INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

Comparison of Cryptographic Techniques

Lakshay Thakur
Computer Science And Engineering,
Amity University, Noida
thakur.lakshay99@gmail.com

Roshan Lal Chokkar
Computer Science And Engineering,
Amity University, Noida
rchokkar@amity.edu

Abstract: The study of hiding information is referred to as cryptography. When communicating over the untrusted med. Such as the internet it becomes very important to protect the sensitive information and hence cryptography plays a crucial role there. It is the study of hiding of info. Over an untrusted medium like the internet where it becomes compulsory to protect the information form the third party or the eavesdropper. On the other hand, steganography provides a cover or a protection layer to the sensitive information being transferred. Steganography deals with the composting of hidden messages so that only the sender is aware of the message being sent and if the third party tries to interfere he/she gets nothing but the cover medium being developed with the help of steganography.
There have been many logical combinations of steganographic techniques which result in efficient protection for any content to be transferred. In this paper, we try to try out some of the famous combination of steganographic techniques and result out the best of them in terms of speed efficiency, security, and reliability for the user.

Keywords: Security, Steganography, Cryptography, Encryption, Decryption, Data Protection.

I. INTRODUCTION

The word Steganography is derived from the Greek words stegos meaning cover and grafia which means writing defining it as covered writing or the practice of concealing messages or information within other non-secret text or data. It is the practice/art of encoding/embedding or protecting any kind of secret information in such a manner that the existing information is protected or it is an art of hiding data in such a manner that the information/sensitive data to be sent over a medium can't be seen or becomes invisible. The first recorded track of steganography is found in 440BC. In ancient Greece, people used wax-covered tablets to write. Steganography and Cryptography are well known used methods or techniques that have the ability to manipulate information in order to hide it or crypt the existence of the sensitive data. Steganography cannot be confused traditional cryptography because in cryptography one can tell that a message is encrypted and the message cannot be decoded without knowing the proper key whereas in Steganography the message itself may not be difficult to decode but most fail to detect even the presence of a message.
This paper will use some of the famous encryption algorithms with the steganography technique to provide a double authentication system which will double secure the transfer of sensitive information over any medium.

II. LITERATURE REVIEW

Cryptography: It is the study of protecting sensitive information by data encoding and transformation techniques. Nowadays cryptography has evolved so much that now it is sometimes coined as Modern Cryptography. It is now a cornerstone of computer and communications security whose foundations are laid on mathematical concepts such as number theory, computational complexity theory, and probability theory. Cryptography can be considered as the toolkit containing different techniques for the security of communication internet being the medium. There are two types of cryptographic schemes available on the basis of key:

Symmetric key cryptography: This cryptographic key uses a common key for enciphering and deciphering the message." [8]

Asymmetric key cryptography: "This type of cryptographic schemes uses two keys for encryption and decryption called Public key and Private Key." [8]

Although steganography is known to be an ancient subject, the modern formulation of it is mostly given by the prisoner's problem proposed by Simmons G., where two inmates wish to communicate in secret to hatch an escape plan. All of their

communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication.

Anderson, R.J. & Petitcolas proposed a model in which the warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information. [2][3]

Steganography is a major part of cryptography and a lot of work has been done in this particular field of cryptography. There are some advancements also which has resulted in making Steganography a more secure and reliable method of transmitting information over different mediums and to different ends. A lot of significant work has been done in this field of Steganography by many famous authors and scientists who have discovered and shared their valuable ideas through research papers like "Securing Data by Using Cryptography with Steganography" by Ajit Singh and Swati Malik have discussed and compared some combinations of steganography and cryptography for improving the data security.

The dominant part of today's steganographic frameworks utilizes objects like the picture, sound, video and so forth as cover media individuals frequently transmit computerized pictures over email and Internet correspondence. Present day Steganography utilizes chance of concealing data into computerized sight and sound and furthermore at the network level. The term Steganography came into use in the 1500s after the appearance of Trithemius book on the subject Steganographia.

Hiding information into a medium requires following elements:

1. The cover medium that holds the secret message to be sent.
2. The secret message may be plain text, digital image files or any type of data.
3. The steganographic techniques. 4. A stage-key may be used to hide and unhide the message.

Today steganography has been divided into five types depending on the cover medium: - Text Steganography. 2. Image Steganography. 3. Audio Steganography. 4. Video Steganography. 5. Protocol Steganography. [9][10]

We will only describe some details about the text, image, and audio steganography as they have been majorly used for comparison analysis. Text Steganography is hiding information using text files is the most widely used method of Steganography. The method was to hide a secret message into a text message but after the evolution of the internet, it lost its important and new techniques were introduced. Image Steganography is Images are one of the most popular cover media for Steganography. A Message using an embedding algorithm can be used to embed in the image. The main benefit of stage images is that unauthenticated persons can only notice the transfer of image but never can see the existence of hidden message in it. Audio Steganography is a technique of transmitting hidden information through modification of an audio signal in a unnoticeable manner. The message before steganography and stage message after steganography has same characteristics.

III.PROPOSED MODEL

Encryption is basically a method of protecting any kind of data from any kind of unwanted access which is not tolerable at any cost. For example, when we use our bank card at any shopping website, our computer encrypts that particular information so that others can't steal our personal details which are being transferred. For encryption, there are many algorithms having their own advantages and disadvantages. In this paper, we use cryptography and steganography combination on different data forms and formats to compare and analyze them on different performance parameters. We would first encrypt the file using any suitable algorithm and then embed that encrypted file into the file we will use as cover media to apply steganography.

1) *TEXT IN IMAGE:* For text in the image we first use RSA (Rivest-Shamir-Adleman) algorithm to encrypt any message in text form. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one being used to encrypt a message can only decrypt it.[6] Using RSA's one key we get an encrypted message. We use Python language to implement the RSA algorithm and also through Python we are able to generate a .txt file. After that, we place the image file into the same folder as that of text's file. Now in cmd, we use the cd... Command to go to the folder where the two files are. Once in that directory using copy /b Name-of-initial-image.jpg + Name-of-file-containing-text-you-want-to-hide.txt. Resulting-image-name.jpg we'll get encrypted image file which will have the encrypted data which we got from the RSA Algorithm in the same folder.Both images i.e., the mediacover.jpg used for the media cover for the encrypted .txt file and the Resulting image are identical.

Fig. 1 Original Image

Fig. 2 Coverage (StegoImage)

As from the above two images it is clearly visible that the normal and the encrypted stage image looks exactly same as each other and if one tries to distinguish between any of them it would be nearly as impossible because not only on the basis of occurrence even the size and property of the images are same.
Now, we took different text files of different sizes and then tried to embed them in the cover media file. We noted the change in the image size which is our cover media file after applying steganography and also observed the time it took for getting embedded in the image.

TABLE I
EMBEDDING ENCRYPTED FILE IN IMAGE

Original text file size (bytes)	**Original Cover mediaSize (Bytes)**	**Final Cover media size (Bytes)**	**Embedding time (sec)**
64	50410	50420	0.27248
560	50410	50425	0.27330
2000	50410	50698	0.27480
4000	50410	50834	0.27502
6000	50410	51025	0.27858
8000	50410	52745	0.27956
10000	50410	53582	0.28123

From the above table it is clearly observed that the even after taking the large text files with different Line of codes or sentences doesn't majorly effect the cover media file size, embedding time or we can say that the embedding time and final cover media size is not even affected by any parameters because the time of compilation from the beginning to the last is merely affected in decimal fractions of the microseconds which is totally negligible and for the size of the stage image we have the same cases where the final size differs in very small margins from the original image.

2) DATA IN AUDIO: Digital music MP3 files are a crucial part of audio compression standards on the internet. MP3 has the destructive technologies to attain higher compression rates so that the original file size is compressed to a very significant size. [4][5] To protect this kind of media many algorithms have been proposed over the time and we will use one of those famous algorithms to see some parameters like result file size time of embedding and will compare these parameters with others. We start off with the text data encryption in which we use the above mentioned RSA Algorithm. We start off with the encryption of normal text file by any of the most efficient algorithms and then after getting the encrypted text file, we use it for embedding it in the audio files. In this way, we will use the double security option for the file to be sent for say because firstly we encrypted the normal text file adding a security layer to it and the again embedding the same encrypted file is embedded into the audio file. The amount of time taken to encrypt the original message will be the same as taken in the above text in image combination but the amount of time taken in embedding the encrypted data in audio is different. We use information hiding methods to hide some more information into the audio media file (MP3). The bits of information will be hidden between frames (BF) in MP3 file. We use RSA algorithm for embedding in the sound file the text file. In the experimental results, we try to hide more characters in audios and extract them correctly and accordingly.

TABLE II
EMBEDDING ENCRYPTED FILE IN AUSIO

Size file	**bytes**	**Original size(audio)**	**Result file size**	**Time of embedding**
1KB	3175	5138432	5136260	1.944
2KB	5279	5138432	5138364	1.94575
4KB	9527	5138432	5142612	1.946375
10KB	22103	5138432	5155188	2.01145
20KB	43343	5138432	5176428	2.02112
40KB	85367	5138432	5218452	2.029923
80KB	170543	5138432	5303628	2.0337432
100	212687	5138432	5345772	2.109365

From the above table it is clearly seen that the embedded file size affects directly the cover file size since the embedding process involves insertion of text between frames of the audio file. So we can say that this method allows integration of large files within a particular cover file but it is effective only when used for relatively smaller sizes.

CONCLUSIONS

Steganography is really an important and interesting subject which is also outside the mainstream of cryptography and the system administration that mostly is dealt by everyone one a daily basis. The major difference between both of them is that in steganography the existence of message is only known to sender and receiver but in cryptography, the existence of encrypted message is accessible to the world. There are numbers of encryption algorithms of different domains and also we know that steganography tools use implementation of intelligent algorithms to carefully embed encrypted text messages or data inside other files which are larger in sizes such as video, audio, text or any other kind of executable file. There are numerous steganography tools available on the internet but only a few of them are to work with and they are most of the time insufficient in fulfilling the needs of the user and also they don't guarantee the reliability and security for the same.

Through this paper, we have shown some of the important aspects of the two most important and majorly used feature for security in communications for the sensitive data i.e., cryptography and steganography. We started off with discussing cryptography's brief and steganography's brief and then we proposed a scheme where we used cryptography and steganography to provide a particular double security feature to a file so that it becomes doubly secured for the communications over any medium. Security is provided in such a way that if the eavesdropper tries to exploit the file he will, to some extent, will get access to the cover media only but will again need to decrypt the firstly encrypted file. In this way, an option for providing security for the encrypted file is developed.

After comparing the result analysis for the two combinations as discussed above through table (1) and table (2) we tried to draw a conclusion as of which among them is more reliable, fast and offers more versatility to the user.

We found that among text in image and data in audio more reliable, fast and compatible is the text in image combination because as from the records we can easily see that time taken in embedding the text in the image takes less time as compared to the time taken for embedding data in audio.

We also tried to analyze the difference in embedding time when different text file size is introduced and also in that, we found that the combination of text in the image is much better.

So we have finally proposed a scheme for comparison of some famous combinations in cryptography and steganography and drawn out the results on the basis of their speed of encryption, embedding time and also shown how a double security layer can be added to the data being transmitted over any medium.

REFERENCES

[1] New Technique for Hiding Data in Audio File Mohammed Salem Atoum and Osamah Abdulgader Al- Rababah, Alaa Ismat Al-Attili

[2] On the Limits of Steganography Ross J. Anderson, Fabien A.P. Petitcolas

[3] Information Hiding—A Survey Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn

[4] New Technique for Hiding Data in Audio File Mohammed Salem Atoum † and Osamah Abdulgader Al- Rababah ††, Alaa Ismat Al-Attili†††

[5] D. Pan, "A tutorial on MPEG/Audio compression", IEEE Multimedia, 2(2), pp. 60-74, 1995.

[6] https://www.groovypost.com/howto/hide-text-inside-image-files

[7] C. Cachin (2005). "Digital Steganography", Encyclopedia of Cryptography and Security.

[8] DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation-Based Performance Analysis Jawahar Thakur1, Nagesh Kumar2

[9] Least Significant Bit algorithm for image steganography Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Institute of Technology, Bangalore, India

[10] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu "A Comparative Analysis of Image Steganography", International Journal of computer Applications, Vol2- No3, May 2010.

