSA cryptography and two rounds of audio steganography to provide a higher level of security. This is used by all academic institutions, business and government organisations to process their data.

Radha S Phadte and Rachel Dhanaraj[15]proposed that LSB based method is used to hide an image into another image.Thestego image is then encrypted using chaotic theory.This method ensures the high security of secret image as it is split into two parts and embedded into two different cover images.The two images are sent separately over the network.If the intruder intercepts one image and tries to extract the data,they are able to now the data only partially.It ensures lossless transmission of data the receiver end.It provides security at three different levels:steganography ,cryptography and transmission by splitting. B.Sivaranjani and Dr.N.Radha[16]developed a technique which is used to enhance the security of patients medical data. During the transmission, the data is concealed with ECG signal.The ECG signal of the human being vary from person to person. Here ECG signal is used as host signal.RSA algorithm is used to encrypt the patient information with the help of key pairs. Arnold catmap technique is used to scramble the encrypted data for more security of information. Singular Value Decomposition (SVD) is used for effective transformation with high security. These proposed methods perform well in hiding patient data. It not only reduces the transport cost but also the increasing traffic at hospitals and medical centre.

Taranpreet Singh Ruprah, Vishal S Kore and Yogesh K Mali[17]proposed that a variety of algorithms like AES,DES,RSA are used to achieve the confidentiality in the data. In this ECC technique is used for sending the encrypted message from one android smart phone to another. The quick development of advanced mobile phones and getting to different types of touchy substance has prompted to the rise of risks. This proposed system will help us to transfer the text messages in very secure manner. In future, this can be extended to secure multimedia files, banking applications where data contains transaction details, military data transfer applications, secure banking related message.MoshiraA.Ibrahim and Islam A.M EI-Maddah,HodaK.Mohmed[18]discussed that cloud computing integrates huge resources and presents flexible service to users. It has some problems like data security which is a critical factor in cloud environment. In this paper, the author had proposed a security model to protect cloud data from unauthorised access using cryptography and steganography. The model combines the features of cryptographic and steganographic techniques.AES-256 is applied for data encryption and advanced LSB algorithm is also applied for data hiding. This proposed system is better compared to other algorithms, which ensure the effectiveness of the model.

G.Prashanti, B.V.Jyothirmai and K.SaiChandana[19] proposed a dual security model. The encrypted message obtained from different encryption methods is hidden in a image based on LSB steganography. We can further use different steganographic techniques like DCT, DWT for different image formats.KunalHossain, Susovan Jana, Saswati Mukherjee and RanjanParekh[20]discussed that digital

representation of biomedical images and videos has grown enormously.Manipulation of sensitive biomedical data in the path of transmission can mislead critical diagnosis and treatment. Multilevel security is provided by applying encryption and steganography techniques to protect biomedical images and videos. DCT andLSB mechanisms are applied to form the stego-image followed by image encryption that increase robustness and hiding technique.This is an effective technique because it becomes quite hard for an intruder to retrieve the original image or video.

BayuAnggorojati and RamjeePrasad[21]stated that IOT allows the information collected by smart devices to be transmitted to the people across the globe through internet and enhancing the people lives in many aspects such as health, energy, transportation etc. IOT is vulnerable to threats like tampering of information and key distribution issue. Proposed method is to secure communication that manages trust of IOT in federated fashion while minimising usage of resources in IOT devices. Ensuring security in network that consists of constrained devices such as IOT, is a challenging task. It is even more challenging when the communicating entities are located across different network domains with different trust authority. A scheme based on IBC has been proposed to secure Inter domain communication in IOT.

Vinita V. Korgaonkar and NaikGaonkar[22]discussed that the technique of hiding the secret data in other multimedia is steganography. Video steganography is considered to be more powerful type of steganography since data hiding capacity is more and processinga video is very complex.They have presented a novel approach of hiding text data within a video. This approach combines a DCT and DWT technique of hiding information together to get high capacity of hiding ratio.

NishantMadhukarSurse and PreetidaVinayakrayJani[23]proposed the use of DWT along with different transforms and algorithms in image steganography and how it helps in achieving the security for the information hidden in the cover image. We can use other transforms and algorithms in DWT domain for increasing the imperceptibility and capacity of image steganography and making it more secure and robust.AchmadSolichin and Erwin WahyuRamadhan[24]proposed the combination of cryptographic method and DES algorithm and steganographic method with DCT to develop a digital data security application. The application can be used to secure document data in word, excel, powerpoint or PDF format. Data is encrypted with DES algorithm and further hidden in image cover using DCT algorithm. The combination of DES cryptographic and DCT steganographic methods proved to improve data security because it has two levels of security.

VI. CONCLUSION

The intensive growth of modern communication desires a distinctive means of security particularly on computer network. As there appears a risk that the delicate information transferred might be interrupted or misleading by unintentional observers for the openness of the internet. So there is an explosive growth in secure communication and information hiding. Additionally, the information hiding technique can be used widely in applications like military, business, anti-criminal,commercials and so on. Both cryptography and steganography methods provide security in their own means, but to add multiple layers of security combination of these techniques can be a better contribution. In this paper, concepts of cryptography steganography, and their applications in securing the digital data across network is studied and survey of moderntechniques which combined steganography and cryptography is presented.

References

[1]R.Nivedhitha, Dr.T.Meyyappan"Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.
[2]DiptiKapoorSarmah ,NehaBajpai "Proposed System for data hiding using Cryptography and Steganography", 2013.
[3]Md. Khalid Imam Rahmani ,KamiyaArora , Naina Pal,"A Crypto-Steganography Survey", International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014.
[4] Nikhil Patel, ShwetaMeena "LSB Based Image Steganography Using Dynamic Key Cryptography", in 2014.
[5]Vishnu S Babu , Prof. Helen K J "A Study on Combined Cryptography and Steganography", in 2015.

[6]Varsha,Dr.Rajendra Singh Chhillar,"Data Hiding using Steganography and Cryptography"International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 802-805.
[7]DeepaliBhat ,Krithi V, ManjunathKN, SrikanthPrabhu, Renuka A, "Information Hiding through Dynamic Text Steganography and Cryptography"in 2015.
[8]Marwa E. Saleh, Abdelmgeid A. Aly , Fatma A. Omara "Data Security Using Cryptography and Steganography Techniques",International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.
[9]AnkitGambhir, SibaramKhara,"Integrating RSA Cryptography & Audio Steganography" International Conference on Computing, Communication and Automation (ICCCA2016).
[10]M.Saritha ,Sushravya.M ,Vishwanath.M.Khadabad, "Image and Text Steganography with Cryptography using MATLAB", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.
[11]Lipi Kothari, RikinThakkar, SatvikKhara, "Data hiding on web using combination of Steganography and Cryptography"International Conference on Computer, Communications and ElectronicsManipal University Jaipur,2017.
[12]Sajisha K S, Dr. Sheena Mathew,"An Encryption based on DNA cryptography and Steganography", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.
[13]SofyaneLadghamChikouche, NoureddineChikouche ,"An Improved Approach for LSB-Based Image Steganography using AES Algorithm",The 5th International Conference on Electrical Engineering – Boumerdes (ICEE-B) October 29-31, 2017, Boumerdes, Algeria.
[14]Kripa N Bangera ,YashikaPaddambail, Dr.N.V. Subba Reddy, Shivaprasad,"Multilayer Security Using RSA Cryptography and Dual Audio Steganography", 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.
[15]Radha S. Phadte, Rachel Dhanaraj,"Enhanced Blend of Image Steganography and Cryptography",International Conference on Computing Methodologies and Communication (ICCMC)in 2017.
[16]B.Sivaranjani, Dr.N.Radha ,"Securing Patient's Confidiential Information using ECG Steganography"2nd International Conference on Communication and Electronics Systems (ICCES 2017).
[17]Taranpreet Singh Ruprah, Vishal S Kore, YogeshKMali,AshtaSangli "Secure Data Transfer in Android using Elliptical Curve Cryptography", in 2017.
[18]MoshiraA.Ibrahim,Islam A.M EI- Maddah,HodaK.Mohmed,"Hybrid Model for Cloud Data Security using Steganography", in 2017.
[19]G.Prashanti,B.V.Jyothirmai, K.SaiChandana,"Data Confidentiality Using Steganography and Cryptographic Techniques"International Conference on circuits Power and Computing Technologies [ICCPCT], in 2017.
[20]KunalHossain, Susovan Jana, Saswati Mukherjee, Ranjan Parekh, "A Novel Approach to Secure Biomedical Images and Videos for Transmission",3rd International Conference on research in computational intelligence and communication networks 2017.
[21]BayuAnggorojati, RamjeePrasad,"Securing Communication in Inter Domains Internet of Things using Identity-based Cryptography" in 2017.
[22]Vinita V. KorgaonkarManishaNaikGaonkar,"A DWT-DCT Combined Approach for Video Steganography"2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.
[23]NishantMadhukarSurse and PreetidaVinayakray-JaniSardarPatel,"A Comparative Study on Recent Image Steganography Techniques Based on DWT "IEEE WiSPNET 2017 conference.
[24]AchmadSolichin, Erwin WahyuRamadhan, "Enhancing Data Security Using DES-based Cryptography and DCT-based Steganography"3rd International Conference on Science in Information Technology (ICSITech), 2017.