International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Chosen-Plaintext Attack on Permutation-Only Image Encryption Schemes and Steganography on Images

Soja Prasannan[1], Devi Murali[2]

[1]M .Tech student, Sree Buddha College of Engineering, Elavumthitta, Kerala, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering, Elavumthitta, Kerala, India

Abstract: ***An encryption process which is a commonly used primitive in multimedia for both images and videos is permutation scheme, and many permutation-only algorithms have been proposed in recent years for the protection of multimedia data. The image matrix entries in permutation-only image ciphers are scrambled using a pseudo-random number generated permutation mapping matrix. The literature survey done on the cryptanalysis of the image ciphers in the previous works indicates that the permutation-only image ciphers are prone to cipher text-only attacks and/or known/chosen-plaintext attacks. Steganography is a type of hidden communication in which a file, message, image, or video is concealed within another file, message, image, or video. The previous works on cryptanalysis of permutation-only image encryption schemes were studied in this paper and the cryptanalysis performed on chosen-plaintext attacks were made more efficient and along with this a steganographic process is done to hide text data as well. It was proved that in all permutation-only image ciphers, nevertheless of the cipher structure, the exact permutation mapping is recovered completely by a chosen-plaintext attack. A chosen-plaintext attack is introduced in this paper that determines the exact plaintext elements perfectly using a deterministic method. When the plain-images are of size M × N and with L different color potency, the number m of chosen plain-images required for breaking the permutation-only image encryption algorithm is*** $m = [log_L (M N)]$***. The complexity of the proposed attack is small as permutation is used and hence the consumption time is also small. To endorse the performance of the proposed chosen-plaintext attack, an experiment was performed on a recently proposed permutation-only image/video ciphers. Both the theoretical and the experimental results exhibited that the proposed attack surpasses the state-of-the art cryptanalytic methods. The steganographic step provides an additional security to the overallsystem by hiding the image data within another image.***

Keywords: Chosen-plaintext attack, Cryptanalysis, Image encryption, Steganography, Payload

1. Introduction

Information is an important asset that needs to be secured from attacks. Information transferred over the computer networks currently is not only text but also audio, video and other multimedia data types. The fast growing demand for digital multimedia applications has opened up a number of challenges regarding the confidentiality of images and videos in many multimedia-based services, such as Pay-TV, remote video conferencing, and medical imaging. Reliable storage and secure transmission of visual content is a legitimate concern of Intellectual Property (IP) owners. Thus, there is an extreme need to safeguard images and videos against unauthorized use or other security violations. In an attempt to solve the problems of data security, researchers and practitioners are placing increasing emphasis on encryption and steganography. There are several symmetric block cipher algorithms which are adopted as the standard encryption methods such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Even though these methods are standard algorithms there are certain constraints imposed by the data structure and the application requirements, such as format compliance, real-time performance, complexity, compression efficiency, perceptibility and the security level. Since the digital images have grid structure, three different types of operations of image encryption methods are utilized: value transformation, position permutation, and the combination form. From all these operations, permutation is a commonly used primeval in many image encryption schemes due to the simple implementations 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 (PRNG). A PRNG isalgorithms that generate a sequence of numbers whose properties approximate the properties of sequences of random numbers. From the design point of view, permutation dissolves the statistical structure of the plaintext into long range statistics and it is suitable for fast processing requirements of massive digital multimedia data unveiled in [12], [13]. Hidden information has a variety of uses in products and protocols. The extra information about an image can be stored in them without actually changing the original data. Because the electronic communication is very prone to eavesdropping and malicious interventions, the issues of security and privacy are more pertinent today than ever. The cryptographic approach to privacy is to make the exchanged information unreadable to those who do not have the right decryption key. Steganography offers a feasible alternative to encryption in oppressive regimes where using cryptography might attract unwanted attention or in countries where the use of cryptography is legally prohibited.

Despite the advantages of permutation, it has a number of inherent limitations. Permutation-only ciphers disclose some of the 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 practicable arrangements for the plaintext elements is less than the key space, the number of effective keys get reduced, and hence, the permutation mapping can be revealed. Moreover, permutation-only encryption/decryption is not simple sequential operations that can be done dynamically. In general, permutation may need a buffer with a size comparable to that of the plaintext. Therefore, due to the limitations above, permutation-only ciphers are nowadays only used in applications where substitution is technically infeasible and/or only a moderate level of protection is required. Considering typical examples of permutation-only image ciphers, in [9] and [10] image entries are dislocated using pseudo-random permutations; in [11] permutation operations are performed on the bit-planes of the image entries; and in [14] permutation operations are performed on DCT/wavelet coefficients.

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 ciphertext-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. Despite the extensive cryptanalysis of permutation-only multimedia ciphers, lately, many permutation-only ciphers have been proposed for the protection of different types of multimedia data, including digital images [9], [11] and video [10], [14]. This is mainly because the above-mentioned cryptanalytic methods can only be applied to specific encryption methods and cannot be generalized to a wider class of permutation-only multimedia ciphers [15] and [16]. In addition, even the best known methods of known/chosen-plaintext attacks ([19], [20]) cannot ensure the complete retrieval of the correct plaintext content, and hence, it is still ambiguous as to whether the security of permutation-only image ciphers can be effectively improved by designing new methods to generate better pseudo-random permutations.

A cryptanalysis was presented in this paper which breaks most permutation-only multimedia ciphers. In fact, it was shown that all permutation-only image ciphers are perfectly broken by chosen-plaintext attacks and no better pseudo-random permutation mapping can be realized to offer a higher level of security against chosen-plaintext attacks. For a successful attack, a tight lower bound for the required number m of chosen plain-images was derived, that is, $n = log_L(M\,N)$, comparing to the currently known results $O(\lceil log_L(M\,N)\rceil)$[19], [20], where M×N is the size of the image and L − 1 is the maximum color intensity, that is, a color intensity is specified by l ($0 \le l \le L-1$). The computational complexity of the proposed attack is O(n*MN). To verify the feasibility of the proposed attack, an experiment was performed on the recently proposed permutation-only image ciphers by Fu et al. [11]. The experimental results support the theoretical results that pseudo-random permutations alone cannot provide sufficient security against chosen-plaintext attacks. Compared to the state of the art cryptanalytic methods of [19] and [20], which partially (quantitatively) determine the permutation mapping, the chosen-plaintext attack gives a precise procedure for the careful construction of the chosen plain-imagesrequired, and therefore, completely discloses the correct permutation mapping with less data and computational complexity.

The remaining sections of this paper are structured as follows. In section 2, the procedure of the chosen-plaintext attack is described. Section 3 briefs the steps involved in steganography. Section 4 overviews a typical permutation-only image ciphers (case studies) proposed by Fu et al. [11]. Experimental results are shown in Section 5 to support the theoretical cryptanalysis. Section 6shows the simulation result. Finally the paper is concluded in the last section.

2. Chosen-Plaintext Attack

Before elaborating the chosen-plaintext attack, the following definitions are given to outline a permutation-only image cipher.

Definition 1: Let S = {s|s = 0, 1,..., MN - 1} denote the set of entry locations for an image with size M × N.

Definition 2: Consider that locations of image entries are scanned in a raster scan order and they are quantified by non-negative integers, which are chosen from the set of entry locations. Let R denote the matrix of entry locations, that is,

$$R = \begin{bmatrix} 0 & 1 & \cdots & N-1 \\ N & N+1 & \cdots & 2N-1 \\ \vdots & \vdots & \vdots & \vdots \\ (M-1)N & (M-1)N+1 & \cdots & MN-1 \end{bmatrix} \quad (1)$$

Definition 3: Let ***P*** and ***C***bedesignated as the plain-image and cipher-image, correspondingly. Note that each plain-image or cipher-image is represented by an *M* x *N* matrix the entry at position *s* of the matrixcorresponds to color intensities. For any *s* ($0 \le s \le M\,N - 1$), at the position s of the plain-image and cipher-image let *p (s)* and *c (s)* be the color intensities correspondingly.

Definition 4: Let *X*be considered as a finite set. The permutationπ^k: $X \rightarrow X$ is a bijection which maps the elements of *X* to itself. Each secret key $k \in K$ assigns a different permutation.

Definition 5: A permutation-only image cipher ρ is definedby a permutation which, given a secret key *k*, maps anyentry location *s* ($0 \le s \le M\,N - 1$) of a plain-image to itscorresponding location $\rho_k(s)$in the cipher-image, where$\rho_k$is a permutation determined by *k*.

The permutation-only image cipher is only pseudo-randomif it permutes the location of plain-image entries, withan approximate uniform probability, from the set of allpossible *(#S)*! arrangements.

Let'snow explain the procedure of the proposed chosen-

plaintext attack. Deducing the permutation mappingρ_k isequivalent to finding the secret key *k*. Hence, the problemof breaking the cipher is defined as an attempt to deducethe permutation mapping without any prior knowledge of the key. Consider the adversary as an oracle machine which hasaccess to the encryption and decryption functions, that is,ρ_k and$\rho_k{}^{-1}$. The adversary asks *m*number of ρ_k or $\rho_k{}^{-1}$queriesto obtaina set of*m*plain-image and cipher-

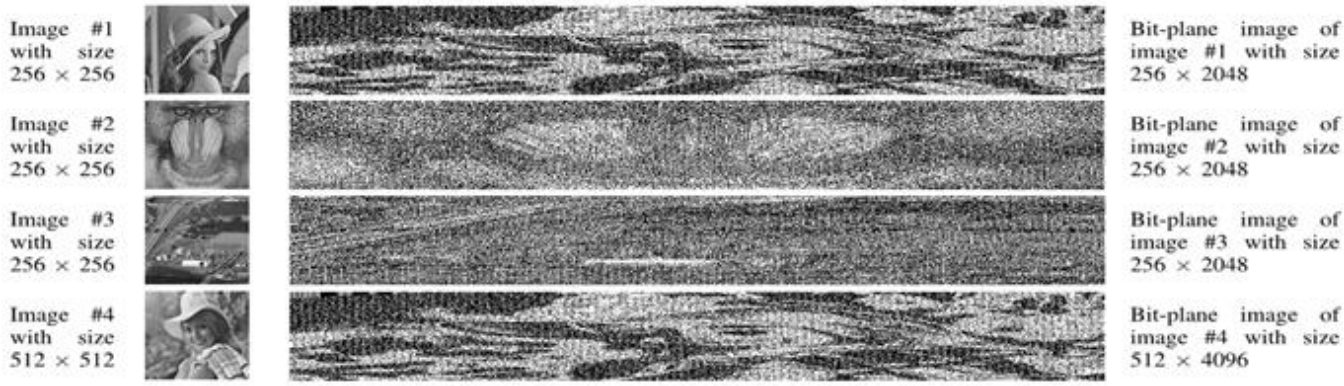


Figure 1: Test images used in the experiments

image pairs, thatis, $\partial = \{(\boldsymbol{P_i}, \boldsymbol{C_i})$ |where the $i=\{1, 2, \ldots, n\}$.

Proposition 1: For any value of $i(1 \leq i \leq n)$ and $j(1 \leq j \leq n)$,if either $\boldsymbol{P_i} = \boldsymbol{P_j}$or $\boldsymbol{C_i} = \boldsymbol{C_j}$, then $i = j$ and pairs $(\boldsymbol{P_i},\boldsymbol{C_i})$and $(\boldsymbol{P_j},\boldsymbol{C_j})$ are identical.

Proof: This proposition is an obvious result, because thecipher is defined by a bijective permutation.

Definition 6: Given *m*pairs of plain-images andcipher-images, namely, $(\boldsymbol{P_1}, \boldsymbol{C_1}),(\boldsymbol{P_2}, \boldsymbol{C_2}),\ldots,(\boldsymbol{P_n}, \boldsymbol{C_n})$,for any pair number r $(1 \leq r \leq n)$, source locations $(0 \leq s \leq M\ N - 1)$, target location t $(0 \leq t \leq M\ N - 1)$,and color intensity l $(0 \leq l \leq L - 1)$, where $M \times N$ is the sizeof the image and $L - 1$ is the maximum color intensity, the*equivalent set* $J_r(s)$ is defined as a set of target locations inthe r^{th} cipher-image, whose values are equal to the colorintensity l of the s^{th} location in the r^{th} plain-image, that is,

$$J_r(s) = \{t | c_r(t) = p_r(s), (0 \leq t \leq M\ N - 1)\} \quad (2)$$

Obviously, by definition, the following condition holds for the equivalent sets:

$$\cup_{s=0}^{M\ N-1} J_r(s) = \{t | t = 0,1,\ldots,M\ N - 1\} \quad (3)$$

For any r $(1 \leq r \leq n)$, each pair of plain-images andcipher-images, that is, $(\boldsymbol{P_r}, \boldsymbol{C_r})$, involves two matrices withvalues assigned to entries. Consider the set *S* of entry locationsin the plain-image. As explained in the beginning of thissection, the permutation mapping ρ (see Definition 5) mapsthe source locations in the plain-image to the target locationsin the cipher-image. To uniquely determine the permutation mapping, it is sufficient to study the arrangement of distinct entries in the pair of plain-images and cipher-images.In the case that all entries are assigned distinct values, thepermutation is individually determined by a single pair. However, the set of color intensities, that is, {0, 1,..., L - 1}, is finiteand the images under study may have more than L entries.Therefore, for any r $(1 \leq r \leq n)$ and s $(0 \leq s \leq M\ N - 1)$,by the pigeonhole principle the cardinality of some equivalentsets $\# J_r(s)$ may not equal 1, and it is thus difficult to deducea unique permutation mapping by knowing only one pairof plain-images and cipher-images. Hence, it is required to haveenough pairs of plain-images and cipher-images to determine the targetlocation where

Each source location is mapped into. Therefore,the interest lies in using a collection of pairs, all of whichhave repeated values, to individually determine the underlyingpermutation. Clearly, the mapping of location s is uniquelydetermined if for any s $(0 \leq s \leq M\ N - 1)$and r $(1 \leq r \leq n)$,the identical sets $J_r(s)$ intersect in a singleton, that is, $\cap_{r=1}^{n} J_r(s) = \{\rho(s)\}$, and hence it is sufficient to determinethe permutationρ if this is true for all *s*. Two further questions then appear:

- Is this condition ample to determine unique ρ?
- With what validity and computational cost can themapping ρ be determined from sufficient pairs?

To answer these questions, it is essential to find a relationshipamong the number of plain-image/cipher-image pairs *n*, thenumber of locations $M\ N$ and the number of assigned valuesin the locations L. To perform a successful chosen-plaintextattack, it is necessary to find a lower bound on the numberof required pairs. Nonetheless, it is possible for two given pairsto be related by a permutation on the color intensities, suchthat both pairs give the same information regarding possibleplain-image and cipher-image locations. Thus, a useful boundon the number of required pairs will entail some restrictionthat avoids this possible redundancy.

Theorem: The number of required chosen plain-images *m* to perform a successful chosen-plaintext attack on a permutation-only image encryption algorithm is$m = [log_L(\mathrm{MN})]$.

Proof: Theoretically, the permutation mapping can be easily deduced using an input matrix of size $M \times N$ whose entries are sequentially labeled with distinct values 0, 1,...,$M\ N$. However, this is not practical because the encryption/decryption machine is only defined for entries of at most $L - 1$, which is usually less than the number of entries. Therefore, to make the attack feasible, the entries are firstly expanded by $log_L(\mathrm{MN})$].digits with radix L. This matrix is then separated into $[log_L(\mathrm{MN})]$numbers of plain-images based on the digit positions in radix L. Once permutation ρ is applied to the plain-images, it

produceslog_L(MN)cipher-images with entries in radix *L*. A combination of cipher-images using the positional digits reveals the mapped locations of the original locations.

3. Steganography

Before summarizing the steps in steganographic process lets specify certain terms associated with steganography.

- Cover-Image (host) – An image in which the secret information is going to be hidden. "Cover" is the term used to describe the original, innocent data, message, audio, still, video etc.
- Stego-Image – The medium in which the information is masked. The "stego" data is the data containing both the cover image and the "embedded" information. Analytically, the processing of hiding the secret information in the cover image is known as embedding.
- Payload: The information which is to be concealed. The important datato be hidden in the cover data is known as the "embedded" data.

Steps involved in steganographic process are itemized below:

1) First a texture image (color image)is selected on which the original image needs tobe hid.
2) The cover image is generated next by repeating the texture image into 6x6 matrixes.
3) Since the cover image is available now the payload that needs to be hidden is enteredusing the underlying software.
4) The payload is then converted into 8 bit data and then concatenated with each row ofthe pixels of the cover image.
5) The resulting image will be the stego-image which contains the hidden text messageand can be transmitted over the network.

Steps involved in retrieving the hidden image from the stego-image:

1) The stego-image is first converted into binary from its decimal form.
2) Then from each row the payload can be extracted.
3) The payload that is in the binary form is then converted to the decimal form and thenconverted to the 8 bit unit.
4) The payload and the cover image can then be shown separately.

4. Case Studies – Typical Permutation-Only Image/Video Ciphers

To verify the correctness of the above-discussed chosen-plaintext attack, it was tested on a typical permutation-only image/video ciphers. With respect to this, therecently proposed permutation-only image/video cipher by Fu et al. [11] is briefly overviewed.

4.1 Fu et al.'s Encryption Scheme

Fu et al.'s encryption algorithm is a type of bit-level permutation scheme, which encrypts plain-images in two iterative stages. Firstly, the plain-image is extended into a bit-plane (binary) image, which is constructed by expanding every column of the plain-image into bit-plane columns. An image of size $M \times N$ with 256 color intensities can be extended to a bit-plane image with size $M \times 8N$. In the first stage, a pseudo-random sequence is generated by a Chebyshev map, ensuring that there is no repetition, and this sequence is interpreted as the permutation mapping. A Chebyshev map is a typical invertible iterated map that generates orthogonal real-valued sequences. The Chebyshev map of degree D (D = 2, 3,. . .) is based on a trigonometric function defined as

$$s_{m+1} = f(s_m) = \cos(D \cos^{-1}(s_m)) \quad (4)$$

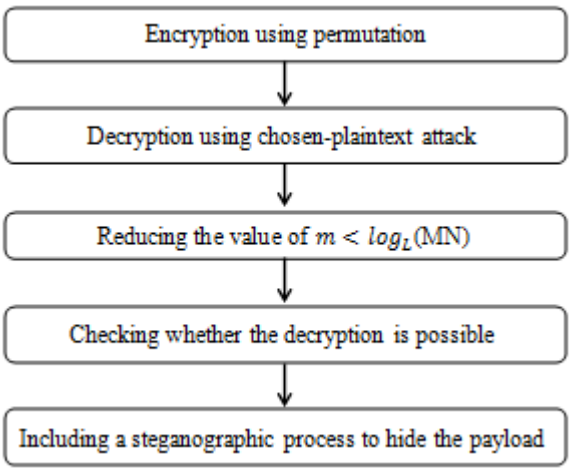
where f: $S \rightarrow S$, $S \in$ [-1,+1]. To avoid the harmful effect of transitional procedure, the Chebyshev map is firstly iterated for N_0times, where $N_0$is a constant. Then, two permutation sequences of length M and $N\times 8$ are generated, which are employed to shuffle the rows and columns of the bit-plane image, respectively. In the second stage, the shuffled bit plane is firstly divided into eight bit-squares of equal size. Then, each bit-square is shuffled independently with different control parameters by a discretized version of Arnold Cat Map (ACM) with different control parameters. The discretized ACM is defined as

$$\begin{bmatrix} x_{m+1} \\ y_{m+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_m \\ y_m \end{bmatrix} \text{ modN}, \quad (5)$$

Where N is the number of pixels in one row (or column), a and b are control parameters, x and y are pixel coordinates, andx_n, $y_n \in \{0, 1,. . ., N - 1\}$. The determinant of this map is 1; hence, it is invertible and area-preserving. This stage is iterated n ($1 \leq n$) rounds. Finally, both stages 1 and 2 are iterated $n$times. To construct the cipher image, all the 8 bit-squares are concatenated from left to right and recovered to a pixel-plane. If truth be told, both stages of Fu et al.'s encryption algorithm can be viewed as a one permutation stage which scrambles the entries of the bit-plane image. As explained by Fu et al. [11], the image conversion to a bit-plane image and its inverse are straightforward linear transformations. Therefore, without loss of generality, it is assumed that Fu et al.'s algorithm encrypts bit-plane images. Thus the secret key for Fu et al.'s encryption algorithm is (s_0, D, a, b, n, m).

5. Experimental Analysis

According to the cryptanalysis (see Section 2), the permutation mapping of the case study, which was described in Section 4, can be easily deduced by log_L(MN) chosen plain-images.To verify this claim, numerous experiments were performed. Figure 1 depicts some of the test images which were used to perform the experiment. These test images were of size $M \times N$ = 256 × 256 and 512 × 512 with L = 256 color intensities. Figure 1 also depicts the bit-plane images of the test images. To deduce a unique permutation mapping, the log_L(MN)chosen plain-images were built based on the proposed coding (see Section 2). To verify the breaking performance, the corresponding cipher-images were decrypted with the inferred permutation matrices, and the recovered plain-images were compared with the original test images depicted in Figure 1. In the following subsections, the experimental results for breaking Fu et al.'s encryption algorithm will be given.



Flow Chart: Experimental steps performed.

5.1 Experimental Results on Fu et al.'s Encryption Algorithm

The bit-plane (binary) images depicted in Figure 1 were encrypted by Fu et al.'s encryption algorithm using$(s0, D, a, b, n, m)$ = $(0.7, 4, 5, 2, 3, 1)$ as the secret key.The corresponding cipher bit-planes and cipher-imagesare depicted in Figure 2. To deduce the 256 × 2048permutation mapping, the adversary only requires$[log_2(256 \times 2048)]$ = 19 pairs of input/output binaryimages. For a 512 × 4096 case, a similar procedure requiresonly $[log_2(512 \times 4096)]$ = 21 pairs of input/output binaryimages. The inputimages were built based on the above described coding to achieve a unique permutation mapping.

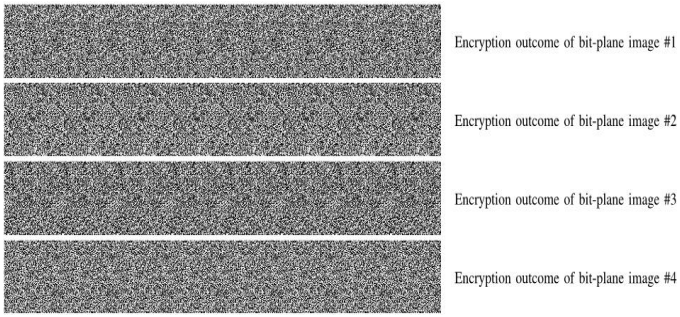


Figure 2: Corresponding encrypted bit-plane images of the four test bit-plane images

6. Simulation Results

MATLAB is a programming language developed by MathWorks. MATLAB R2015b is used as a simulation platform on a machine with Intel Core i5 1.80 GHz processor and 4 GB of installed memory running under Windows 8.

6.1 Cryptanalysis on Encrypted Data

The cryptanalysis was done on image #1. In the first case, where the value of $m > log_L(MN)$, the image #1 was decrypted successfully. But when $m$was made less than $log_L(MN)$ the image could not be decrypted. This is shown in Figure 3. The main advantage of this attack is that it presents a precise method for the construction of the chosenplain-images which ensures the correct retrieval of the permutation mapping. In addition,the attack gives a tight lower bound for the number of required chosen plain-images for asuccessful chosen-plaintext attack.

Figure 3: Decrypted images in both cases.

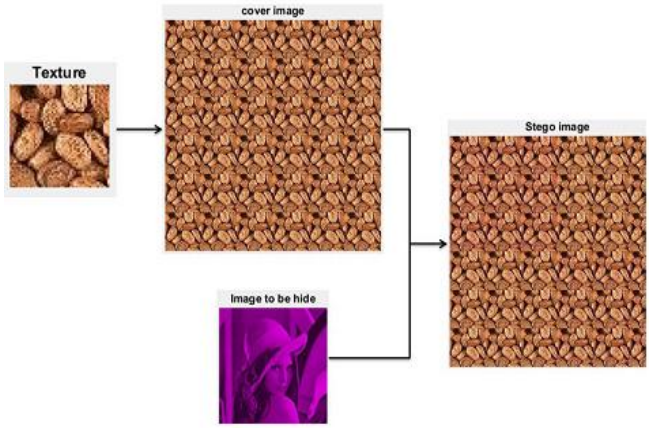


Figure 4: Steganographic Process

6.2 Steganographic Process

In the steganographic process first a texture image say 50×50 size is used as shown in the Figure 4. Then the image is fragmented into a 300×300 pixel image. This image is called the cover image. The payload image or the image to be hidden can now be entered into the image by converting the payload image initially to 8 bit data and then from decimal to binary form. The data is then concantenated along to each row of the cover image which is converted to binary form. This generates the stego-image. Thus the stego-image currently contains the payload.

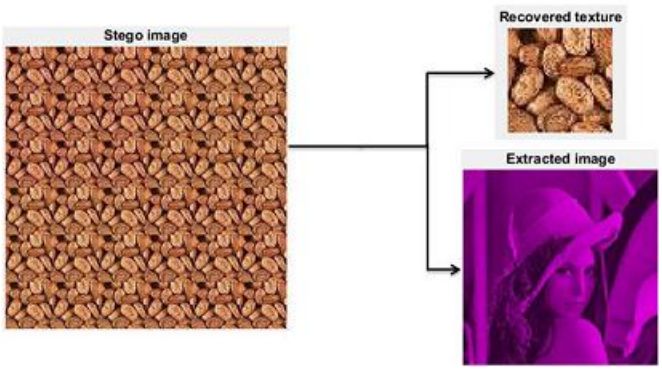


Figure 5: Extraction Process.

Figure 6.3 describes the receiver section. For extracting the payload data from the stego-image first the stego image is

converted into thebinary form from its decimal format. Then the payload data is recovered from the stego image. Finally the texture image and the payload image are separated.

7. Conclusion

In this paper, it was proved that permutation-only image ciphers are completely broken against chosen-plaintext attacks. Based on the above cryptanalysis, the permutation mapping can be easily deduced using an input matrix of size $M \times N$ whose distinct entries are selected from the log_L(MN) digit expansions in radix L for 0, 1,..., $M N$ - 1 in respective locations. In a practical attack, the number $m$of required chosen plain-images to break the permutation-only image encryption algorithm islog_L(MN). It has also been found that the attack complexity is practically small. This shows that the proposed cryptanalysis is efficiently achievable by means of a limited number of chosen plain-images using a polynomial amount of computation time. Some experiments on a permutation-only image cipher have been performed to validate the performance of the proposed chosen-plaintext attack. Both theoretical and experimental results verified the feasibility of the proposed attack. From the results of this paper, it is concluded that no better pseudorandom 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 to a frequency smaller thanlog_L(MN). The cryptanalysis is exact; offering a lower bound on the number of required chosen plain-images and can be achieved in less computation time.Using steganography, the original image is hidden within the cover image and the stego image is transmitted. Thus the image is safely hidden within another image and the attacker will not be aware of this. The original image can then be extracted from the stego-image at the receiver section. Steganography can be used for electronic communications which includes the concealment of information within computer files. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

8. Acknowledgment

I would like to express profound gratitude to our Head of the Department, Ms. Sangeeta T. R.,for his encouragement and for providing all facilities for my work.I express my highest regard and sincere thanks to my guide, Asst. Prof. Ms. Devi Murali, who provided the necessary guidance and serious advice for my work.

References

[1] AlirezaJolfaei, Xin-Wen Wu, “On the Security of Permutation-Only Image EncryptionSchemes,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, Feb. 2016.
[2] D. Engel, T. Sttz, and A. Uhl, “A survey on JPEG2000 encryption,” Multimedia Syst., vol. 15, no. 4, pp. 243-270, 2009.
[3] H. Cheng and X. Li, “Partial encryption of compressed images and videos,” IEEE Trans. Signal Process., vol. 48, no. 8, pp. 2439-2451, Aug. 2000.
[4] D. Engel, E. Pschernig, and A. Uhl, “An analysis of lightweight encryption schemesfor fingerprint images,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 2, pp. 173-182, Jun. 2008.
[5] X. Zhang, Y. Ren, L. Shen, Z. Qian, and G. Feng, “Compressing encrypted imageswith auxiliary information,” IEEE Trans. Multimedia, vol. 16, no. 5, pp. 1327-1336, Aug. 2014.
[6] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, “On the design of perceptualMPEG-video encryption algorithms,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 2, pp. 214-223, Feb. 2007.
[7] Ajay Kumar Dubey and Chandra Kant Shukla, “Chaos based Encryption and Decryption of Image and Video in Time and Frequency Domain,” in IJCA Special Issue on Network Security and Cryptography NSC, 2011.
[8] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, “Overview on selective encryption of image and video: Challenges and perspectives,” EURASIP J. Inf. Secur., vol. 2008, Dec. 2008, Art. ID 179290.
[9] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, “Designing an efficient image encryptionthen-compression system via prediction error clustering and random permutation,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 39-50, Jan. 2014.
[10] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, “Chaos-cryptography based privacy preservation technique for video surveillance,” Multimedia Syst., vol. 18, no. 2, pp. 145-155, 2012.
[11] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, “A novel chaos-based bit-levelpermutation scheme for digital image encryption,” Opt. Commun., vol. 284, no. 23, pp. 5415-5423, 2011.
[12] R. B. Lee, “Accelerating multimedia with enhanced microprocessors,” IEEE Micro, vol. 15, no. 2, pp. 22–32, Apr. 1995.
[13] C. Kachris, N. Bourbakis, and A. Dollas, “A reconfigurable logic-based processor for the SCAN image and video encryption algorithm,” Int. J.Parallel Prog., vol. 31, no. 6, pp. 489–506, 2003.
[14] C. Wang, H.-B. Yu, and M. Zheng, “A DCT-based MPEG-2 transparent scramblingalgorithm,” IEEE Trans. Consum. Electron., vol. 49, no. 4, pp. 1208-1213, Nov. 2003.A. Swaminathan, Y. Mao, and M. Wu,“Robust and Secure Image Hashing,”IEEE Trans. on Inf. Forensics and Security, Vol 1,Issue2, pp.215-230, June 2006.
[15] Y. Matias and A. Shamir, “A video scrambling technique based on space fillingcurves,” Advances in Cryptology (Lecture Notes in Computer Science), vol. 293, C. Pomerance, Ed. Berlin, Germany: Springer-Verlag, 1987, pp. 398-417.
[16] M. Bertilsson, E. F. Brickell, and I. Ingemarson, “Cryptanalysis of video encryptionbased on space-filling curves,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 434, Berlin, Germany: Springer-Verlag, 1989, pp. 403-411.
[17] M. Kuhn, “Analysis for the Nagravision Video Scrambling Method,” 1998.
[18] W. Li, Y. Yan, and N. Yu, “Breaking row-column shuffle based image cipher,” in Proc. 20th ACM Int.

Conf. Multimedia (MM), New York, NY, USA, 2012, pp. 1097-1100.
[19] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation only multimedia ciphers against plaintext attacks," Image Commun., vol. 23, no. 3, pp. 212-223, 2008.
[20] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," Signal Process., vol. 91, no. 4, pp. 949-954, 2011.

Author Profile

Soja Prasannan received B-Tech degree in Electronics and Communication Engineering from M.G University, Kerala at Sree Buddha college of Engineering for women in 2014. And now she is pursuing her M-Tech degree in Communication Engineering under the same university in Sree Buddha college of Engineering.

Devi Murali isworking as Assistant Professor in department of Electronics and Communication, Sree Buddha college of Engineering, Elavumthitta, Pathanamthitta.