Grid-based Image Encryption using RSA

Binay Kumar Singh
Department of Computer Science and Engineering
Indian Institute of Technology
Dhanbad-826004, India

Sudhir Kumar Gupta
Department of Computer Science
Keshav Mahavidyalaya, University of Delhi
New Delhi-110032, India

ABSTRACT

In recent years, security of several kinds of images is a major issue in secure data communication over any unreliable network. In this paper, a new technique to secure images by using grid-based encryption and decryption approach with RSA cryptosystem has been devised. This approach has taken original image, performed block transformation followed by grid transformation, then finally a public key cryptosystem is applied pixel-by-pixel to secure image. Experimental images have been taken and performed encryption and decryption to elaborate this technique. Error analysis shows that the technique is robust.

General Terms

RSA cryptosystem, Image Encryption, Image Decryption et. al.

Keywords

Block Shuffling, Grid Shuffling, Grid-Based Encryption (GBE), Grid-Based Decryption (GBD).

1. INTRODUCTION

In image data communication, researchers and scientists are facing tremendous challenges for transmission of image data securely and safely. Image data are of significant uses in various areas, such as- banking and finance, military services, medical services, telecommunication, governmental services, etc. When communication networks are heavily unsecure from hackers and intruders then it is inevitable to find ways to transmit data securely. In order to do this, we have proposed a unique technique which allows users to use the concept of grid-based encryption (GBE) with RSA cryptosystem and grid-based decryption (GBD) to transmit images. Although, several techniques have been proposed for encryption and decryption of images, this technique advances in terms of applying level-by-level initial encryption and decryption, before using any basic cryptosystem [1-3].

2. ORGANIZATION OF THE PAPER

This paper is organized in the following order: Section 3 discusses about previous work done on image encryption and decryption. In the same section, RSA cryptosystem and its usability over image encryption and decryption have been covered. Section 4 demonstrates in detail this proposed technique and how image encryption from block shuffling, grid shuffling, pixel shuffling have been chronologically done in encryption and decryption. And, finally after encryption, how decryption of image on receiver end has been performed to receive original image. Our section 5 deals in statistical analysis of the proposed technique by presenting histogram of original, encrypted, and decrypted image. Conclusion of the proposed technique is given in section 6 with future work could be implemented on audio and video encryption and decryption. This section 7 contains referenced materials in terms of books, and research papers which have been studied in the entire duration of research to get insight understanding and develop knowledge to propose this technique in a varied way.

3. RSA CRYPTOSYSTEM AND IMAGE ENCRYPTION

3.1 RSA Cryptosystem

All cryptographic techniques are broadly classified into two categories: symmetric- key cryptography and asymmetric –key cryptography [4, 5]. The main difference between these two cryptosystem is in terms of the type of key they use for encryption and decryption process. Encryption process is performed on sender side to encrypt the message or plain text (that could be in any format, like- text, image, audio, and video) [6]. This encrypted message is in an unreadable format (this unreadable format or also known as cipher text is used for transmission from sender to receiver in the data communication), whereas decryption process, reverse of encryption process, done on receiver side to decrypt received cipher text to get original message.

In symmetric-key cryptography, only one key is used for both encryption and decryption technique [7-9]. This one key is known as private key. When only one key is used to perform encryption and decryption process, then chances are high that a message could be easily decrypted. But this demerit does not necessitate to avoid it totally, this cryptography, because of its hidden efficiency in it.

In asymmetric -key cryptography, two keys- one private key and another public key is used for encryption and decryption process. This gives more security and feasibility over symmetric -key cryptography. In this case, public key is used for encryption of message and private key is used for decryption of message. Asymmetric-key cryptography is based on complex mathematical concepts, where it is computationally infeasible to find the correct private key of the receiver to decrypt the message correctly, although, public key could be known to everyone. There are several types of attacks still possible on this cryptography, but all these attacks are inexpensive in terms of disclosing the cipher text.

RSA cryptosystem is one of the asymmetric-key cryptography, which based its technique on some mathematical concepts, is robust in terms of, by making it computationally infeasible, inflexible, and inexpensive to find private key, public key pair in a timely manner [10]. Although, some attacks are possible on this cryptosystem, but this does not in any way lessening its usability and profitability [11, 12].

3.2 Image Encryption and Decryption using RSA

In basic RSA cryptosystem, only text data are encrypted and decrypted [13]. Initially, this approach takes an image or frame divides it into multiple blocks of equal sizes (first level division) and shuffle each and every block in the same level. Our below given equation (i) depicts it more clearly.

$$frame = \sum_{l=0}^{l=N} \sum_{m=0}^{m=N} B_{lm};$$
$$where, B = Block\ of\ an\ image ....(i)$$

In equation (ii), first block of partially encrypted image (of first level division) has been taken and further divided it into multiple grids (second level division). Grids are further shuffled.

$$B_{11} = \sum_{n=0}^{n=M} \sum_{r=0}^{r=M} G_{nr};$$
$$where, G = grid\ of\ a\ block ....(ii)$$

The second level division of partially encrypted image or also known as grid -based division is further taken into pixels, which is derived in equation (iii). At the same level, shuffling is again performed.

$$G_{11} = \sum_{x=0}^{x=K} \sum_{y=0}^{y=K} p_{xy};$$
$$where,\ p = pixel\ in\ a\ grid ....(iii)$$

Final encryption of any partially encrypted image is done in equation (iv). In this equation, this approach encrypted the entire partially encrypted image from multiple levels. Here, we use RSA cryptosystem for final encryption to get encrypted pixels.

$$p_{ij} \rightarrow p'_{ij};$$
$$where,\ p_{ij} = original\ image\ pixel,$$
$$p'_{ij} = encrypted\ image\ pixel ....(iv)$$

This entire procedure of encryption from several levels is given in below Fig. (1).

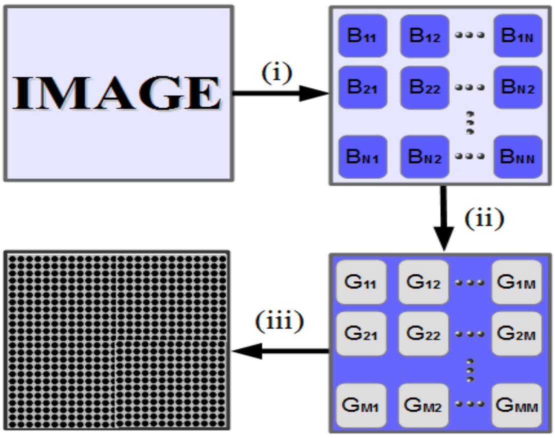

Fig 1: (i) Before encryption original image is divided into several blocks, each one of equal size and shuffled in a pre -specified way; (ii) It represents how one block is further divided into multiple grids, of equal size and shuffled in a specified manner; (iii) Finally, inside gird pixels are shuffled and encrypted using RSA cryptosystem.

After encrypting the image pixel by pixel, transmission of encrypted image will be done.

When it is received by the receiver, receiver performs the entire operation in reverse order, i.e. it considered the encrypted image nothing but group of pixels.

First, each pixel is decrypted using RSA cryptosystem, which is derived in equation (v). In the same equation, it is shown that how each pixel for further level –wise operation has been done.

$$p'_{ij} \rightarrow p_{ij};$$
$$where,\ p'_{ij} = encrypted\ image\ pixel,$$
$$p_{ij} = decrypted\ image\ pixel ....(v)$$

In equation (vi), partially decrypted image pixels are rearranged to create grids of equal sizes.

$$G_{11} = \sum_{x=0}^{x=K} \sum_{y=0}^{y=K} p_{xy};$$
$$where,\ p = decrypted\ \ pixel\ in\ a\ grid\ ....(vi)$$

Below given equation (vii) describes how GBE is finalized into a particular block.

$$B_{11} = \sum_{n=0}^{n=M} \sum_{r=0}^{r=M} G_{nr};$$
$$where, G = decrypted\ grid\ in\ a\ block ....(vii)$$

The below given equation (viii) depicts how blocks which are combined from grids are grouped together to form the original image. This means that now the receiver is able to receive the original image correctly.

$$frame = \sum_{l=0}^{l=N} \sum_{m=0}^{m=N} B_{lm};$$
$$where, B = decrypted\ block\ in\ an\ image..........(viii)$$

In the below given Fig. (2), it has been shown that how grids from pixels have been formed, then grids are reshuffled to get original block. In the next iteration, how blocks are originated and reshuffled to get the original image or frame.

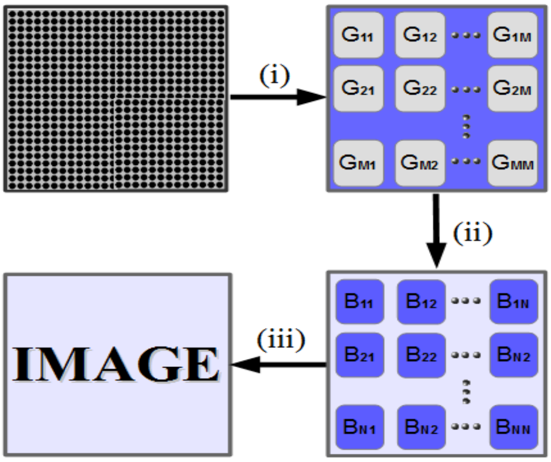

Fig 2: (i) On receiver side, decryption of encrypted image is done by RSA then pixels are rearranged; (ii) Here, pixels are reshuffled to get the original order of the grid; (iii) At last, blocks are rearranged to get the original image.

4. PROPOSED GRID BASED IMAGE ENCRYPTION AND DECRYPTION TECHNIQUE USING RSA CRYPTOSYSTEM

4.1 Proposed Encryption Technique

In this paper, the encryption technique is a step-by-step procedure which is given below.

Step 1: Divide original image into a number of blocks each of equal sizes:

```
    Step 1.1: for each block do
        Shuffle: $B_{00} \rightarrow B_{MM}; B_{01} \rightarrow B_{M-1M}$ and so on;
                 for every $B_{nr}$; where $n = 0...M, r = 0...M$;
        Step 1.2: for each grid do
            Shuffle: $G_{00} \rightarrow G_{KK}; G_{01} \rightarrow G_{K-1K}$ and so on;
                     for every $G_{xy}$; where $x = 0...K, y = 0...K$;
            Step 1.3: for each pixel do
                Shuffle: $P_{00} \rightarrow P_{LL}; P_{01} \rightarrow P_{L-1L}$ and so on;
                         for every $P_{lm}$; where $l = 0...L, m = 0...L$;
            end for
        end for
    end for
```

Step2: Encrypt each pixel p_{ij} from RSA cryptosystem, i.e.; $p_{ij} \rightarrow p'_{ij}$.

Step3: Group all P_{LL}. Stop *Step 1.3.*

Step4: Group all G_{KK} Stop *Step 1.2.*

Step5: Group all B_{MM}. Stop *Step 1.1.*

4.2 Proposed Decryption Technique

Decryption process also is also a step-by-step process which is presented below.

Step 1: Decrypt each pixel using RSA cryptosystem $p'_{ij} \rightarrow p_{ij}$.

Step 2: Take group of pixels. Combine into a grid.

```
    Step2.1: for each pixel in a grid do
        Re-shuffle:
        $B_{MM} \rightarrow B_{00}; B_{M-1M} \rightarrow B_{01}$ and so on;
        for every $B_{nr}$; where $n = M...0, r = M...0$;
        Step 2.2: for each grid in a block do
            Re-shuffle:
            $G_{KK} \rightarrow G_{00}; G_{K-1K} \rightarrow G_{01}$ and so on;
            for every $G_{xy}$; where $x = K...0, y = K...0$;
            Step 2.3: for block in an image do
                Re-shuffle:
                $P_{LL} \rightarrow P_{00}; P_{L-1L} \rightarrow P_{01}$ and so on;
                for every $P_{lm}$; where $l = L...0, m = L...0$;
            end for
        end for
    end for
```

Step3: Group all P_{LL}. Stop *Step 2.3.*

Step4: Group all G_{KK} Stop *Step 2.2.*

Step5: Group all B_{MM}. Stop *Step 2.1.*

From this proposed technique, original image, encrypted image, and decrypted image is presented in figure 3(i), figure 3(ii), and figure 3(iii), respectively.

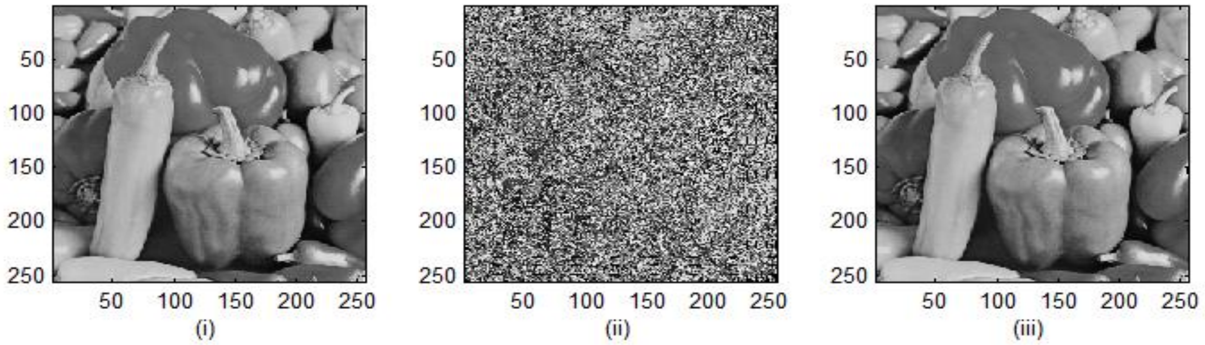

Fig 3: (i) Original image of pepper in pixel size 256×256; (ii) Final encrypted image of pepper using this proposed approach; (iii) Decrypted image.

5. STATISTICAL ANALYSIS

A part of data analytics known as statistical analysis is used for analyzing and creating relationship among data [14]. In this case, to find the robustness of the proposed model it has been used and correspondingly, histogram of images has been carried out.

5.1 Histogram Analysis

Histogram of an image depicts the intensity values of image pixels. It is a graph which shows how number of pixels is dispersed in an image at several intensity levels in an image. In other words, it gives estimation for the density of image pixels.

5.1.1 Histogram of Original Image

In figure 4(i), histogram of original image has been shown. In this histogram, the density of pixel is shown corresponding to the original image.

5.1.2 Histogram of Encrypted Image

Figure 4(ii) presented below depicts decrypted image histogram. Here, this histogram is totally different from the original image histogram of figure 4(i). This says that decrypted image in any case is not same as encrypted image.

5.1.3 Histogram of Decrypted Image

Below given figure 4(iii) represents histogram of decrypted image. From this histogram one can say that the original image histogram is same as decrypted image histogram. This means that the original image is completely recovered from the encrypted image.

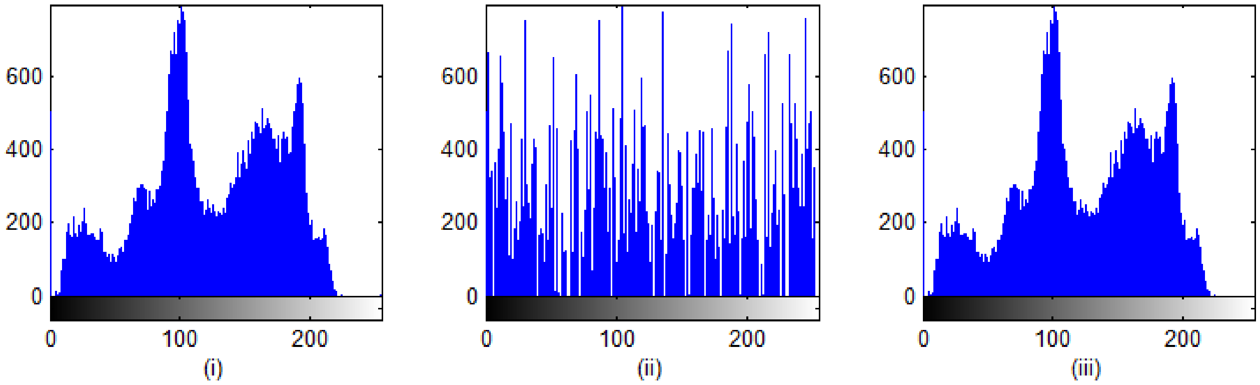

Fig 4: (i) Histogram of original image; (ii) Histogram of encrypted image; (iii) Histogram of decrypted image.

6. CONCLUSION

This paper presented an approach for encryption and decryption of images. Here, encryption of an image is done on several levels- blocks, grids, and finally pixels. Herein, these level–wise encryption needs shuffling of images in some pre-specified manner. Due to this level- wise division, it could be considered in some way symmetric encryption followed by asymmetric encryption. The division of levels generates more robustness of encryption. Then after, usual RSA cryptosystem is applied to encrypt the image. Part of decryption process is working in reverse order.

This paper future work can include applying of other asymmetric cryptosystem and in the case of division of images any symmetric cryptosystem. Additionally, it can be applied on audio and video encryption and decryption.

7. REFERENCES

[1] Biryukov A., Kushilevitz E. Proceedings of CRYPTO’98, 1462:72-88, 1998. From differential cryptanalysis to cipher-only attacks.

[2] Rivest R., Shamir A., Adleman L. Communications of the ACM, Feb 1978. A method for obtaining digital signatures and public key cryptosystems.

[3] Lamba C.S., Second International Conference on Communication Software and Networks, 2010. Design and Analysis of Stream Cipher for Network Security.

[4] Lian, Shiguo. CRC Press, 2008. Multimedia Content Encryption: Algorithms and Application.

[5] Stallings W. 4th edition, Pearson Education Inc, 2006. Cryptography and Network Security Principles and Practices.

[6] Ding, W. and Marchionini, G. 1997. A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[7] C. Kaufman, R. Perlman, M. Speciner. Prentice Hall 1995. Network security.

[8] Rivest, Ronald L. Shmir A. Len A. MIT Laboratory for Computer Science Technical Memorandum 82 (April 1977). On Digital Signatures and Public Key Cryptosystems.

[9] Flinn, Patrick J. and Jordan, James M. Alston & Bird LLP, July 9, 1997. Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?

[10] Juneja Mamta, Sandhu Parvinder S. International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009. Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption.

[11] Paar Christof, Pelzl Jan. ISBN 978-3-642-04100-6, Springer, 2010. Understanding Cryptography.

[12] Furht Borko, Kirovski Darko. ISBN: 0-8493-7212-7, 2006. Multimedia Encryption and Authentication Techniques and Applications.

[13] Katz Jonathan, Lindell Yehuda. ISBN: 978-1-58488-551-1, 2008.Introduction to Modern Cryptography: Principles and Protocols.

[14] Hoffstein Jeffrey, Pipher Jill, Silverman Joseph H. ISBN: 978-0-387-77993-5, 2008. An Introduction to Mathematical Cryptography.