JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

TYPICAL ANALYSIS OF CRYPTOGRAPHY AND STEGANOGRAPHY IN DIVERSITY OF APPLICATIONS

[1]Balireddi Durga Anuja, [2]A.Sumathi, [3]Nagireddi Surya Kala
[1]Lecturer in Computer Applications, [2] Lecturer in Computer Science, [3]Assistant professor in CSE
[1]Department of Computer Applications, [2] Department of Computer Science, [3] Department of CSE
Govt. Degree College for Women, Srikalahasti, India

Abstract: In present techno commercial era the world bind with e-commerce and e-communication. Every application is internet based thus each bit of information that flow in the network need to be confidential and secure. In this perspective Network Security take a key role in network communication .To provide secure communication conventionally used techniques are Cryptography and Steganography.. this paper cope up with models of cryptography and Steganography along with analysis on various cryptographic and Steganography schemes used. It carries out analysis of traditional Steganography techniques with HSS method.

Index Terms- **Cryptography, Steganography, Information Security, Hexa Symbol Steganography.**

I.INTRODUCTION

Nowadays rapid growth of technologies over network makes extensive data to cross over the internet results in concerning about sensitivity of data and security of data to persist confidentiality, availability and integrity [1].

To provide confidentiality and integrity to the messages over network need of information security methodologies. One of the key approaches is hiding information. The most popularly used methods to infract the menace to security are Cryptography and Steganography [1].

II.MODEL AND APPLICATIONS:

Cryptography and Steganography

Cryptography:

Cryptography is a procedure which is deliberately used to transform data and assures Secrecy, integrity of data, validation, authorization and non-repudiation like security aspects [2].The techniques consists of an algorithm and a key. These algorithms are a numerical procedure that encrypts messages with key.

Cryptography Model:

Cryptography is a process or algorithmic approach that transfer data in a secure channel by transforming readable message to irrational or cryptic form so that intended receiver can read the message[15][16].

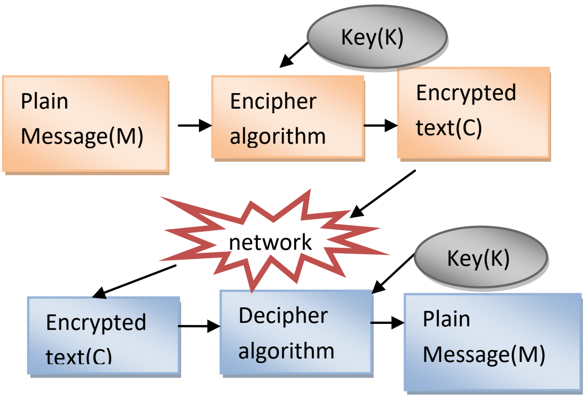


Figure1: Cryptography Process Model [2]

Applications of Cryptography:

1. Digital Signatures(DS) and Authentication
2. Time Stamping
3. E-money Transfer
4. In Secure Network Communications
5. Unidentified Remailers
6. Encryption of Disk etc,
7.

III.CRYPTOGRAPHIC ENCRYPTION SCHEMES

Cryptographic algorithms can be symmetric and asymmetric. In symmetric for encryption and decryption same key is used by both sender and receiver where as in asymmetric method two different keys are used by communication parties. These asymmetric algorithms called as public key algorithms generally used for privacy of data. The Keys used in public key cryptography i.e public key and private key both are related to each other and generated by some key generation algorithms. The key management must be done between communication entities either physically or by trusted third party.

On basis of time and space complexity The Comparison analysis of algorithm will be performed [4].the security of techniques depends on strength of algorithm which contains basic parameters as generation of key, length of key, message block size ,number of rounds in algorithm, encipher and decipher process[6].

Single Key Encryption (Symmetric key Encryption)

i) DES(Data Encryption Standard)
64-bit block of data with 56-bit key-size uses for encryption process in this algorithm.
ii) Triple DES:
It is advancement to DES that uses 64-bit block size along with 192 bit key size for encryption process. It increases encryption level to 3 times.
iii) AES
Advanced encryption standard is a block cipher algorithm. It includes variable key size 128,192, or 256 bit. Default key size 256 bit. it encrypts 128-bit block in 10,12 and 14rounds based on key size [8].AES has tested for many security applications[11].
iv) BLOWFISH
Blowfish is one of the conventional key encryption that includes 64 bit block size and variable length key size from 32 bits to 448 bits. Compromise of this algorithm is tricky because of its large key size.
v) RC4
It is most widely used stream cipher in cryptography. XOR operation between data stream and series of keys generated.

Asymmetric Key Encryption:

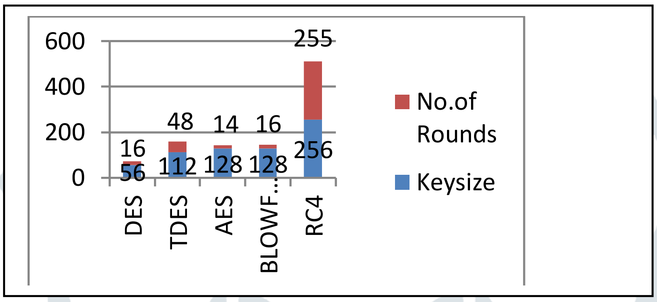
i) RSA:
Rivest-Shamir-Adlemen is the most generally used two key cryptography method. It includes exchange of secret keys to send cryptic message without a separate key sharing. RSA operates with two large prime numbers.
ii) Diffie-Hellman
This key exchange algorithm allows both the sender and receiver to jointly establish a shared secret key. This key can be used to encrypt further communication. With usage of optimized mathematical group this algorithm is considered to be secure [9].

Selection of optimal cryptographic technique for application relies on time, memory, security, nature of data to be protected, type of data i.e whether it is text or image or video[7].

IV.COMPARATIVE STUDY OF CRYPTOGRAPHIC ALGORITHM BASED ON PARAMETERS: In existing cryptographic algorithms DES,AES,3DES,BLOWFISH and RC4 are briefed for comparison. The Comparison parameter is structure of algorithms.[10][7]

Algorithm	**Structure**	**Blocksize**	**Keysize (bits)**	**No.of Rounds**
DES	Feistel	64	56	16
Triple DES	Feistel	64	112,168	48
AES	Feistel	128	128,192, 256	10,12,14
BLOWFISH	Feistel	64	128-448	16
RC4	Feistel	64	256 bytes	1-255

Table1: Quantitative Measures



Graph1: Comparison on Key size and Rounds

Comparative study based on speed, memory usage, flexibility and level of security parameters [12][14].

Algorithm	**Speed**	**Speed depends on key**	**Memory Usage**	**Flexibility**	**Level of Security**
DES	Slow	Yes	Moderate	Yes	insecure
Triple DES	Very slow	No	Moderate	Yes	Moderate Secure
AES	fast	yes	low	Yes	Secure
BLOWFISH	fast	no	High	Yes	Believe secure
RC4	Very fast	no	low	Yes	Moderately Secure

Table2: Qualitative Measures

In this comprehensive comparative study we also are mentioning known attacks on different cryptographic algorithms.

Algorithm	**Known Attacks**
DES	Brute Force attack
Triple DES	Brute Force, Chosen plain text, known plain text
AES	Side channel attack
BLOWFISH	Dictionary attack
RC4	Brute force attack, Analytical attack

Table3: Known Attacks on Techniques

V.STEGANOGRAPHY

Steganography is a art and method of embedding confidential messages in a cover message so that anyone apart from source and destination entities cannot suspects the existence of the message [15].

Steganography model:

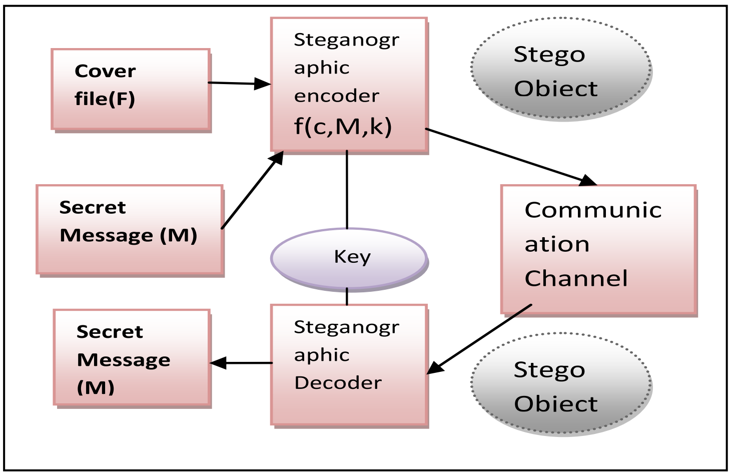


Figure 2: Steganography Process Model [7]

Applications of Steganography:

i) Secret communication and confidential data storing.
ii) Protection from data alteration.
iii) Access control system of digital content distribution.
iv) Media database systems.

Steganography Techniques Classification: The classification mainly focuses on the medium that uses to mask the confidential message.

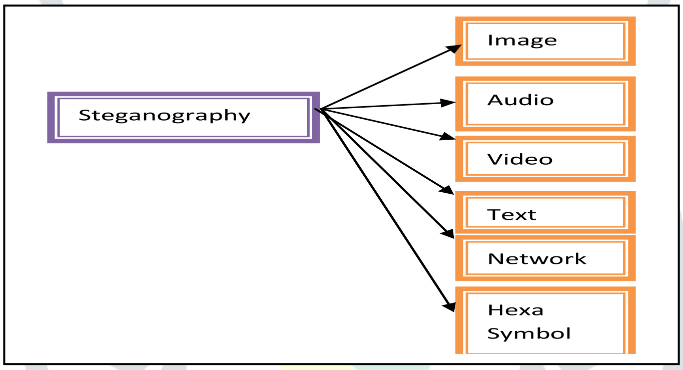


Figure 3: Classification of Steganography [17][18]

Text Steganography:

Hiding confidential information inside the text or text files performs changing of existing content, random character sequence generation or uses context free grammar to make readable texts. Procedures to place the secret data in text are:

- Format Based method
- Random and Statistical Generation
- Linguistic method

Image Steganography:

The usage of Image as Cover object to hide the confidential information is called as image Steganography. Widely used approaches for Image Steganography are:

- Least Significant Bit Insertion (LSB)
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

Audio Steganography:

An audio signal embedded with secret message and that alters binary sequence of corresponding audio file. This is critical process when compared to other techniques. approaches for Audio Steganography are:

- Least Significant Bit Insertion (LSB)
- Parity Encoding
- Phase Encoding
- Spread Spectrum

Video Steganography:

The confidential message can be hide in a digital video format. A large volume of data can be placed inside it is its advantage. This approach can be called as combination of audio and image Steganography.

Two vital classes of Video Steganography

- Place secret data in a uncompressed raw video and compress it later.
- compressed data stream includes secret data directly

Network Steganography:

It is a approach of including confidential information with network control protocols and in data transmission such TCP,UDP ,ICMP etc,. TCP/IP packet header can have this secret information in same folder.

Hexa Symbol Steganography:

It uses hexa symbol carrier files to cover up the private information instead of digital multimedia [18].

VI.COMPARISON OF CONVENTIONAL STEGANOGRAPHY METHODS WITH HSS

In this comparison primary steganographic measures has been considered.

Imperceptibility:

In Traditional Steganography methods(TSM) covered data can be recognized in the form of interference in audio and video files, changes in image frames and colors.

In HSS the secret data will be hidden into hex symbol, so it is critical to identify with human sight.

Capacity:

In TSM limited capacity to embed secret data.
In HSS more capacity to embed secret data.

Robustness:

HSS is more robust in nature when compared to TSM.

Security:

Adequate security by TSM. Excellent Security by HSS.

Code:

Binary codes are used in traditional Steganography methods to conceal data whereas hexa symbol codes are used in HSS.

CONCLUSION

In recent times the e-commerce and e-communications are became crucial in day to day life and at the same time it’s becoming challenge to provide security for these aspects from unauthorized access in networks. In this paper we are presented various cryptography and Steganography methods and analysis of techniques used in both models. we briefed analysis of conventional or traditional Steganography with HSS by using basic stenographic measures so that the above techniques can be used diversity of applications in network security.

REFERENCES

[1]“William Stallings” Network Security Essentials (Applications And Stands), Pearson Education 2004.

[2]William Stallings “Cryptography and Network Security “ Prentice Hall,1995.

[3]“ National Bureau of Standards” “Data Encryption Standard” FIPS publication 1977.

[4]Mandal, A. K. Prakash, C. and Tiwari A(2012) Performance Evaluation of Cryptographic Algorithms DES and AES. Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students Conference on IEEE 2012.

[5]S Almuhamnadi and A Al-Shaaby, “ A Survey on Recent Apporches Combining Cryptography and Steganography”, Computer science and Information Technology(CS&IT),2017.

[6]Nadeem .A And Younus Javed .M(2005). “ A Performance Comparision Of Data Encryption Algorithms.Information And Communication Technology 2005. ICICT 2005.First International Conference On IEEE.

[7]Kritika Acharya, Manista Sajwan, Sanjay Bhargava “ Analysis Of Cryptographic Algorithms For Network Security” IJCATR, Vol.3 ,2014.

[8]Punita Mellu & Sitender Mai “AES: Assymmetric Key Cryptographic System” International Journal Of Information Technology And Knowledge Management, Vol. No 4, 2011.

[9]Zirra Peter Buba & Gregory Maksha Wajiga “ Cryptographic Algorithms For Secure Data Communication” In IJCSS, Vol:5, Issue2.

[10]www.edurekha.com

[11]Daemen J And Rijman V “ Rijindel : The Advanced Encryption Standard” Dr. Dobb’s Journal, 2001.

[12]M Kumar, V Kumar And A Sharma “ A Survey On Various Cryptography Techniques” IJETTCS, Vol:3 Issue 4, 2014.

[13]S. Swathi, P. Lakshmi, B. Thomas “ Encryption Algorithms : A Survey”, Ijarcst, Vol:4, Issue 2, 2016.

[14]Zoran Heraigonja, Durga Gimnazija, Varazdin Croatia “Comparative Analysis Of Cryptographic Algorithms” International Journal Of Digital Technology And Economy Vol 4, Issue 2,2016.

[15]S. Mishra , P Pandey : “ A Review On Steganography Techniques Using Cryptography” Ijarse, Vol. 4, Special Issue (01),2015.

[16]M. Pandey And D.Dubey “ Survey Paper : Cryptography The Art Of Hiding Information”, Ijarcet, Vol 2,Issue 12,2013.

[17]P. Joseph and S. Vishnu Kumar “ A study on Steganographic Techniques”, proceedings of global conference on communication technologies (GCCT), IEEE 2015.

[18]S. Abesh, H. Al-sewadi , S. Hammoudeh and A. Hammoudeh, “ Hexa Symbol algorithm for anti-forensic artifacts on android devices” International Journal of Advanced Computer Science and Applications IJACSA, vol:7, 2016.

[19]Alpha Agath, Chintan Sidpara, Darshan Upadhay “ Critical Analysis Of Cryptography And Steganography” IJSRSET, Vol. 4,Issue 2-2018.