A BLEND OF CRYPTOGRAPHY AND STEGANOGRAPHY

[1]Natasha Taneja, [2]Dr. Prinima Gupta

[1]M.Tech Scholar, [2]Assistant Professor, Department of Computer Science,
Manav Rachna College of Engineering, Faridabad (India)

ABSTRACT

Due to increase in demand of internet applications, it is required to transmit data securely from one place to another. The data transmitted is not protected as it can be hampered by hacker or intruder. So, for this purpose we have to use Cryptography and Steganography or the combination of both to enhance the security by providing dual security structure. Cryptography is to hide the data using encryption algorithms. Steganography is used to hide the data into another data or a file known as cover file. In order to make faithful and secure communication, a dual security technique is proposed in this paper. We are merging these two techniques in order to upgrade the security and making communication more reliable.

Keywords: Cryptography, Steganography.

I. INTRODUCTION

Internet is widely used around the world. Its applications are required to send and receive information and their major issue of concern is information security. Transmission of data is not secured in public communication as data can be obstructed by intruder or eavesdropper. In any communication, it is necessary to maintain the integrity of data. With the advancement in technologies, the networks over the long distance may not be reliable to provide the secure communication. To overcome this problem Cryptography and Steganography are the techniques which are used widely. Cryptography is an art of keeping the data secret to ensure that it is unaltered and secure. Steganography is combined with cryptography to enhance the security. Steganography is an art of hiding or embedding file in a cover file to ensure the data confidentiality and authenticity. The blend of these two techniques can ensure the secure transmission of data.

II. CRYPTOGRAPHY

Cryptography means "Hidden Writing". It is one of the techniques which are used to ensure the secure transmission of data between sender and receiver by scrambling the input message to produce the output. In this technique plain text is converted into cipher text by applying several algorithm such as private key cryptography, public key or symmetric and asymmetric algorithm for security of the information. It provides solution to several set of parties but the attacker can easily interpret or modify this text without letting aware of their presence between the communications so to overcome this problem Cryptographic techniques are used.

2.1 Cryptography Schemes

To maintain the security of data, three types of schemes are widely used. These are as follows:

1) *Private / Symmetric Key*: As the name states there should be a same or a secret key used for encryption of plaintext and decryption of cipher text. Plaintext is the original messages send by the sender whereas

Cipher text is the scrambled message which is produced as output at the receiver side. The following diagrams describes two important phases of cryptography: Encryption Phase and Decryption Phase (Figure1.1 and Figure 1.2)

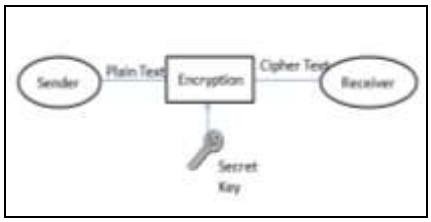

Fig 1.1: Encryption Phase

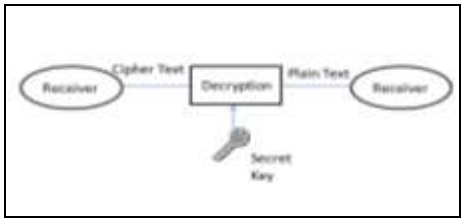

Fig 1.2: Decryption Phase

2) *Public / Asymmetric Key*: In this scheme, different keys are used for encryption and decryption phases. To enhance the security two keys are used: Public Key and Private Key. In Encryption phase, the sender uses public key of receiver to encrypt a message and the receiver uses his private key to decrypt the cipher text. In order to provide authentication, private key of the sender is used to encrypt a message and public key of the sender is used to decrypt the message at the receiver's side.

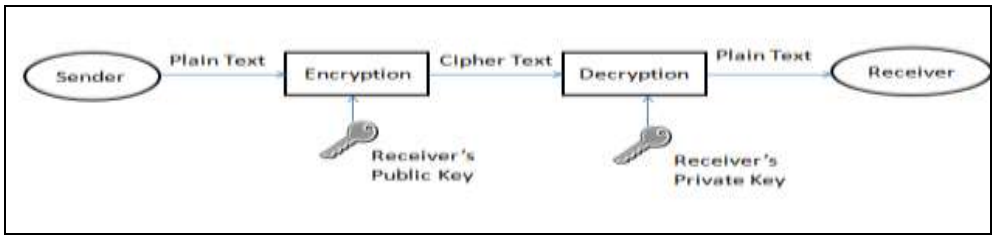

Fig 1.3: Encryption

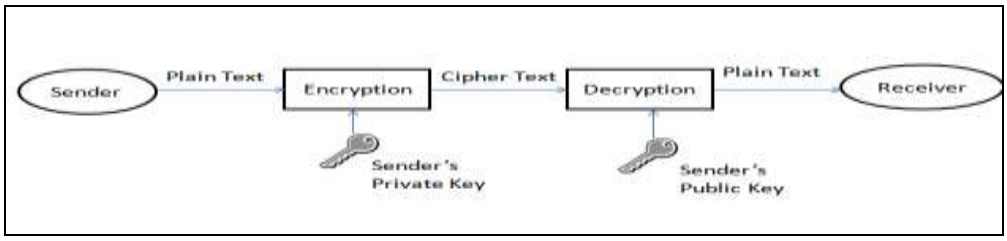

Fig 1.4: Authentication

3) *Hash Functio*n: It is also known as message digest. It maps a message of variable length to a fixed length hash value. This fixed - size output is also known as hash code. It is often used to ensure that file is unaltered or not affected by intruder or hacker.

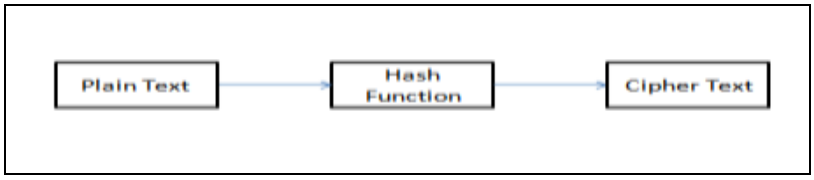

Fig 1.5: Hash Function

One of the most important developments on public key cryptography schemes is Digital Signature. Public key cryptography is being preferred as it is more secure and data integrity is maintained.

Digital Signature is one of the important aspects for securing the content. For that Digital Signature is being used as it overcomes all the limitations of the conventional signature. Now days, it is widely used in email, Credit cards for transaction and many more. The two broad techniques of digital signature are: symmetric key cryptosystem and public key cryptosystem. Cryptosystem here refers to encryption technique.

- *Symmetric Key Cryptosystem*: In symmetric key cryptosystem, secret key is being used which is only known to sender, there only one key or a unique key is used between the sender and receiver or in another words between two users. Its limitation is generation, distribution and keeping track is difficult.
- *Public Key Cryptosystem*: In public key cryptosystem, a pairs of keys is used, private key is only known to a sender and public key is known to all the recipients who are interested in communicating with a sender.

To maintain confidentiality of the message, it should be encrypted with sender's public key on which decryption can be performed by sender's private key.

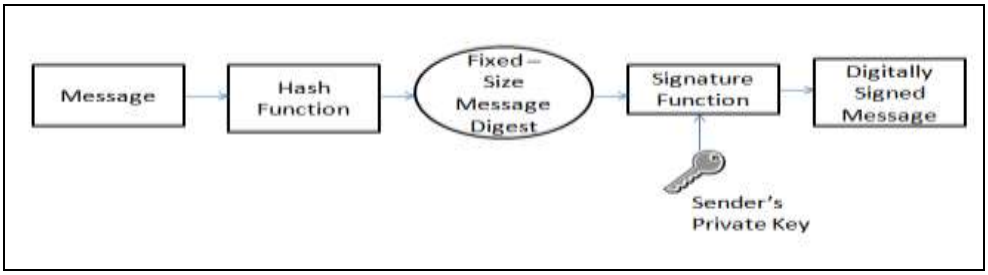

Fig 1.6: Digital Signature

III. STEGANOGRAPHY

Steganography is an art of hiding or embedding one file into another. Cryptography is used to scramble the message but does not to hide the encrypted data whereas in Steganography, message remains unaltered but its presence is hidden by embedding it into a cover file.

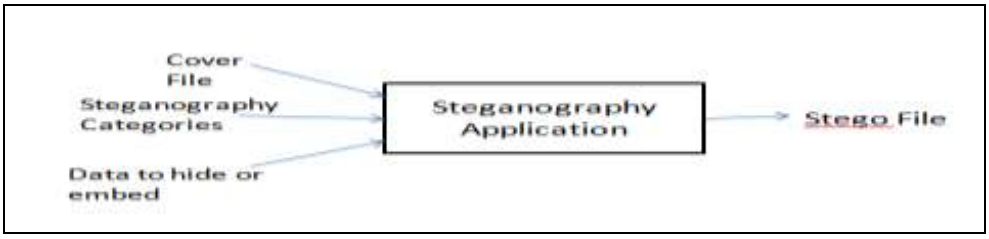

Fig 1.7: Steganography

Fig1.7 describes the following components of Steganography:

- *Cover File*: Data to be concealed is embedded.
- *Data to hide or embed*: Data to be hide.
- *Steganography Categories*: Different categories of Steganography, like text, audio, video etc.
- *Steganography Application*: Is used to hide data within a cover file.
- *Stego File*: It contain cover file along with hidden information.

IV. COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY

Merging these two security approaches provides more privacy and security. Cryptography changes the format of the data that cannot be access by any third party and Steganography on another hand hides this coded data into a cover file. So that no one can easily decrypt the data and also prevent from intruder or hacker.

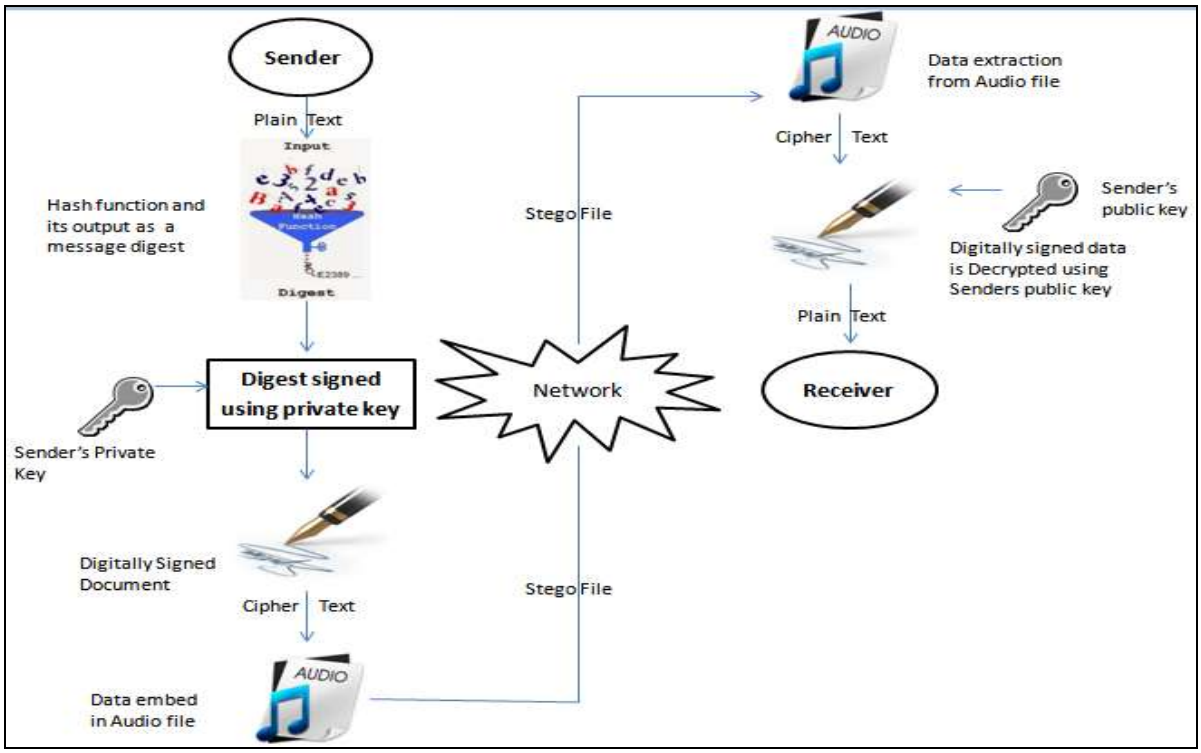

Fig 1.8: Combining Cryptography and Steganography

In Fig 1.8 Sender sends plaintext or original text, this plain text is converted to digitally signed document using hash function and a certificate which further produces a Digitally Signed document. This Digitally Signed document is converted to Stego file using Audio Steganography. The message is decrypted at receiver's end by converting Stego file to Digitally Signed data then to plain text.

If any of these technologies, Cryptography and Steganography is used individually then may lack some security issues which can be achieved by amalgamation of these two. Table 1.1 Depicts the result of combination of these two and how this helps in raising the security against threats.

S.No.	Cryptography	Steganography	Combination
1.	The message is in unreadable format as transformed to Cipher text.	The message is obscured within another medium or Cover file and produces Stego file.	Plain text is transformed to Cipher text then Cipher Text in transformed to Stego file.
2.	The message can be detected and modified easily by anyone.	The message cannot be detect easily as it is hidden within another medium.	The message is encrypted as well as secured from interceptor.
3.	The objective is to prevent unauthorised access.	The objective is to secure the existence of the hidden data from the interceptor.	To prevent from unauthorized attack as well as prevents data from being read by third party.
4.	Data can be discovered easily but extraction of data is complex.	Discovery as well as extraction of data is complex.	Detection as well as extraction of data both are made complex.
5.	Reverse engineering is performed in order to enhance or duplicate the security.	Exchanged data is analyzed and regularly monitored.	Enhancement of security by using Reverse engineering as well as regular monitoring of data.

Table 1.1: Cryptography, Steganography and their combination

However combining both the techniques provides the enhanced security but either of these techniques cannot provide protection as compare to dual protection provided by their combination. Merging of these two is more beneficial as it increases the confidentiality, prevents from unauthorized attacks and improves data secrecy.

V. CONCLUSION

The advantage of Steganography over Cryptography individually is that identity of messages is hidden from phisher. Whereas the objective of Cryptography is to scramble the message to convert it to unreadable by a third party, the objective of Steganography is to conceal the data from a third party. Therefore, combining both Cryptography and Steganography will be a best choice as it will maximize the security, ensures data integrity and provide more authentication as well as privacy.

V1. ACKNOWLEDGMENT

I take this opportunity to express a deep sense of gratitude and thank Dr. Prinima Gupta, Assistant Professor, Department of Information Technology, Manav Rachna College of Engineering for her cordial support, valuable information and guidance in writing this paper.

REFERENCES

[1] Pramendra Kumar and Vijay Kumar Sharma," Information Security Based on Steganography & Cryptography Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering 4(10), October - 2014, pp. 246-250.

[2] Ankit Uppal, Rajni Sehgal, Renuka Ngapal and Aakash Gupta," Merging Cryptography& Steganography Combination Of Cryptography: RC6 Enhanced Ciphering And Steganography: JPEG", Proceedings of 5th SARC-IRF International Conference, 25 May-2014, pp. 62-64..

[3] S.R. Subramanya and Byung K. YI,"Digital signatures", IEEE Potentials, 2006, pp. 5-8.

[4] R.Valarmathi., M.Sc.,M.Phil 1, G.M.Kadhar Nawaz M.C.A., Ph.D 2," Information Hiding Using Audio Steganography with Encrypted Data", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, January 2014.

[5] Elżbieta Zielińska, Wojciech Mazurczyk, Krzysztof Szczypiorski,"Development Trends in Steganography", Warsaw University of Technology, Institute of Telecommunications Warsaw, Poland, 00-665, Nowowiejska 15/19.

[6] Abdulaleem Z. Al-Othmani1, Azizah Abdul Manaf2 and Akram M. Zeki3," A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[7] Jayram , Ranganatha H, Anupama H," INFORMATION HIDING USING AUDIO STEGANOGRAPHY- A SURVEY", The International Journal of Multimedia & Its Applications (IJMA), vol. 3, no. 3, August 2011.

[8] Erfaneh Noorouzi1 , AMIR REZA ESTAKHRIAN HAGHIGHI ,Farzad Peyravi, Ahmad Khadem zadeh," A New Digital Signature Algorithm", 2009 International Conference on Machine Learning and Computing IPCSIT, vol.3 (2011).

[9] Niels Provos, Peter Honeyman ,"Hide and Seek: An Introduction to Steganography", IEEE Computer Society, IEEE Security & Privacy , 1540-7993.