SC402 Introduction to Cryptography
SC402

Project Report - Autumn 2022

Image Encryption using Paillier Homomorphic Encryption

Dhairya Somaiya (201901047),
Dharmik Patel (201901300),
Mohil Desai (201901301),
Fenil Kamdar (201901418)

supervised by
Manish Gupta

Abstract

With the increase in communication using images, it is necessary to store the images in server in an encrypted manner to prevent theft of user data in case of attacks. To solve this, we have implemented an image encryption and decryption system using Paillier Homomorphic Encryption. We have also analyzed the results obtained from test images.

Contents

1 Introduction

Due to the huge rise of social media platforms in recent years, messages containing text, audio, images and video are exchanged at an enormous rate between people everyday. To serve the purpose of privacy of the user's data, secure and efficient algorithms are needed to encrypt and decrypt the messages of people. Many people have come up with different cryptography algorithms which help in encrypting and decrypting different forms of media. In this report, we are going to discuss the encryption and decryption of images. To encrypt and decrypt images, various types of cryptography like DNA cryptography, symmetric cryptography and elliptic curve cryptography are used. These cryptosystems convert the original image to a form which cannot be decoded easily to ensure that no one can interpret the contents of the image. We will discuss how Paillier cryptosystem alongwith homomorphic encryption can be used to encrypt and decrypt images.

2 Problem Statement

With the rising popularity of image sharing and image editing services, huge number of images are uploaded on such sites everyday. The security of these sites and their servers cannot be trusted as the implementation details are hidden and attackers can access the servers containing the images of the user leading to leak of private data. Thus the objective is to implement a cryptosystem which will encrypt images before storing them on the server and will decrypt the image from server when the user requests the image.

3 Literature Review

Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. "Image encryption using elliptic curve cryptography." Procedia Computer Science 54 (2015): 472-481.

Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh have implemented an image encryption algorithm using elliptic curve cryptography. As performing operations of cryptography on every pixel of the image can be very computationally expensive and time consuming, they first create groups of the pixels of the image into a single integer. Then these integers are sent to the ECC system as a plain text message. The ECC system generates a cipher text for each group integer. The cipher texts are padded through a mechanism and a cipher image is obtained which is sent to the receiver. To obtain the group of pixels back during decryption, the values of the cipher image are scaled down to the 0-255 range by the decryption system after which the original image is obtained by the receiver. Their results show that the frequency of pixels in the cipher image is evenly distributed even if the plain images have varying frequency distribution of pixels. Thus the probability of each pixel in the cipher image getting mapped to a pixel in the original image will be almost equal.

M. Ashtiyani, P. M. Birgani and H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography," 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008, pp. 1-5, doi: 10.1109/ICTTA.2008.4530291. M. Ashtiyani, P. M. Birgani and H. M. Hosseini have implemented an image encryption system using chaos functions and symmetric cryptography. The encryption system first scrambles the pixels of the image by using chaotic mapping. The authors have used Cat Map Chaotic Mapping for this purpose. The pixels of the image are scrambled for n rounds in the first stage. Then the image is sent to the next stage where diffusion in the pixels takes place. This diffusion is performed with the help of the S-AES algorithm. Their results show that the histogram of frequency distribution of pixels in the original image, scrambled image and scrambled plus encrypted image differ highly which suggests that the image has been encrypted efficiently.

Manish Kumar, Akhlad Iqbal, Pranjal Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Processing, Volume 125, 2016, Pages 187-202, ISSN 0165-1684

Manish Kumar, Akhlad Iqbal, Pranjal Kumar have implemented an image encryption and decryption algorithm which uses DNA cryptography and elliptic curve Diffie-Hellman cryptography. For the encryption of the original image, the image is divided into three layers of RGB (Red, Green and Blue) and DNA sequence matrix is generated. Thereafter, DNA addition and scrambling is performed on the image pixels to introduce randomness between the pixel values. The layers of the image are then interleaved. In the next stage, the obtained image is passed to the ECDHE system and the resultant image is again interleaved in the final stage to obtain the final encrypted image.

O'Keeffe, Michael. "The paillier cryptosystem." Mathematics Department April 18

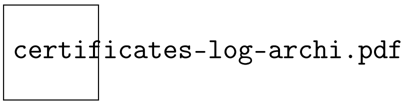

Figure 2: Try to guess what this figure illustrates; I double-dare you...

(2008): 1-16. The above mentioned paper gives us an idea on how the Paillier Cryptosystem works, briefs about some of its interesting properties and how this cryptosystem can be used by working on these properties. It discusses how the Carmichael's Theorem is useful in encryption and decryption of the Paillier system. Finally it discusses the multiplying property, how to change cipher text without the plain text, and property of powers. It gives us the corollary from which we find out how the three properties are related. Finally it takes a real life example of electronic voting and how the system is implemented using these properties.

4 Solution

The solution section covers all of your contributions (architecture, algorithms, formulas, findings). It explains in detail each contribution, if possible with figures/schematics.

Don't forget that a figure goes a long way towards helping your reader understand your work. For instance, Figure 1 outlines the layers involved in a distributed certification service, and how they articulate together. Nevertheless, a figure must always come with at least one paragraph of explanation. The rule is that anyone should be able to understand your solution from reading the text in this section, even if they skip the figures.

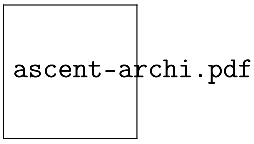

Figure 1: Architecture of our distributed certification service

Figure 2 is a pretty good example of a figure that is completely useless unless it is not accompanied by a textual explanation.

5 Results and Discussion

The results section details your metrics and experiments for the assessment of your solution. It then provides experimental validation for your approach with visual aids such as data tables and graphs. In particular, it allows you to compare your idea with other approaches you've tested, for example solutions you've mentioned in your related work section.

5.1 Experimentation protocol

It is of the utmost importance to describe how you came up with the measurements and results that support your evaluation.

5.2 Data tables

Every data table should be numbered, have a brief description as its title, and specify the units used.

As an example, Table 1 compares the average latencies of native application calls to networked services. The experiments were conducted on an Apple MacBook Air 2010 with a CPU speed of 1.4GHz and a bus speed of 800MHz. Each data point is a mean over 20 instances of each call, after discarding both the lowest and the highest measurement.

Network Applications		
Service	Protocol	Latency (ms)
DNS	UDP	13.65 ms
	TCP	0.01 ms
NTP	UDP	92.50 ms
SMTP	TCP	33.33 ms
HTTP	TCP	8.99 ms

Table 1: Comparison of latencies between services running on `localhost`.

5.3 Graphs

Graphs are often the most important information in your report; you should design and plot them with great care. A graph contains a lot of information in a short space. Graphs should be numbered and have a title. Their axes should be labelled, with the quantities and units specified. Make sure that individual data points (your measurements) stand out clearly. And of course, always associate your graph with text that explains your results, and outlines the conclusions you draw from these results.

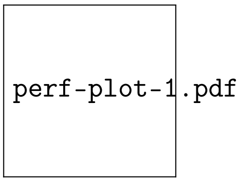

Figure 3: Probability of including [k] faulty/malicious nodes in the service

For example, Figure 3 compares the efficiency of three different service architectures in eliminating adversarial behaviors. Every data point gives the probability that k faulty/malicious nodes managed to participate in a computation that involves 32 nodes. In the absence of at least one reliable node ($k = 32$), the failure will go undetected ; but the results show that this case is extremely unlikely, regardless of the architecture. The most significant result pertains to $k = 16$: the reliable nodes detect the failure, but cannot reach a majority to recover. The graph shows that the `CORPS 5%` architecture is much more resilient than the `DHT 30%` architecture, by a magnitude of 10^{11}.

6 Discussion

The discussion section focuses on the main challenges/issues you had to overcome during the project. Outline what your approach does better than the ones you mentioned in your related work, and explain why. Do the same with issues where other solutions outperform your own. Are there limitations to your approach? If so, what would you recommend towards removing/mitigating them? Given the experience you've gathered working on this project, are there other approaches that you feel are worth exploring?

7 Conclusion

Give a clear, short, and informative summary of all your important results. Answer the initial question(s) or respond to what you wanted to do, as stated in your introduction. It can be a short table or a list, and possibly one or two short comments or explanations.

Target a reader who may not have time to read the whole report yet, but needs the results or the conclusions immediately. This is a typical situation in real life. Some readers will read your introduction and skip to your conclusion first, and read the whole report only later (if at all).

You may also draw perspectives. What's missing? In what directions could your work be extended?