ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Error Calculation of Encrypted Images using Wavelength Compression

Mohammadi Arshiya
Assistant Professor
Computer science Department
India

Abstract: ***The aim of this paper is to ensure secure transfer of an image using cryptography. The implementation of the image cryptography uses the RSA algorithm. The original image is encrypted frame wise and the encrypted image is constructed according to the new encrypted values after the passing through RSA. It is then decrypted to achieve the original image. A compression technique is used to remove any noisy data and redundant value and reduce the size of the image for easy transmission. The final phase of the image includes comparison of the original image and the decrypted image and calculates error.***

Keywords: Cryptography; RSA algorithm; Image compression; Wavelet compression; Histogram; Gray scale Image.

I. INTRODUCTION

A. Cryptography

Cryptography comes from Greek words meaning “hidden writing”. Cryptography converts readable data or cleartext into encoded data called ciphertext. By definition cryptography is the science of hiding information so that unauthorized users cannot read it. Cryptography performs other critical security requirements for data including authentication, repudiation, confidentiality, and integrity.

There are two different basic encryption methods, they are

- Symmetric-key algorithms: These are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- Public-key cryptography: Also known as asymmetric cryptography is a class of cryptographic algorithms which require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

B. Image Processing

An image may be defined as a two-dimensional function, f(x,y), where x and y are spatial(plane) coordinates, and the amplitude of f at any pair of coordinates (x,y) is called the intensity of gray level of the image at that point. When x,y, and the intensity values of f are all finite, discrete quantities, we call the image a digital image. Pixel is the term used most widely to denote the elements of a Digital image.

The fundamental steps of image processing are Image Acquisition, Image enhancement, Image restoration, Image Compression, Morphological processing, Image Segmentation, Representation and Recognition.

C. Image compression

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. Lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless.

II. IMPLEMENTATION DETAIL

A. *Block diagram*

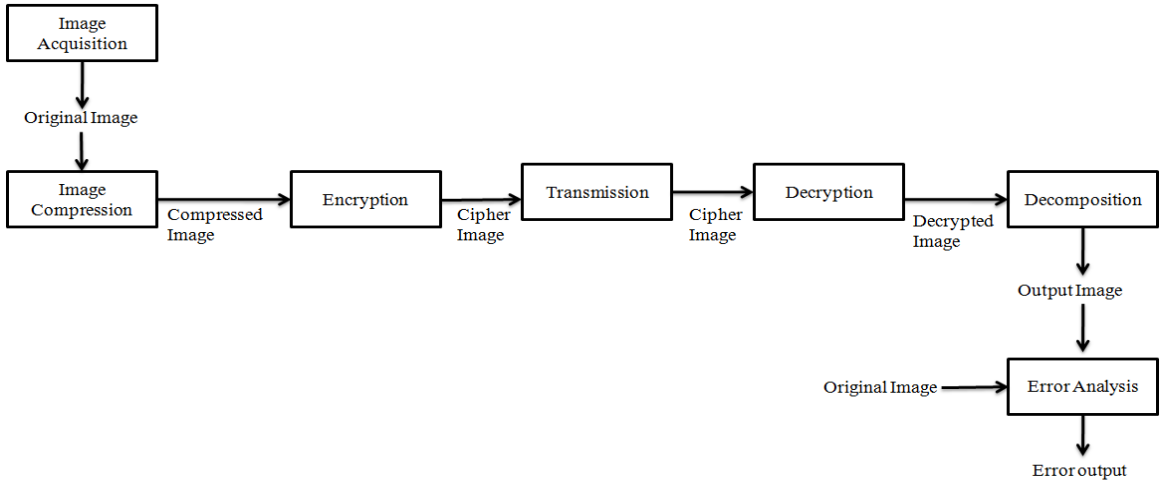


Fig: Block Diagram

B. *Development of RSA program*

The RSA algorithm involves three steps: key generation, encryption and decryption.

Encryption: $c = m^e \pmod n$

Decryption: $m = c^d \pmod n$

Where *m* is the plaintext, *c* is the cipher text, *e* is the public key and *d* is the private key.

Once the RSA algorithm is developed for accepting strings, it has to be modified to except an image. It is already known that an image comprises of pixels, which are the smallest unit of an image. Each pixel corresponds to a pixel value which ranges from 0 – 255.

Each pixel from the original image is taken and passed through the encryption. The value thrown out of this function is plotted in a new matrix at the same position from where it is retrieved in the original image. This way the entire image is constructed frame wise giving a scrambled or distorted image. The decryption of the encrypted image is the reverse process where each pixel is chosen and passed through the same function but with a different key. This leads back to the construction of the original image.

C. *Compression technique*

Compression is used in this program to reduce the size of image and also to remove any noisy and redundant data. This way the encryption of the image is faster and transmission of the image is easier. The compression technique used here is wavelet compression. Initially it calculates the four filters associated with the orthogonal and biorthogonal wavelet. Then the wavelet decomposition of the matrix is calculated, after which the image is compressed. The decomposition level of the image must be given by the user and ranges between 1 – 3.

Once the compression is complete the coefficients of the image are generated which are transmitted and on the receiver end the image is reconstructed.

III. Error Calculation

Error is calculated by taking the difference of the original image and the decompressed image. The error is depicted using an image. Two cases have been used, first an image encryption and decryption without compression and the same with a compression. Both the cases are compared to understand which displays better results.

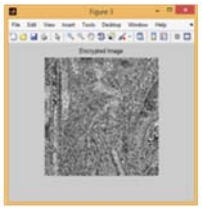
A. Output of an image without compression

The original image is converted to grayscale image and then encrypted pixel wise by using RSA algorithm. The encrypted image is then decrypted by using RSA algorithm and then the original image and decrypted image are compared by histograms of the images.

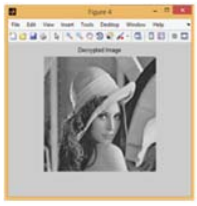
Original Image

Grayscale Image

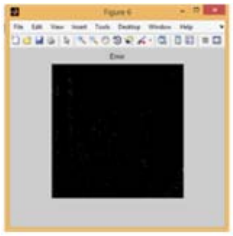
Encrypted Image



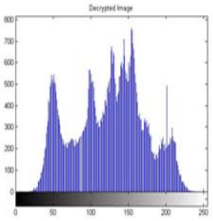
Decrypted Image



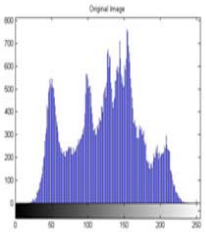
Error Calculation



Histogram of Decrypted Image



Histogram of Original Image



The results displayed above are for .jpeg format. Similar results were obtained for .png and .bmp

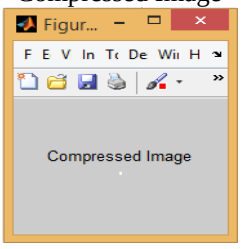
As noticed, the algorithm produces errors which may be due to noise in the image or any redundant values. For this purpose the image must be transformed before being encrypted.

B. Output of an image after applying compression

Original Image

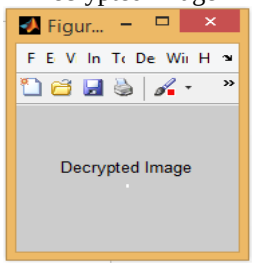
Grayscale Image

Compressed Image



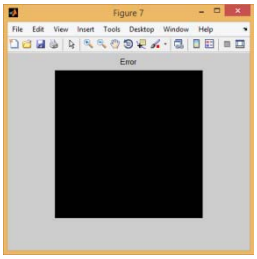
Encrypted Image

Decrypted Image

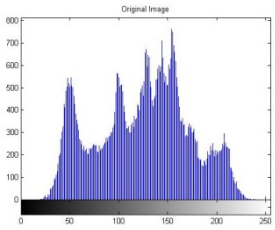


Decompressed Image

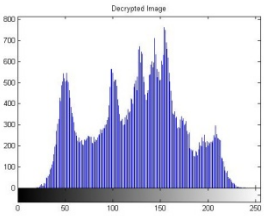
Error Calculation



Histogram of Original Image



Histogram of Decrypted Image



After compressing the image, the size of the image reduces considerably and all the noise and redundant values are lost. Thus encryption and decryption of image successfully achieved and the reconstruction of the image is error free.

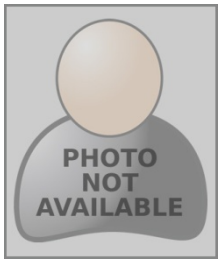
IV. Conclusion

This paper is a combination of two widely researched fields, cryptography and image processing. It is designed to communicate an image securely from one destination to another. The encryption algorithm used here is already a very secure algorithm but has been modified to suite the needs of the image. The reason for choosing a secure algorithm is that the third party should not be able to decipher the image. Under such circumstances algorithms such as AES or RSA is an excellent choice as they are highly secure and cannot be decrypted easily. Certain enhancements need to be done to the image before passing it to the algorithm.

References

1. S. M. Metev Samoud Ali, CherifAdnen, “RSA algorithm implementation for medical image ciphering” International Journal of Computers and Electronics Research [Volume 1, Issue 2, August 2012] ISSN: 2278-5795.
2. Manoj B., Manjula N Harihar, “Image Encryption and Decryption using AES” International Journal of Engineering and Advanced Technology ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
3. Rafael C. Gonzalez, Richard E. Woods, “Digital Image Processing” Third Edition Pearson Education International.
4. William Stallings, “Cryptography and Network Security, Principles and Practice” Fifth Edition.

Author(s) Profile



Mohammadi Arshiya, received the M.Tech degree in computer science from JNTU Hyderabad. Worked as Assistant Professor in Mother Theressa College of Engineering and Technology affiliates to JNTU Hyderabad, India for four years. Worked as Assistant professor in Core International studies of higher education - BITS offshore campus in RAK, UAE for 1 year.

