iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: TPAM-2018 Issue: onference Month of publication: March 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

A Secure Method to Hide Confidential Data Using RSA Algorithm and Image Steganography

Mrs.Bobby[1], Swathi S[2,] Rubia Thasneem P[3]

Assistant Professor, [1,2,3] Department of computer scienceSt.Joseph's College of Arts and Science for Women – Hosur.

Abstract: Today's information world is a digital world. Now a days data transmission over an unsecure channel is becoming a major issue of concern. At the same time intruders are spreading over the internet and becoming very active. In order to protect the secret data from intruders, security measures are to be taken. In order to preserve the secret various techniques have been implemented to encrypt and decrypt the data in which Cryptography and Steganography are the two most prominent techniques. Public key cryptography is used to encrypt messages so that they can be read only by the authorized receiver. The most commonly used public key cryptography is RSA cryptosystem. Image steganography is one such innocent looking tool, where messages are carried inside digital images and the same cannot be decoded unless the receiver knows about the existence of such a message inside the image. To order to achieve the required robustness and security both cryptography and steganography is combined. In previous steganography algorithm, to hide data, the secret content has to be hidden in a cover message. In our research, data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. Image is taken as a cover medium for steganography. RSA algorithm is used for text encryption.In this proposed method digital image steganography is used for embedding the message in the image file and the message is encrypted using the RSA encryption method. Our project is divided in to three phases. The first phase is an encryption phase. It deals with the process of converting the actual message into cipher text using the RSA algorithm. The second phase is an embedding phase, where the cipher text is embedded into an image. The third phase is the decryption phase. The text is decrypted from the image using the secret key.

I. INTRODUCTION

Encryption is the process of translating plain text data into something that appears to be random and meaningless (cipher-text). Decryption is the process of converting cipher-text back to plain text. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher-text without using the key. The longer the key, the more difficult it is to decrypt a piece of cipher-text without possessing the key.

It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successful resisted all attacks. Normally encryption is of two types – Symmetric and Asymmetric. In symmetric key encryption, only one key is used for both encryption &decryption. The key is kept secret. To ensure secure communications between everyone in a group of n people a total of $n(n-1)/2$ keys are needed, which is the total number of possible communication channels. The other names of symmetric key algorithms are secret key, single key or shared key. Asymmetric encryption is also called as public key encryption. It uses two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. The first asymmetric key encryption was found in 1976 called Diffie Hellman algorithm. Public key encryption is pretty good and popular for transmitting information via the Internet. They are extremely secure and relatively simple to use.The RSA algorithm was given by three MIT's Rivest, Shamir & Adelman. It is a message encryption cryptosystem in which two prime numbers are taken initially and then these values are used to create public and private keys. These keys are further used to encrypt and decrypt the message. The digital steganography could be used in a way that original text is embedded in the cover image in the form of cipher text. By using algorithm we are increasing the security to a level above.

Steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. Hiding data is the process of embedding information into digital content without causing perceptual degradation. In data hiding, three famous techniques can be used. They are watermarking, steganography and cryptography. Steganography is defined as covering writing in Greek. It includes any process that deals with data or information within other data. Steganography is hiding the existence of a message by hiding information into various carriers. The major intent is to prevent the detection of hidden information. Research in steganography technique has been done back in ancient Greek where during that time

the ancient Greek practice of tattooing a secret message on the shaved head of a messenger, and letting his hair grow back before sending him through enemy territory where the latency of this communications system was measured in months.

The most famous method of traditional steganography technique around 440 B.C.marking the document with invisible secret ink, like the juice of a lemon to hide information. Another method is to mark selected characters within a document by pinholes and to generate a pattern or signature. However, the majority of the development and use of computerized steganography only occurred in year 2000. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme. There are several steganography techniques used for hiding data. Research in hiding data inside image using steganography technique has been done by many researchers. There are approaches to hide data inside the audiovisual files too. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

II. CONCLUSION

To hide confidential information steganography can be effectively used. The objective of any Steganographic method is to hide maximum secret information which is immune to external attacks and also should not convey the fact that the cover medium can carry any secret information. In this project, we have proposed the combination of cryptography by using RSA algorithm and digital image steganography. RSA is used to encrypt and decrypt the data and digital steganography is used to hide encrypted secret text into cover image. To yield better imperceptibility the proposed method provide a higher similarity between the cover and Stego pictures as a result when steganography is combined with encryption a good security was achieved between two parties in case of secret communication, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication. The proposed approach has many applications in hiding and coding messaging within standard media.

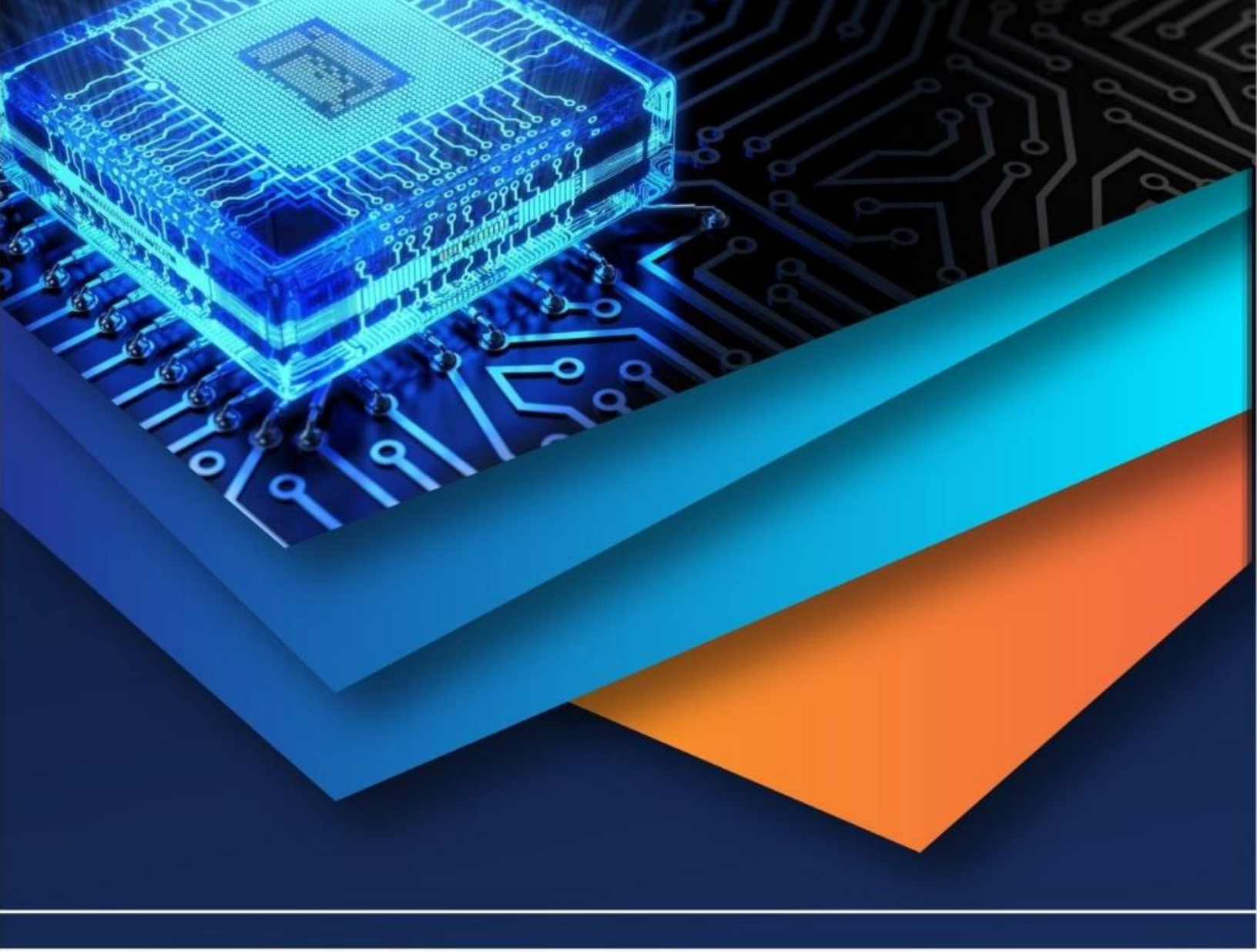
Figure 1 Rsa And Steganographthy

III. FUTURE WORK

In this work it explores only a small part of the science of steganography. As a new displine, there is a great deal more research and development to do. In future scope this work can be enhanced for other data files like video, audio, text. Steganographic techniques can be developed for 3D images also. Steganographic applications are available on the Internet, but it is not known if they are being used. It may be possible to develop an application to serve as a web browser to retrieve data embedded in web page images.

REFERENCES

[1] Adams, C., Meijer, H.: Security-related comments regarding McEliece's public-key cryptosystem. IEEE Trans. Inform. Theory 35, 454–455 (1989)
[2] R.L. Rivest, A. Shamir, and L.M. Adleman, "A methodfor obtaining digital signatures and public-keycryptosystems", Communications of the ACM, volume21, pages 120-126, February1978.
[3] Ronald L. Rivest, Adi Shamir, Len Adelman, "OnDigital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science TechnicalMemorandum 82 (April 1977).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY