IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

Impact of Attacks on Permutation Only Image Encryption Scheme

Snehal Bharat Ambare
G.H. Raisoni College of Engineering and Management, Ahmednagar
ambare.snehal@gmail.com

Abstract: Permutation is a commonly used primitive in multi- media (image/video) encryption schemes, and many permutation-only algorithms have been proposed in recent years for the protection of multimedia data. In permutation-only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is built by splitting and shuffling the part of the image. The literature on the cryptanalysis of image ciphers indicates that permutation-only image ciphers are insecure against ciphertext-only attacks and/or known/chosen- plaintext attacks. However, previous studies have not been able to ensure the correct retrieval of the complete plaintext elements. In this paper, we re-visited the previous works on cryptanalysis of permutation-only image encryption schemes and made the cryptanalysis work on chosen-plaintext attacks complete and more efficient. We proved that in all permutation-only image ciphers, regardless of the cipher structure, the correct permutation mapping is recovered completely by a making multiple combinations of two encrypted images. To the best of our knowledge, for the first time, this paper gives a combination attack that completely determines the correct plaintext elements using a deterministic method. Also, the detection of a hacker at admin side with the help of IP detection and blocking system is to be done in this system for future prevention of permutation attack.

Keywords: Chosen-plaintext Attack, Cryptanalysis, Image Encryption, Permutation.

I. INTRODUCTION

The fast growing demand for digital multimedia applications has opened up a telephone number of challenges regarding the confidentiality of images and videos in many multimedia based services, such as Pay-Video, remote control video conferencing, and medical imaging. Reliable storage and secure transmission of visual content are a legitimate concern of Intellect Property (IP) owners. Thus, there is a strong need to protect images and videos against unauthorized use or other security measure violations. Encryption is a solvent to maintain confidentiality. Multimedia Encryption obfuscates the image/video data stream to ensure secure transmission of image/video data between two companies over a public distribution channel. Given the fact that raw picture data is constructed by an episode of still simulacrum (frame of reference), image encryption techniques can be applied to still images or a single frame of reference in a video. Despite the advantages of permutation, it has a number of inherent limitations. Permutation only ciphers disclose some essential characteristics of the plaintext, such as the frequency distribution of symbols in the plaintext. Also, when the size of plaintext is small, that is, the number of possible arrangements for the plaintext elements is less than the key space, the number of effective keys can be reduced, and hence, the permutation mapping can be disclosed. Moreover, permutation-only encryption/decryption are not simple sequential operations that can be done dynamically The security of permutation-only image encryption schemes has been studied for a long time, and it has been shown that most of such schemes are insecure against cipher text-only attacks and/or known/chosen-plaintext attacks, which is due to the high information redundancy in the multimedia data and some specific weaknesses in the encryption algorithms. This paper presents a cryptanalysis which breaks most (if not all) permutation-only multimedia ciphers. In fact, it is shown that all permutation-only image ciphers are completely broken by chosen-plaintext attacks and no better pseudorandom permutation mapping can be realized to offer a higher level of security against chosen-plaintext attacks.

II. RELATED WORK

X. Zhang, Y. Ren, L. Shen, Z. Qian and G. Feng In this newspaper propose a novel outline of compression AES encrypted pictures. The content owner encrypts the originally uncompressed simulacrums by double encryption methods. Then, the communication channel provider who cannot memory access the original content may compress the encrypted images by a quantization method with optimal parameters.
At the receiver side, the principle image content can be reconstructed using the compressed encrypted image and the secret samara. Experimental result appearance the ratio-distortion performance of the proposed scheme is better than that of previous technique. [1]

J.Zhou, X.Liu, O.C.Au and Y.Y.Tang, The proposed persona encryption scheme operated in the prediction erroneousness domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic cryptography -based approach path can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only slightly worse, in terms of compression efficiency, than the body politic -of-the-artistic production lossless/lossy image programmer, which take original, unencrypted images as inputs. In contrast, most of the existing ETC answer induce significant penalty on the compression efficiency. [2]

A.Pande, J. Zambreno, The proposed algorithms ensure a considerable grade of security for low-power embedded systems such as portable video player and surveillance cameras. These schemes have zero or little compaction losses and conserve the desired properties of compressed data in the encrypted bit stream to ensure secure and scalable transmission of videos over heterogeneous networks.[3]

Z. Galias and W. Tucker, The interrogation of the coexisting draw for the Henon map is studied numerically by performing an exhaustive search in the argument place. As a result, several parameter values for which more than two attracted coexist are found. Using tools from interval analysis, we show rigorously that the attractors exist. In the eccentric of periodic orbits, we verify that they are stable, and thus proper sinks. Regions of existence in parameter space of the found sinks are located using a protraction method acting; the basins of attraction are found numerically.[4]

S. Li The proposed intent is actually an encryption configuration that can work with any watercourse caught or cube cipher. Compared with the previously proposed schemes, the new design provides more useful features, such as strict sizing -saving, on-the-fly encryption and multiple perceptibility, which make it possible to support more applications with different requirement. In addition, four different measures are suggested to provide better security against known/chosen-plaintext attacks. [5]

Sk. Md. Mizanur Rahman, M.A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto In this report, we first recap recent Privacy Enabling Technologies (Dearie). Later, we discuss pertinent evaluation criteria for effective privacy protection. We then put forward a model to assess the capacity of Favorite solvent to hide distinguishing facial information and to conceal identity operator. Comprehensive and rigorous experiments were conducted to evaluate the performance of face recognition algorithms applied to icon altered by PET. Results show the ineffectiveness of PET such as pixelization and blur. Conversely, they demonstrate the effectiveness of more sophisticated scrambling techniques to transparency face recognition [6]

III.SOFTWARE REQUIREMENT SPECIFICATION

1. Java 8.
    - jdk-8u121-windows-x64.exe.
2. Eclipse Java EE IDE for Web Developers.
    - Version - Mars 2
3. Database: mysql-5.1.54 mysql-connector-java-5.1.8-bin.jar.

IV.PROPOSED SYSTEM

The architecture diagram of the system shown below helps us to understand the system. The primary focus of this work is to get ip address of hacker and block IP Address of hacker. This system proves that permutation only image ciphers are completely broken against chosen plaintext attacks.

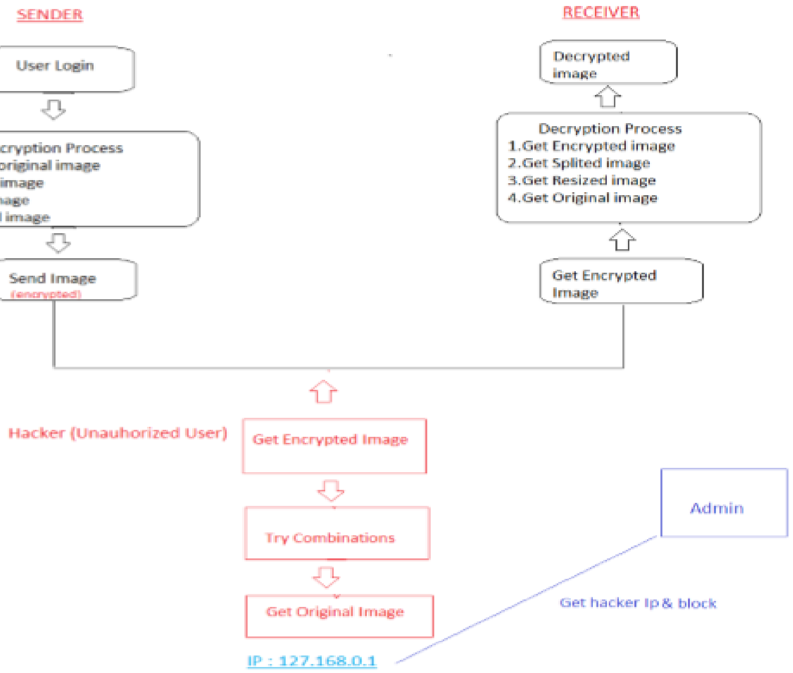


Fig. 1 System Architecture

A. Parameters of Image Encryption

Tune-ability: The dynamic definition of the encryption parameters and the encrypted part according to various requirements and applications. Static definition of the encrypted part and encrypted parameters helps in scalability for schemes usage.
Cryptographic Security: This defines to know the security of encryption scheme against the plaintext attacks and brute force; and the security is measured as high, medium or low.
Speed: This defines the faster time for encryption and decryption processing of algorithms.
Encryption Ratio: This helps in the measurement of encrypted data, and encryption ratio needs to be minimized to reduce or avoid computational complexity.
Format Compliance: The encrypted bitstream needs to be work with the compressor, while standard decoder needs to be work for decode the encrypted bit stream not with decryption.
Compression: This helps in maintaining the bandwidth of the image while transmission and also helps during the decryption.
Visual Degradation (VD): This helps in the measurement of the image data perceptual distortion according to with plain image

B. Image Encryption

The technology advancement helps in data, image, and video transmission over the internet. Every image data type will have the different type of aspect hence different security techniques need to adapt in the image transmission. The security solution is encryption which provides end to end transmission securely. The process starts with the taking an input image from the storage and then any encryption technique is applied to the image. After the encryption, the image is compressed for transmission purpose. In next process, the image is forwarded and collected as Cipher image and then decompressed to perform the decryption. The decryption techniques are applied to get the output image.

C. Permutation in Image Encryption

Due to the grid structure of digital images, image encryption methods utilize three different types of operations: position permutation, value transformation, and the combination form. Among different operations, permutation (transposition) is commonly used primitive in many image encryption schemes. This is mainly due to the easy implementation and applicability of permutation in both spatial and frequency domains. In addition, by combining permutation with other simple value transformation operations, such as XOR, a highly secure multimedia encryption scheme can be achieved. In all the well-known permutation-only ciphers, image entries (or bit-planes) are permuted by a mapping matrix which is built by a pseudo-random number generator. From the design point of view, permutation dissipates the statistical structure of the plaintext into long range statistics and it is suitable for fast processing requirements of massive digital multimedia data.

D. Attack on Permutation encrypted image

A cryptanalysis which breaks most (if not all) permutation-only multimedia ciphers. The Permutation-only image ciphers are completely broken by chosen-plaintext attacks and no better pseudorandom permutation mapping can be realized to offer a higher level of security against chosen-plaintext attacks.

V. PERMUTATION ONLY IMAGE CIPHERS

A. Algorithm 1: Encryption Process

step 1: Start

step 2: Select Image

```
    JFileChooser jfc = new JFileChooser (FileSystemView.getFileSystemView().getHomeDirectory());
```

step 3: Show Original Image

```
    img = ImageIO.read(new File(path));
    Icon ic=new ImageIcon(img);
```

step 4: Resize image

```
     resize(inputImagePath, outputImagePath, scaledWidth, scaledHeight);
```

step 5: Split Image

```
      BufferedImage imgs[] = new BufferedImage[chunks]; //Image array to hold image chunks
      for (int x = 0; x < rows; x++) {
      for (int y = 0; y < cols; y++) {
      imgs[count] = new BufferedImage(chunkWidth, chunkHeight, image.getType());
      Graphics2D gr = imgs[count++].createGraphics();
      gr.drawImage(image, 0, 0, chunkWidth, chunkHeight, chunkWidth * y, chunkHeight * x, chunkWidth * y + chunkWidth,
      chunkHeight * x + chunkHeight, null);               gr.dispose();           } }
```

step 6: Shuffel Image by changing postions of splited image using following sequence String

```
     seq[]=new String[]{"1","5","2","7","4","6","8","0","3"};
```

step 7: Stop

B. Algorithm 2: Decryption Process

step 1 : Start

step 2: Select Encrypted Image

```
    JFileChooser jfc = new JFileChooser (FileSystemView.getFileSystemView().getHomeDirectory());
```

step 3: Split image

```
      BufferedImage imgs[] = new BufferedImage[chunks]; //Image array to hold image chunks
    for (int x = 0; x < rows; x++) {
    for (int y = 0; y < cols; y++) {
    imgs[count] = new BufferedImage(chunkWidth, chunkHeight, image.getType());
    Graphics2D gr = imgs[count++].createGraphics();
    gr.drawImage(image, 0, 0, chunkWidth, chunkHeight, chunkWidth * y, chunkHeight * x, chunkWidth * y + chunkWidth,
    chunkHeight * x + chunkHeight, null);
    gr.dispose();           }       }
```

step 4: Get Resized Image by changing postions of splited image using following sequence

```
    String seq[]=new String[]{"1","5","2","7","4","6","8","0","3"};
```

step 5: Show Decrypted Image

```
    img = ImageIO.read(new File(path));
    Icon ic=new ImageIcon(img);
```

step 6: Stop

VI. EXPERIMENTAL RESULT

According to the proposed system the permutation mapping of the image ciphers which were performed in this section.

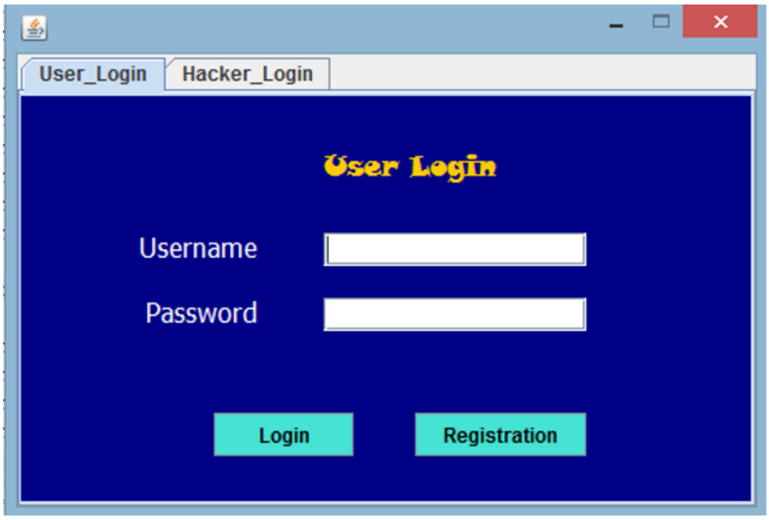
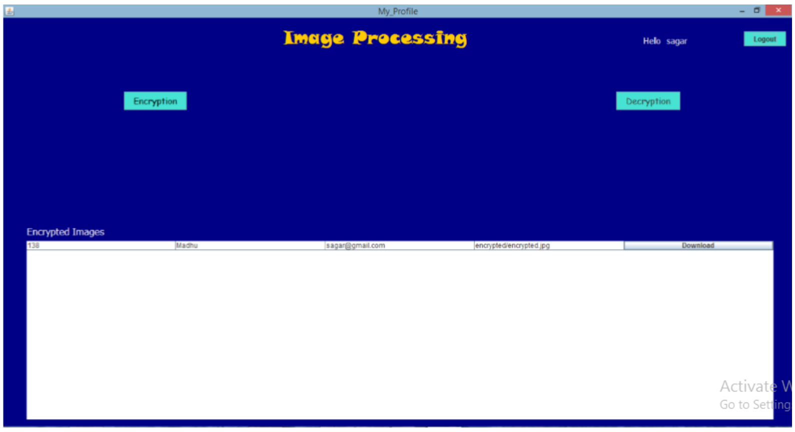


Fig. 2 User Login Page



138	Madhu	sagar@gmail.com	encrypted/encrypted.jpg	Download

Fig. 3 User Dashboard

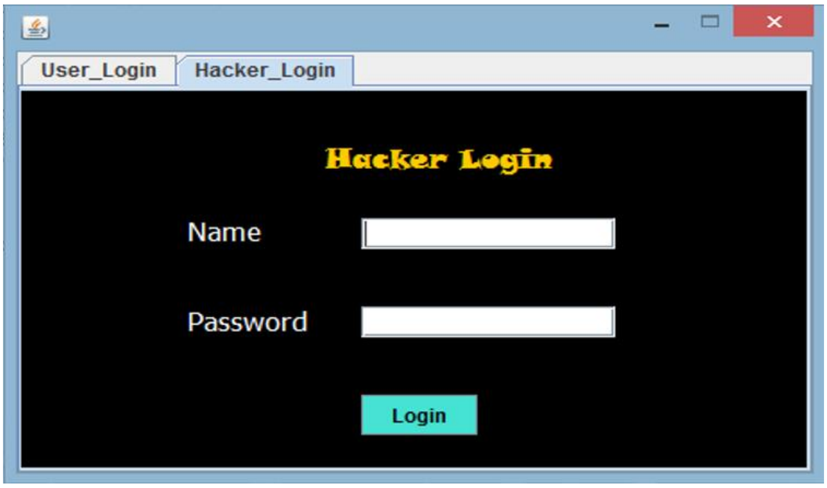
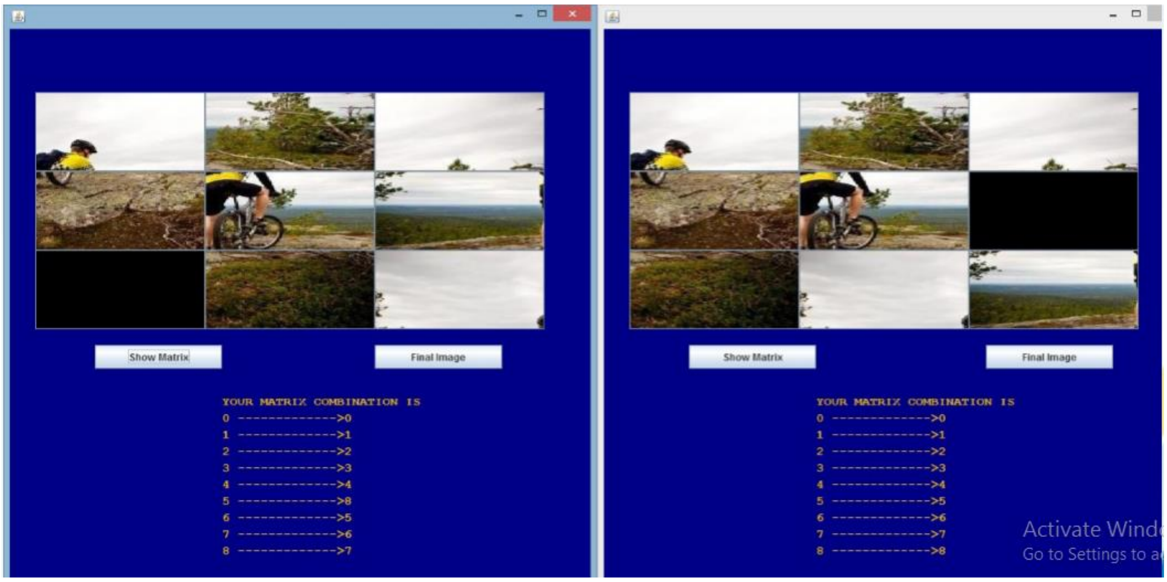


Fig.4 Hacker Login Page



```
YOUR MATRIX COMBINATION IS
0 -------------->0
1 -------------->1
2 -------------->2
3 -------------->3
4 -------------->4
5 -------------->8
6 -------------->5
7 -------------->6
8 -------------->7
```

```
YOUR MATRIX COMBINATION IS
0 -------------->0
1 -------------->1
2 -------------->2
3 -------------->3
4 -------------->4
5 -------------->5
6 -------------->6
7 -------------->7
8 -------------->8
```

Fig. 5 Hacker Dashboard

CONCLUSIONS

In this work, the security of image encryption schemes has been studied in detail. The image encryption schemes can be broken with a chosen plain-image attack when the number of encryption rounds is one. It is concluded that no better pseudo-random permutations can be realized to offer a higher level of security against plaintext attacks. To offer an acceptable security level against plaintext attacks, the pseudo-random permutations should be updated.

ACKNOWLEDGMENT

The author would like to thanks the researchers of the references, and Department of Computer Engineering, G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar for their valuable suggestions and support.

REFERENCES

[1] X. Zhang, Y. Ren, L. Shen, Z. Qian, and G. Feng, "*Compressing Encrypted images with auxiliary information"*, IEEE Trans. Multim., vol. 16, no. 5, pp. 13271336, 2014.

[2] J. Zhou, X. Liu, O.C. Au, and Y.Y. Tang, "*Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation"*, IEEE Trans. Inf. Foren. Sec., vol. 9, no. 1, pp.3950, 2014.

[3] A. Pande, J. Zambreno, "*Embedded Multimedia Security Systems: Algorithms and Architectures"*, Springer-Verlag, London, 2013.

[4] Z. Galias and W. Tucker, "*Numerical study of coexisting attractors for the Henon map, Int. J. Bifurcation Chaos"*, vol. 23, no. 7, pp. 118, 2013.

[5] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "*On the design of perceptual MPEG-video encryption algorithms*", IEEE Trans. Circ.Sys. Video Tech., vol. 17, no. 2, pp. 214223, 2007.

[6] Sk. Md. Mizanur Rahman, M.A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "*Chaos-cryptography based privacy preservation technique for video surveillance*", Multi M. Sys., vol. 18, no. 2, pp. 145 155, 2012.