Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.451 – 456

Cryptography Using Image Steganography

[1]Pooja Rani, [2]Mrs. Preeti Sharma
Department of Computer Science and Application, MD University, Rohtak
[1] poojaahlawat32@gmail.com

Abstract: The growing use of Internet among public masses and availability of public and private digital data and its sharing has driven industry professionals and researchers to pay a particular attention to information security. Internet users frequently need to store, send, or receive private information and this private information needs to be protected against unauthorized access and attacks. Following are the main methods of information security being use watermarking, cryptography and steganography. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people. Steganography techniques are based on hiding the existence of information by embedding the secret message in another cover medium. While all three are information security techniques cryptography and steganography are having wide application as watermarking is limited to having information particularly about the cover medium. In this a combination of cryptography and steganography is proposed to enhance security of digital data.
Keywords: Cryptography, Steganography, RSA encryption.

1. Cryptography

Cryptography is the art and science of achieving security by encoding messages to make them non readable. In this, the structure of message is scrambled to make it meaningless and unintelligible unless the decryption key is available. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of something or someone. Cryptanalysis is the reverse engineering of cryptography.
There are several ways of classifying cryptographic algorithms. The three types of algorithms are:

1. Secret key Cryptography: Uses a single key for both encryption and decryption
2. Public Key Cryptography: Uses one key for encryption and another for decryption.
3. Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information. [2]

1.1 Purpose of Cryptography

Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

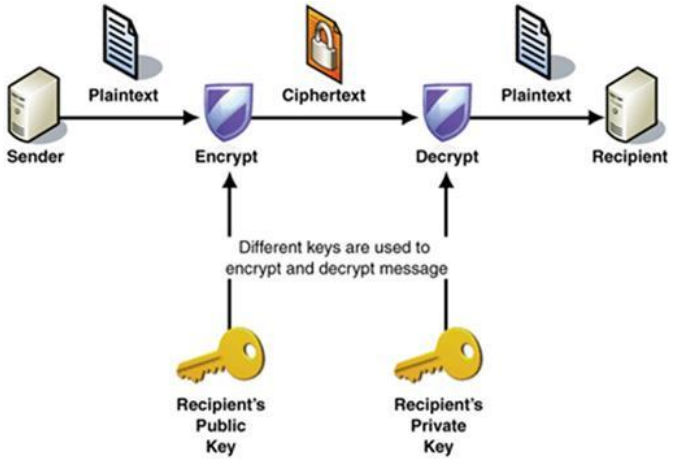

Fig1. Basic Cryptography

There are some specific security requirements, including:

1. Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
2. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
3. Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4. Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography, thus not only protects data from theft or alteration, but can also be used for user authentication. [3]

Attack

Attack on the security of a computer system or network is best characterized by viewing the function of the computer system as providing information. In general, there is a flow of information from a source to a destination. The main security threats are ad follow:

- **Interruption**. An asset of the system is destroyed or becomes unavailable, or even unusable. This is an attack on availability.
- **Interception**. An unauthorized party gains access to an asset, which is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer.
- **Modification**. An unauthorized party not only gains access to an asset, but also tampers with it. This is an attack on integrity.
- **Fabrication**. An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.

2. Steganography

Steganography is a very old technique of information hiding. Steganography refers to the science of invisible communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganography techniques strive to hide the very presence of the message itself from an observer. The term Steganography is forked from the Greek words — "steganos" meaning — cover and — "graphia" meaning — writing defining it as — covered writing. Before performing steganography we need three primary accessories which are Secret message, Cover medium and one or more embedding algorithm(s) besides these we can also use secret key for better security purpose. In the process of steganography the cover medium can be a text file, an image, an audio file or it can be a video file but among these most popular is the Image steganography, so here are the some advantages of using images as cover medium in performing steganography [1].

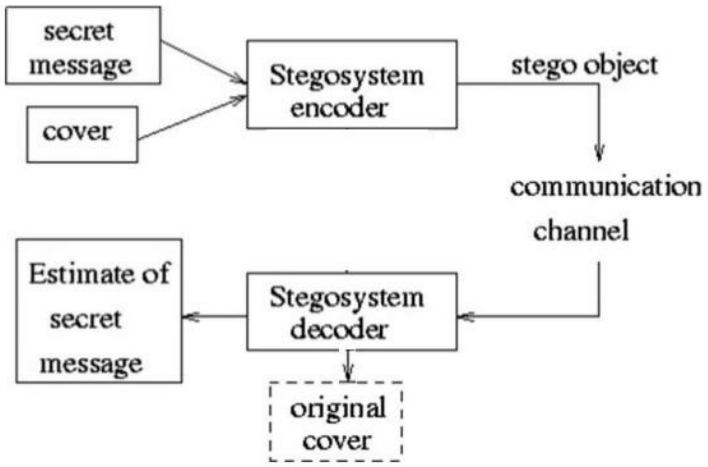

Fig 2: Basic Steganography

Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from the intended recipient knows the existence of the message. The word "steganography" is basically of Greek origin which means "hidden writing". The word is classified into two parts: steganos which means "secret" and "graphic" which means "writing". However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word "steganography" is often considered similar to "cryptography" and "watermarking". Whilst watermarking ensures message integrity and cryptography scrambles the message, steganography hides it. [4]

The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message**.**

2.1 Applications of Steganography

Steganography is the process of hiding secret data within public information. Secret data can be a plaintext or cipher-text, or any kind of data that can be hidden in digital media. Since all kinds of secret data must be translated into binary, we always hide binary data whatever this secret data or file is. Steganography is applicable to various areas but not limited to these areas. The areas differ in the features of the steganography that is utilized in each system. Various areas where steganography used are as follows:

1. Confidential communication and secret data storing
2. Protection of data alteration
3. Access control system for digital content distribution
4. Data storage

2.2 Classification of Steganography

Primarily steganography can be classified into two categories:

1. Spatial Domain Steganography:

In spatial domain steganography we directly deal with the pixel value of the image which means that we directly embed our secret information into some specific value of the pixel. One of the most common and popular spatial domain steganography is the LSB (least significant bit) modification method, it is the most common and also it is a high capacity stenographic method but it is not so much robust against certain attacks like low pass filtering and image compression.

2. Frequency Domain Steganography:

It is also known as transform domain steganography because before doing steganography we have to convert the original image from its spatial domain to frequency domain using certain methods like Discrete cosine transformation (DCT), Discrete Fourier transformation (DFT), Discrete wavelet transformation (DWT) etc. After that we embed our secret information into the coefficients of its transform domain. In this case detection of

steganography is very difficult because we embed our secret information into the frequency domain not in the visual domain [1].

3. RSA – Algorithm

RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it using his own private key [5, 6]. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p & q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the system's overheads by taking more processing time [7].

Key Generation Procedure [8]

1. Choose two distinct large random prime numbers p & q such that $p \neq q$.
2. Compute $n = p \times q$.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that $1<e<\text{phi}(n)$
5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption

Plain text: $P < n$

Cipher text: $C = P^e \bmod n$.

Decryption

Cipher text: C

Plaintext: $P = C^d \bmod n$.

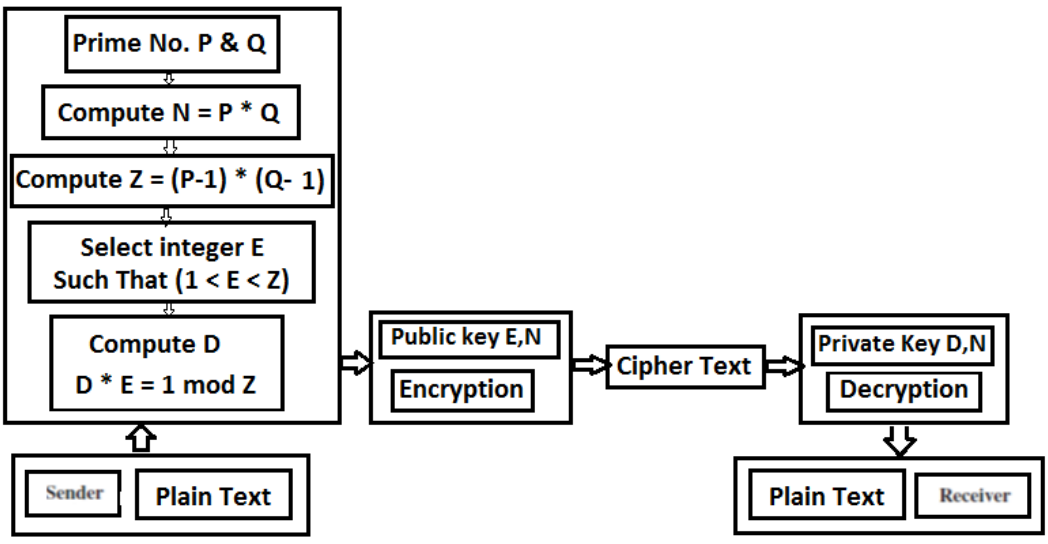

Fig 3: Block Diagram for RSA

4. Proposed Techniques

The aim of proposed scheme is to make more secure and robust method of information exchange so that confidential and private data must be protected against attacks and illegal access. To order to achieve the required robustness and security, cryptography and steganography is combined. Image is taken as a cover medium for steganography and RSA algorithm is used for encryption.

Combination of Cryptography & Steganography

Steganography must not be confused with cryptography that involves transforming the message so as to make its meaning obscure to malicious people who intercept it. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system needs the attacker to detect that steganography has been used and he is able to read the embedded message. According to, steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. 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.

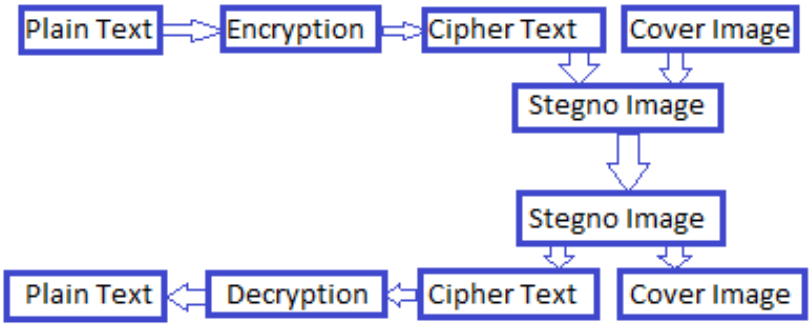

Fig 4: Combination of Steganography and Cryptography

5. Future Work

A development of the complete proposed model is under progress and the complete implementation is also under process. As encryption is lifelong work to secure data. Day after day new and advanced techniques will be required to secure our data from hacker.

6. Conclusion

By this an extra layer of security is added to provide safety 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. Lots of techniques can be applied to get cipher text from plain text. Thus still intruder is far away from getting our precious data.

References

[1] K.Hemachandran, "Study of Image Steganography using LSB, DFT and DWT", International Journal of Computers & Technology, vol 11, oct.25 2013, pp. 2618-2627

[2] Zin.w, soe. N "Implementation and Analysis of three Steganographic Approaches", University of Computer Studies, Mandalay, 2011, pp. 456-460

[3] Manoj.s,"Cryptography and Steganography", International Journal of Computer Applications (0975-8887), 2010, vo1-no.12, pp. 63-68

[4] Kumar S P , K. Anusha, R.Venkata Ramana, "*A Novel Approach to Enhance Robustness in Steganography Using Multiple Watermark Embedding Algorithm*". International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307 (Online), Volume-1, Issue-1, March 2011

[5] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[6] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.
[7] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.
[8] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signatures with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 211-216, 2010.

