Resúmenes de Abstracts e Introducciones

Christofer Fabián Chávez Carazas
Ruben Torres Lima
Universidad Nacional de San Agustín
Proyectos I

24 de abril de 2017

1. Resúmenes

1.1. (Paper 1) An Efficient Parallel Algorithm for Segured Data Communications Using RSA Public Key Cryptography Method

RSA en uno de los algoritmos basados en PKC(public-key pryptography) más importantes. Está basado en una técnica de factorización que da como resultado números muy grandes. Manejar esos números directamente en una infraestructura GCC es imposible. El paper propone un algoritmo paralelo para RSA, con el objetivo de poder manejar los números y las operaciones en la infraestructura GCC.

1.2. (Paper 2) A Novel Image Encryption Algorithm using AES and Visual Cryptography

El principal objetivo de la encriptación de imágenes es transmitir una imagen con seguridad por una red. Ya existen algoritmos que hacen esto, pero no aseguran la *key* o no son muy amigables con el hardware actual. El paper propone un algoritmo que asegura la key usada en AES convirtiéndola en una imagen y dividiéndola en n *shares* usando técnicas de *Visual Secret Sharing*.

1.3. (Paper 3) A New Technique for Color Share Generation using Visual Cryptography

La criptografía visual encripta la imagen en *shares* y la desencripta apilando todos los *shares* para revelar la imagen. En el paper proponen un esquema para generar *shares* con el color de la imagen utilizando los componentes R,G y B.

2. Análisis y Comparación de los Abstracts

2.1. Presentación del Problema

Los autores presentan el problema de maneras diferentes, algunos no lo hacen tan extenso, por ejemplo en el Paper 3 se presenta así:

Now a days, most of our data is travelled over internet so the security of that data is most important. Visual cryptography plays a very crucial role for security of image based secret.

y en el Paper 2 sólo son unas cuantas líneas:

With the current emergence of the Internet, there is a need to securely transfer images between systems.

Tal vez no se explayan en el problema aquí porque lo hacen en la introducción. En cambio, en el Paper 1 casi la mitad del abstract trata de exponer el problema:

Public-key infraestructure based cryptographic algorithms are usually considered as slower than their corresponding symetric key based algorithms due to their root in modular arithmetic [...] the sequential implementation of RSA becomes compute-intensive and takes a lot of time and energy to execute. Moreover, it is very difficult to perform intense modular computations on very large integers because of the limitation in size of basic data types available with GCC infraestructure.

Estos tres papers comienzan con esto. Nos cuentan cuál es el problema y las necesidades del área en done están trabajando para luego darnos una propuesta.

2.2. Propuesta

En esta parte los autores te presentan lo que han hecho. Alguno autores se echan flores y se explayan en su presentación, como en el Paper 1:

In this paper, we are looking into the possibility of improving the performance of proposed parallel RSA algorithm by using two different techniques, first implementing modular calculations on larger integers using GMP library and second by parallelizing it using OpenMP on the GCC infraestructure.

otros son más moderados, como en el Paper 2:

In this context, we propose a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image.

y otros sólo utilizan una línea para presentarlo, como en el Paper 3:

Here we are proposing a new scheme for color share generation.

pero luego explican un poco su propuesta para hacerla más interesante, como en el Paper 3:

In this scheme R, G and B component is extracted from color image then apply gray share generation algorithm on R component and make n number of R gray shares then all shares are combine with B and G component to make color shares.

o como en el Paper 2:

The image is encrypted using AES and an encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing.

Al ser esto parte del Abstract los autores no tienen mucho espacio para explayarse, eso sí se hace en la introducción, por eso las presentaciones de algunas propuestas no son muy amplias, pero aún así tienen que verse interesantes para poder enganchar al lector.

3. Análisis y comparación de las Introducciones

3.1. Contextualización

Todos los papers empiezan contextualizando al lector en el campo de investigación del autor. Introducen diciendo por qué es importante su tema, como en el Paper 3:

In today's world data security is very important because most of our data is travelled over internet. [...]

dan algunas aplicaciones, como en el Paper 2:

Image encryption has applications in many fields including Banking, Telecommunication and Medical Image Processing etc. [...]

y citan algunos trabajos en el área, como en el Paper 1 y el Papper 3:

One of the most important techniques is public-key cryptography (PKC) or asymetric cryptography which was invented by Whirfield Diffie, Martin Hellman [2] and Ralph Merkle [3] [...]

Research shows that using AES and Visual Cryptography to encrypt images is not entirely new. In [2], an encryption scheme has been proposed that splits the Image into R, G, and B components and encrypt them using AES.

No todos los papers tiene esto, por ejemplo, en el Paper 3 en ninguna parte de la introducción se citan trabajos pasados, porque la siguiente sección esta más centrada a eso. Otro ejemplo es el Paper 1, en donde no se menciona las aplicaciones del tema; tal vez porque ya son muy bien conocidas las aplicaciones del RSA. Pero sí todos nos cuentan cuál es la importancia de su trabajo.

3.2. Problema

Aquí los autores amplían un poco más el problema, no sólo describiéndolo sino también contando los problemas que tienen trabajos anteriores, como en el Paper 2:

Another interesting approach to encrypt image is using the chaotic theory based algorithms. [...] However, these are relatively newer algorithms and in certain systems where hardware encryption circuits for default algorithms like AES are built in, these kind of algorithms need an entirely new update of hardware.

En el Paper 1, el autor se toma un párrafo completo para explicar las complicaciones que tiene el RSA secuencial, y el por qué su trabajo es un aporte importante:

[...] it is imposible to work on such large numbers on GCC infraestructure directly.[...]

En el Paper 3 no se muestra muy claramente cuál es el problema, sólo nos vuelve a recalcar la importancia de su trabajo:

Visual cryptography plays a very important role for image security. In this technique image is encrypted in to number of shares and at decryption side all or some of the shares are overlapped with each other to reveal the secret image.

3.3. Propuesta

En el Paper 3, desde la mitad hasta casi el final da su propuesta y explica qué es lo que hace:

In this paper color image is taken as an input to the system then we extract the R, G, and B component from color image. After extraction phase gray share generation algorithms is applied on only R component and generate n number of R gray shares. [...]

El Paper 1 da su propuesta al final de la introducción, pero no lo hace de manera directa sino da a conocer la importancia de las tecnologías que va a usar para resolver el problema:

Recently, the use of OpenMP [6] on the GCC infraestructure for general purpose computing has been gaining widespread usage for parallelizing algorithms. [...]

El Paper 2 también da su propuesta al final de la introducción y sí lo hace de manera directa:

In this paper, we propose an algorithm that secures the key used in AES by converting key into an image and splitting it into n shares using Visual Secret Sharing techniques that is hardware friendly and offers backward compatibility.

4. Estructura del paper

El Paper 1 es el único que no presenta cómo esta estructurado su paper; los otros dos si contienen esta parte:
Paper 2:

The rest of the paper is organized as described. Section II gives basic information about AES and Visual Cryptography. Section III gives details about the proposed algorithm along.[...]

Paper 3:

Organization of this paper is as follow: Section II describes the related work in visual cryptography for color image.[...]