Approaches of Steganography & its Applications

Sumiti Narayan Tewari
Pranveer Singh Institute of Technology, Kanpur

ABSTRACT

Steganography is a science of hiding the presence of data so that it remains safe from intruders. In modern communication scenarios, the use of steganography is very valuable. It can protect the insecurity of wireless communication channels and having enough capability to surprise intruders. In this paper, a brief introduction of steganography along with its association to cryptography is discussed and we believe that it will be very helpful in the development of security protocols for various applications.

Keywords**: Steganography, Cryptography, Wireless Communication, Security Protocols, Network Security**

INTRODUCTION:

Steganography hides the existence of data in order to save it from intruders. The data (message) is kept inside a carrier file. This carrier file can be an image, audio file or a video file. The message text should be kept inside the carrier file in such a way so that no loss of data will be there and it can be retrieved only by intended receiver. The below figure denotes various types of steganography.

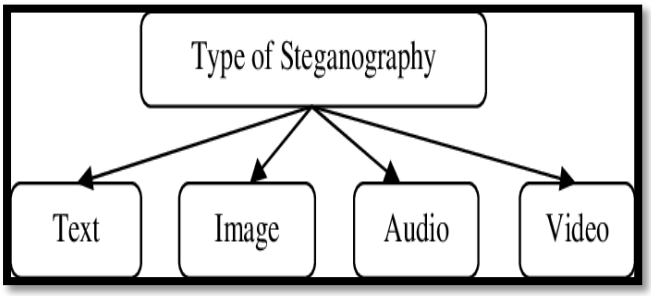

Fig.1. Showing possible types of steganography on the basis of carrier file

Steganographic approaches can also be divided on the basis of technicalities and applied transform method and the below figure illustrates this classification.

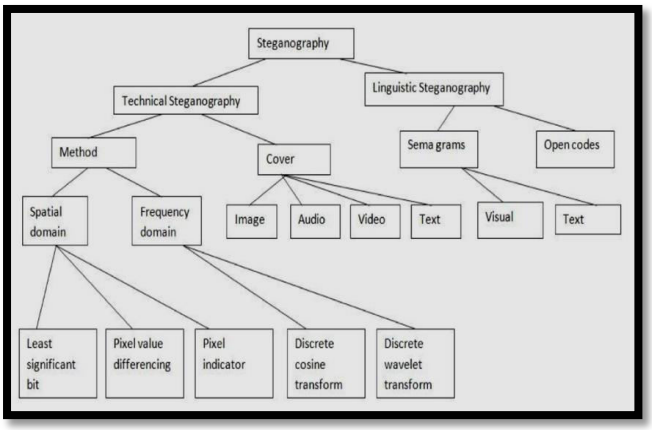

Fig.2. Showing types of steganography on the basis of technicalities and applied transforms

Steganography is a complementary tool for cryptography and security protocols. Steganography can be used with cryptography and its allied areas [1-9]. It can also be used in plenty of wireless communication scenarios [10-15] along with network security related applications [16-20]. Cryptography provides confidentiality, data integrity, authentication and non repudiation and they are known as cryptographic goals as shown in below figure.

Fig.3. Showing cryptographic goals

Steganography also provides communication security but in a different way i.e. by hiding the presence of data. The below figure shows a comparison between cryptography and steganography.

	Steganography	**Cryptography**
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

Fig.4. Showing comparison between steganography and cryptography

Steganography Applications: Steganography provides plenty of applications. Some of them are listed below.

- Provides data security by hiding the presence of data
- Protects data alteration and avoids Denial of Service (DoS) attack [21]
- Encrypted data can also be hidden so provides high security to encrypted data [22]
- Used extensively in media database systems and digital image processing [23]

The below figures illustrates some of the applications of steganography in a better way.

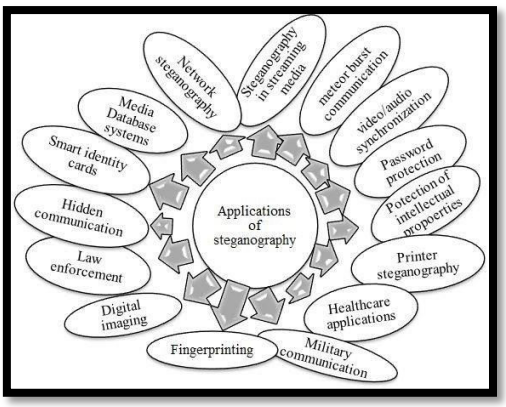

Fig.5. Showing applications of steganography

There are so many open access tools available for steganography. As a beginner, one can use these tools freely and practise various approaches of steganography quickly. The following figure illustrates this.

Tool	*Year*	*Functionality*
CovertTCP	1997	Covert Channels using TCP and IP headers
StegTunnel	2003	Timing channel using TCP header fields
hCovert	2005	Covert channel using HTTP GET requests between webservers
VoVoIP	2007	Embedding data in PCM voice traffic exchanges
SteganRTP	2007	Uses RTP of VoIP as payload medium
Gary-World Team's	2008	Covert channel projects using TCP and IP headers
Steganography Studio	2009	Training suite on network steganography tradecraft
NetCross	2010	Utilizes the DNS protocol to establish covert comm.
OpenPuff	2011	Multiprotocol embedding toolkit
SoCat	2013	Network relay transfer between two independent data channels

Fig.6. Showing open access tools of steganography

These tools can also be divided into categories such as based on carrier file, domain or GUI as shown in below figure.

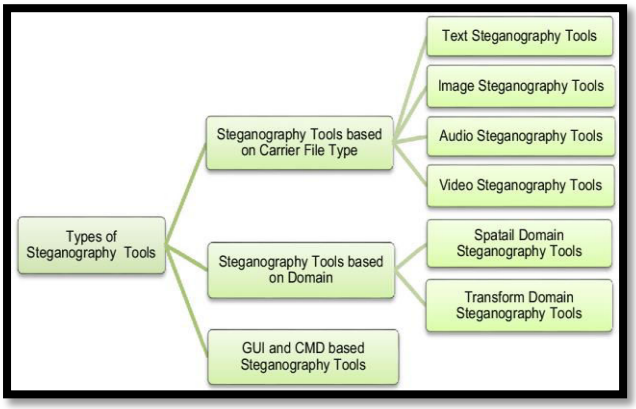

Fig.7. Showing division of steganographic tools based on carrier file, domain and GUI

Some of the examples of famous tools are shown in below figures.

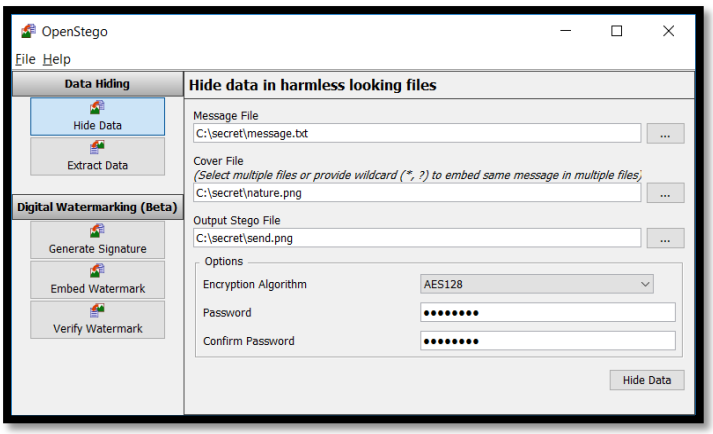

Fig.8. Showing GUI of OpenStego

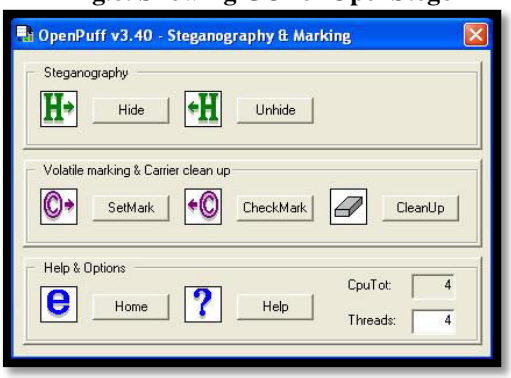

Fig.9. Showing GUI of OpenPuff v 3.40

Fig.10. Showing GUI of HideNSend

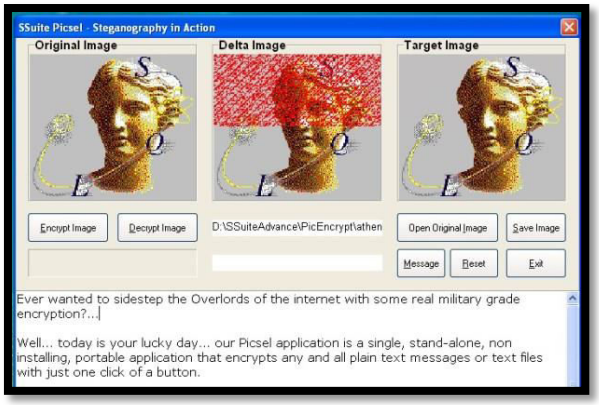

Fig.11. Showing GUI of SSuite Picsel

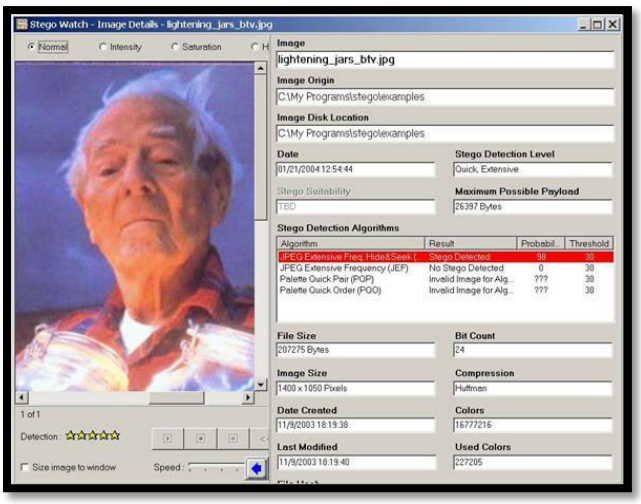

Fig.12. Showing GUI of Stego Watch

CONCLUSION & FUTURE SCOPE:

From the above discussion, it can be concluded that the combination of steganography and cryptography have enough potential to surprise intruders. Steganography hides the presence of secret message while cryptography provides security goals. Steganography can be of many types and can be used in variety of security applications. It is very helpful in wireless security protocols as wireless communication channels are vulnerable to many security attacks. Steganography can resist DoS attack and used extensively in media database systems. There are so many open tools available for steganography and they differ on the basis of GUI, domain or types of carrier files etc. The future scope of the crypto-stegano duo is also very bright as new security protocols are needed in modern scenarios because intruders are very equipped now and they have tremendous computing strength. The emergence of quantum computers can endanger existing security protocols and in that case steganography based security protocols will be very useful as they can provide a new direction to coders and developers.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International

journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. M. Mehic, J. Slachta, M. Voznak, Whispering through DDoS attack, Perspectives in science, volume 7, 2016, 95-100,
DOI: https://doi.org/10.1016/j.pisc.2015.11.016

[22]. A. Jan, S.A. Parah, M. Hussan, B.A. Malik, Double layer security using crypto-stego techniques:
a comprehensive review, Health and technology, volume 12, 2022, 9-31,
DOI: https://doi.org/10.1007/s12553-021-00602-1

[23]. A. Cheddad, J. Condell, K. Curran, P. McKevitt, Digital image steganography: survey and analysis of current methods, Signal processing, volume 90, issue 3, 2010, 727-752,
DOI: https://doi.org/10.1016/j.sigpro.2009.08.010