Integration of Cryptography Standards and Steganography for Secure Communication

Navnath Gavde
Ajeenkya D Y Patil University, Loahegaon

Harshad Darekar
Ajeenkya D Y Patil University, Loahegaon

Shabnam Sharma
INurture Education Solution Bangalore, Karnataka

ABSTRACT
Securing the massive amount of data is one of the greatest challenges and it is equally important to ensure data privacy. When the data transmitted from one computer to another, the probability of accessing the data by un-authorized user becomes high. This paper proposes a solution to enhance the security of data, using both cryptography and steganography. The key focus of this paper is to provide confidentiality of data and authentication of user. Confidentiality is achieved using RSA, a Public-key cryptography algorithm, whereas for Steganography, S-tool is used in this research work.

Keywords
Authentication, Cryptography, Public Key Cryptography, RSA, Steganography

1. INTRODUCTION
Ensuring content access control over the network is considered to be one of the critical security issues. For illustration, ensuring access control to information shared by Military personnel, over the network can be accessed by anyone. Information security stands strong based on three fundamental principles, which can be used to protect information available on network. The principles are Confidentiality, Integrity and Availability, commonly known as (CIA). In this paper, focus is on confidentiality of information/data and authentication of user. Here the term 'data' and 'information' is used interchangeably. For achieving confidentiality and authentication, cryptography and steganography are used, respectively. Cryptography can reformat and transform your data, for example- Encryption, making it safer when it traverses among computers. In cryptography, Encryption is the process of encoding messages or making the information in such a way that only authorized parties can access the actual meaning of message. Steganography is the process of hiding data behind any image or another message. Steganography is such a technique that can be used along with cryptography encryption algorithm as an extra-secure method in order to protect data. Steganography techniques can be applied to images, a video file or an audio file. In this paper, the focus is on Image Steganography. As this research work, primarily focuses on Authentication and Encryption. So, brief about the same is provided in subsequent sections.

Authentication refers to the user identity verification process. Depending on the sensitivity of resources, user identities can be verified. There are three common factors used steganography has been one of the trending research areas. As the information technology field is growing need of information security is increasing side by side. In today's scenario for sending secret information Steganography is a widely used communication technology. The author of [8] has suggested that that the RSA use the mathematical fact for authentication: Something you know (such as a password), something you have (such as a smart card) and something you are (such as a fingerprint or other biometric method). In this paper, proposed approach relies on 'something you know' i.e. password and encryption, which is used in S-Tool. S-Tool provides the facility to hide the data in Graphics Interchange Format (GIF) or Bitmap (.bmp) image files or in .wav sound files. It can also perform encryption with IDEA, DES, Triple-DES, and MDC. Another major section on which proposed methodology relies is confidentiality. Confidentiality is all about ensuring that data is not available or disclosed to unauthorized people. The data should be confidential, so that it cannot be read or understood by any person other than the intended recipient. In this paper, RSA is used as an encryption technique. RSA algorithm belongs to the Public Key Cryptography, which makes the use of two different set of keys, generally referred as Public key and Private Key. Public key, as the name suggests, is known to all the parties, active on network. Whereas, Private Key is known only to intended recipient. To achieve confidentiality, Public Key is used for encrypting messages. The intention is that messages encrypted with the Public key can only be decrypted time using the Private-Key. Even the sender cannot decrypt the message that he or she created once it is encrypted with the Public-Key. In this paper, main focus is on RSA encryption technique and image steganography.

2. REVIEW OF LITERATURE
The author of [1] has suggested that the main focus of Content Access Control is that the system and resources are access only by the authorized parties. The author of [2] has suggested that authentication using password is most prominent and user-friendly authentication process. The author of [3] has suggested that Steganography is closely related to cryptography. Both this together make communication more secure. Cryptography encrypt the message so if it is intercepted, then also it is of no use. The author of [4] has suggested that Modern information hiding technology is an important branch of information security. Three aspects capacity, security, and robustness are generally consider while designing of information hiding schemas. The author of [5] has suggested that the techniques cryptography and steganography used in combination provide enhance security to data. The author of [6] has suggested that the basic file Encryption and Decryption is achieve using Public key and Private key cryptography that provide effective security to document. The author of [7] has suggested that in recent years, image

that, while it is easy to multiply two large primes, it is extremely difficult to factorize their product. So, this product can be used as the encryption key. The author of [9] has suggested that services provided by cloud computing over the network of servers. So it is mandatory to provide the security measures so that there is no misuse of any of the

user's data. The author of [10] has suggested that the most important goal of steganography is Protection of the hidden information. The author of [11] has suggested that the growth of wireless systems increases vulnerabilities in resources. Authentication allows that the information is transferred between only authorized people. Hence we increases

Levels of access to information. The author of [12] has suggested that to increase the effect of image steganography use well-known contents, like famous character images or well-known scene pictures etc. The author of [13] has stated that steganography received a great attention, especially from law enforcement. The author of [14] has stated that for providing security to information cryptography involves privacy, confidentiality, key exchange, authentication, and non-repudiation. The author of [15] has stated that RSA is standard algorithm that use Public-key, Private-key for providing security to data in networks.

3. PROPOSED ALGORITHM

Use the following proposed algorithm so no one can hack your data easily. If hacker compromise one phase (example:- password) then also he/she have to face remaining two phase. If hacker get access to data then also it is of no use because it is in encrypted format. Data is very much secure using this technique. Steps carried out at sender side are depicted in figure 1 and steps are explained using algorithm 1. Steps carried out at receiver side are depicted in figure 2 and steps are explained using algorithm 2. Process at sender side: - first create the file that contain the information that should be secure. Then encrypt that data using Public key in RSA algorithm, then select the image behind which the data should be hide and move it to into the S-tool. After this transfer the encrypted data on the image in S-tool. After doing this assign password and encryption type to file in S-tool. So the data is fruitfully hide behind the image. Process at receiver side: - first transfer the image in S-tool that contain hidden information. Use password and encryption type that should be same as used at the sender side. After this output file that is being in encrypted format decrypt it using Private Key in RSA algorithm. Now we have the file that is in its original format.

Algorithm 3.1: Sender side

Input: Input text message i.e. plain text (P_T).

Calculate Private key (P_R) and Public key (P_U).

Output: Hidden encrypted i.e. cypher text (C_T) behind the image.

Begin

Input message, P_T

Use Public key, P_U

€ ($P_T + P_U$) = C_T

Select the S-tool for image steganography.

Insert the image in S-Tool.

Insert the C_T in s-tool.

Assign the password and encryption type in-

S-tool.

End

Algorithm 3.2: Receiver side

Input: Image file with hidden text message.

Output: Original input text message.

Begin

Select the S-tool for image steganography.

Insert image file having hidden text message.

Insert password and encryption type in s-tool.

Save the C_T file

Use P_R key to get P_T

€ ($C_T + P_R$) =P_T

Output: Original input text message

End

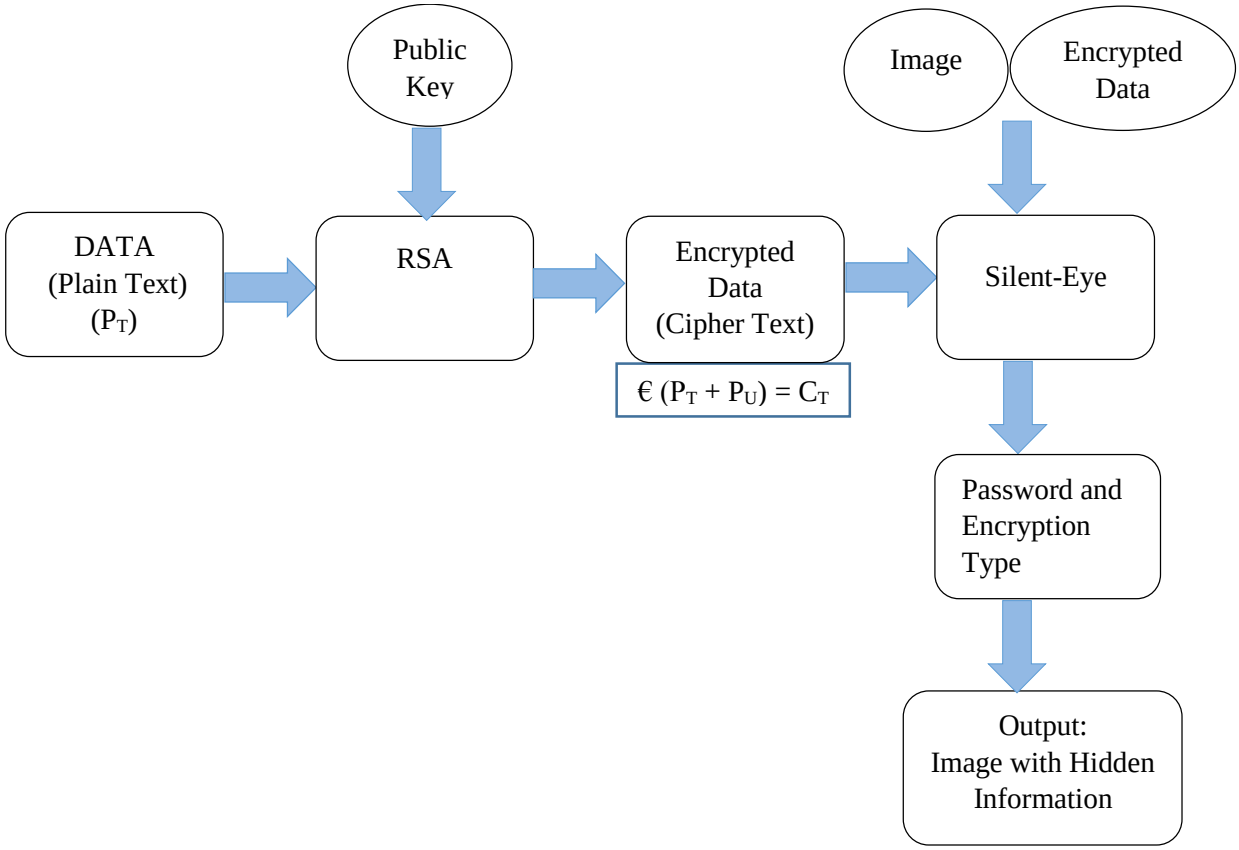

Figure 1: Processing at sender side

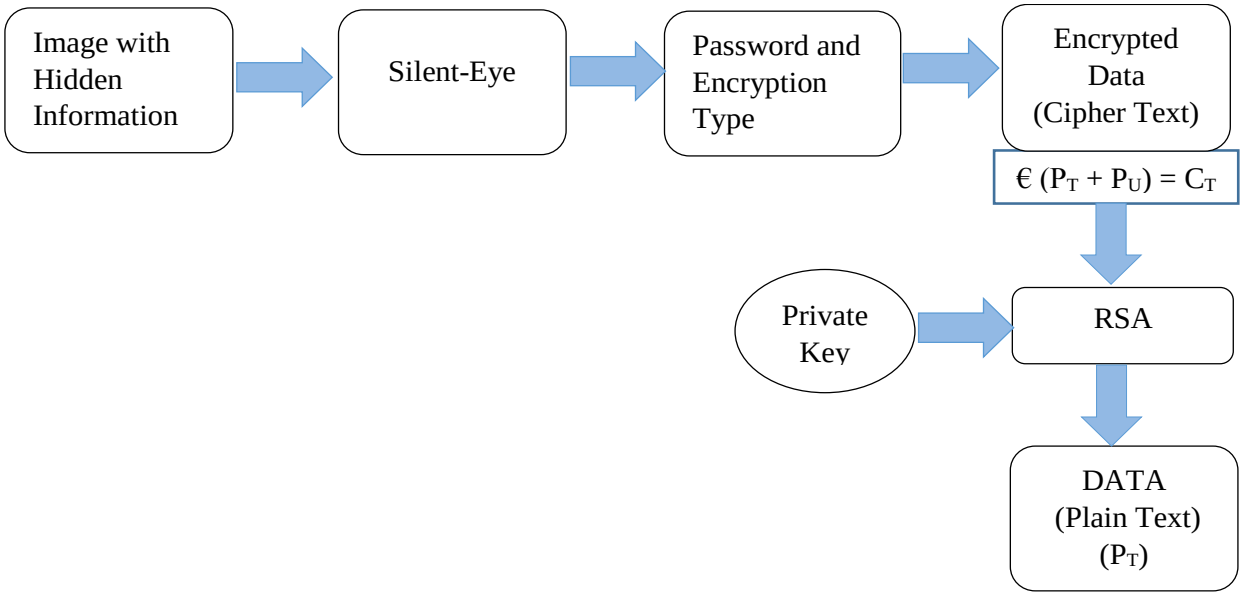

Figure 2: Processing at receiver side

4. CONCLUSION

To provide secure communication over network, a novel technique is proposed. This technique makes the use of two broad categories of Cryptography: Encryption and Steganography. As data travels from one computer to another, there are chances that, data may go out of your control. So, for securing the data and for maintaining its privacy, hybridization of encryption and authentication mechanism becomes necessity. The proposed mechanism offers security using password, encrypting technique – RSA and S-Tool for Steganography. In future, implementation of proposed methodology will be done using Java programming language.

5. REFERENCES

[1] Ragab-Hassen, H., & Lounes, E. (2017). A key management scheme evaluation using Markov processes. International Journal of Information Security, 16(3), 271-280.

[2] Manulis, M., Stebila, D., Kiefer, F., & Denham, N. (2016). Secure modular password authentication for the

web using channel bindings. International Journal of Information Security, 15(6), 597-620.

[3] Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures (Vol. 1). Springer Science & Business Media.

[4] Radke, S. S., & Sambhe, V. K. (2011). Image steganography: an approach for secrete communication. In Thinkquest~ 2010(pp. 205-207). Springer, New Delhi.

[5] Aeloor, D., & Manjrekar, A. A. (2013, August). Securing Biometric Data with Visual Cryptography and Steganography. In International Symposium on Security in Computing and Communication (pp. 330-340). Springer, Berlin, Heidelberg.

[6] Chang, L., & GuangMing, X. (2012). Research and Implementation of File Encryption and Decryption. In Advances in Computer Science and Engineering (pp. 165-170). Springer, Berlin, Heidelberg

[7] Saleema, A., & Amarunnishad, T. (2016). A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks. Procedia Technology, 24, 1566-1574.

[8] Salomaa, A. (2013). Public-key cryptography. Springer Science & Business Media.

[9] Priyansha Garg, Moolchand Sharma, Shivani Agrawal, Yastika Kumar - Security on Cloud Computing Using Split Algorithm Along with Cryptography and Steganography

[10] Roy, R., Sarkar, A., & Changder, S. (2013). Chaos based edge adaptive image steganography. Procedia Technology, 10, 138-146.

[11] Rad, A. I., Alagheband, M. R., & Far, S. B. (2018). Performing and mitigating force and terrorist fraud attacks against two RFID distance-bounding protocols. Journal of information security and applications, 42, 87-94.

[12] Lin, C. C., & Tsai, W. H. (2004). Secret image sharing with steganography and authentication. Journal of Systems and software, 73(3), 405-414.

[13] Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. Journal of information security and applications, 40, 217-235.

[14] Ali, Z. M., & Ahmed, J. M. (2013). New computation technique for encryption and decryption based on RSA and ElGamal cryptosystems. Journal of Theoretical and Applied Information Technology, 47(1), 73-79.

[15] Bhaskar, R., Hegde, G., & Vaya, P. R. (2012). An efficient hardware model for RSA Encryption system using Vedic mathematics. Procedia Engineering, 30, 124-128.