TRIPLE LAYER SECURE ENCRYPTION: BY COMBINED RSA, IMAGE STEGANOGRAPHY&DIGITAL SIGNATURE.

Pooja Ahlawat.
M.Tech Scholar, Dept. of Computer Sc.& Applications, M.D. University, Rohtak, India.

Manuscript Info

Abstract

With increase in use of Internet among public and availability of digital data sharing has taken industry professionals and researchers to give independent focus on information security. With growing internet users frequently required digital media store space to receive and send private information and this information requires protected against unauthorized attacks & access. In this paper I have presented a new technique for providing secure encryption to the user data. New proposed secure encryption will consists of a combination of RSA Encryption, Steganography along with digital signature.

Introduction:

Cryptography offers us the ability to transmit critical data between resources in a way that protect form third party reading it. Cryptography also provide authentication of someone and data. Following types of algorithms are used to specify cryptographic algorithms:

1. Secret key: Encryption and decryption done by single key.
2. Public Key: Two separate key are used for both process.
3. Hash Functions: A mathematical transformation to irreversibly encrypt information \(^1,2\).

Steganography technique overlaps the existence of the secret data from an observer into a cover media. Three primary accessories are needed before performing steganography. First is information or data, Secondly Cover data medium and most important hiding technique. The cover medium can be a text file, an image, an audio file or video file but the most popular is the Image steganography. Primary objective of this technique is to avoid attention from the transmission of hidden information. If intruder detected any changes in the content or material, then the objective that has been processed to achieve the security level of the secret data is at risk, intruder will anyhow try to get the hidden data inside the message.

Background:

RSA Algorithm is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 is represented in figure 1. It uses two big prime numbers randomly generated to define the public and private keys. The two different keys are used for encryption and decryption purpose. Sender, when the message gets transmit to receiver, encrypts the message using Receiver public key and then receiver can decrypt it using his own private key \(^3,4\). RSA operations can be divided into three broad steps; key generation, encryption and decryption.

Key Generation:

1. Select two distinct large random prime numbers p & q such that p ≠ q.

Corresponding Author:- Pooja Ahlawat.
Address:- M.Tech Scholar, Dept. of Computer Sc.& Applications, M.D. University, Rohtak, India.
2. Calculate: n= p × q.
3. Calculate: φ(n) = (p-1)(q-1).
4. Select an integer e such that 1<e<φ(n)
5. Calculate d to satisfy the congruence relation
d × e = 1 mod φ(n); d is kept as private key exponent.
6. Public key is (n, e) and private key is (n, d).

![Figure 1: Block Diagram for RSA](image)

**Encryption:**
Plain text: P < n
Cipher text: C= P^e mod n.

**Decryption:**
Cipher text: C
Plaintext: P=C^d mod n.

**Proposed Methodology:**
Required robustness and security can be achieved: steganography & cryptography is combined along with additional digital signature that provide third layer of security. For cover media I will take Image for steganography and RSA algorithm will be used for encryption and is represented in figure 2. By combining, the data encryption will be done by RSA and then the cipher text will be used as input with Image media with the help of digital signature. The combination of these two methods along with digital signature will enhance the security of the data embedded.

![Figure 2: Combination of Steganography and Cryptography](image)
Working Architecture:-
A development of the complete proposed model is completed and the implementation of Encryption Process is also completed. As encryption is a lifelong work to secure data. Day after day new and advanced techniques will be required to secure our data from hacker.

![Diagram of Detailed Architecture for Proposed Technique](image)

As details architecture is represented by in the figure 3. The Process is stated by converting plain text of uses into the cipher text by using RSA encryption process, Cipher text as plain text for Steganography, Cover Image required is input by user, Digital Signature that is of user choice. Here in implementation I have considered four – digit numeric value for digital signature and that is entered by user. Encryption Process is completed as per the detailed Architecture.

Results:-
According to the details architecture of the proposed new techniques shown in figure 3 I have developed new model. Figure 4 contains the complete encryption process. In Figure 4(a) contains the public & the private key randomly generated with the help of RSA encryption process and Figure 4(b) contains the data to be in secured. Figure 4(c) contains the cipher text that is obtains from RSA encryption process. Further Figure 4(d) contains the source of the cover media along with the last layer of security that is digital signature. And the final image Figure 4(e) contains the final message with the save new media that contains data to be hidden.

Decryption process is illustrated in figure 5. Figure 5(a) contains the source media that contains data along with the digital signature both value input by the user. Further figure 5(b) contains the cipher that is obtains from the step one of decryption process that separates cipher text from cover media with the help if digital signature.

Conclusion & Future Work:-
By this extra layers of security will be available to provide security to our document in today’s words. If any how intruder is able to detect the text in the image. Then also that text is no more than cipher text and is also secured by digital signature. Thus triple Encryption is provided to the user data. Decryption process is not completed in the development of this model. My encryption process is working as per proposed model.
Figure 4: Detailed description of encryption process of new proposed Technique
Figure 5: Description of decryption process of new proposed Technique
References: