Survey on Impact of Attacks on Permutation Only Image Encryption Scheme

[1]Ms. Snehal B. Ambare, [2]Prof. Amruta Amune

[1,2]G. H. Raisoni College of Engineering and Management, Ahmednagar, Maharashtra. India.

[1]ambare.snehal@gmail.com, [2]amruta.amune@raisoni.net

Abstract: Recently four chaos-based image encryption schemes were proposed. Essentially, the four schemes can be merged into single class, which is composed of two parts: permutation of position and diffusion of pixel value with the same cipher-text feedback function. The operations involved in the two basic parts which are determined by a pseudo random number sequence (PRNS). PRNS generated from iterating a chaotic dynamic system. As per the security requirement, the two simple parts are performed for some rounds alternatively. Although the designers claimed that the schemes are of very high quality, we found the following security issues: 1) the schemes are not sensitive to the changes of plain-images; 2) the schemes are not sensitive to the changes of the key streams which is generated by any of secret key; 3) there exists a serious flaw of the diffusion function; 4) the schemes can be broken with no more than dlogL(MN)e+3 chosen-images when the iteration number are equal to only one, where MN is the size of the plain-image and L is the number of various pixel values; 5) the cryptanalysis on single scheme which proposed by different research group is questionable.

Keywords: Chosen-plaintext attack, cryptanalysis, image encryption, permutation.

I. INTRODUCTION

With the fast development of multimedia as well as network technologies, the transmission of multimedia data takes place very frequently. The multimedia data security is crucial part to focus. However, traditional text encryption schemes were not so effective to encrypt the multimedia data due to different attribute of multimedia data[7][11], such as the bulky size as well as strong redundancy of uncompressed data. To satisfy this need, a various multimedia encryption schemes have been introduced in the past decade. Meanwhile, cryptanalysis work has been developed, at same time some of the proposed schemes have been found not secure from the viewpoint of cryptography. An image encryption scheme based on 3D chaotic cat maps was proposed. The scheme is composed of two basic components: position permutation as well as diffusion of pixel value with a cipher-text feedback function. For improving the security of the scheme, the two basic components are alternatively performed for some rounds. However the authors did not discuss how many rounds is sufficient for a satisfactory degree of security.

In this paper, we analyze the four schemes collectively. Meanwhile The following problems we find: 1) the schemes are not sensitive to the changes of plain-images; 2) the schemes are not sensitive to the changes of the key streams which is generated by any secret key; 3) there exists a serious flaw of the diffusion function; 4) the equivalent version of the whole pseudo random number sequence (PRNS) used for diffusion can be recovered when the round number is single; 5) the cryptanalysis is questionable. The rest of this paper is organized as follows. The next section gives us a brief introduction to the class of image encryption schemes. It also focuses on the security analysis of the class of encryption schemes[7].

II. RELATED WORK

X.Zhang,Y.Ren,L.Shen,Z.Qian,andG.Feng In this paper proposes a novel scheme of compressing AES encrypted images. The content owner encrypts the original uncompressed images by double encryption methods[7]. Then, the channel provider who cannot 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 key. Experimental result shows the ratio-distortion performance of the proposed scheme is better than that of previous techniques.[1]

J.Zhou,X.Liu,O.C.Au,andY.Y.Tang The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic coding-based approach 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 state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.[2]

A. Pande, J. Zambreno The proposed algorithms ensure a considerable level of security for low-power embedded systems such as portable video players and surveillance cameras[8][9]. These schemes have zero or little compression losses and preserve the desired properties of compressed data in encrypted bitstream to ensure secure and scalable transmission of videos over heterogeneous networks[3].

Z. Galias and W. Tucker The question of coexisting attractors for the Henon map is studied numerically by performing an exhaustive search in the parameter space. As a result, several parameter values for which more than two attractors coexist are found. Using tools from interval analysis, we show rigorously that the attractors exist. In the case 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 continuation method; the basins of attraction are found numerically.[4]

S. Li The proposed design is actually an encryption configuration that can work with any stream cipher or block cipher. Compared with the previously-proposed schemes, the new design provides more useful features, such as strict size-preservation, on-the-fly encryption and multiple perceptibility, which make it possible to support more applications with different requirements. 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 paper, we first review recent Privacy Enabling Technologies (PET). Later, we discuss pertinent evaluation criteria for effective privacy protection. We then put forward a framework to assess the capacity of PET solutions to hide distinguishing facial information and to conceal identity. Comprehensive and rigorous experiments were conducted to evaluate the performance of face recognition algorithms applied to images 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 foil face recognition[6]

III. PROPOSED WORK

There are three basic permutation is possible in an image [2] which are bit, pixel and block permutation. A digital image is combination of pixels and a pixel in the image is combination of 8-bits. Bit permutation is performed by permuting bit in a pixel using encryption key. The maximum size of encryption key for bit permutation is of 8 bit therefore the maximum number of available key is equal to factorial of 8 which is not very large[10]. The process of permuting pixel in an image according to key is known as pixel permutation. Pixel permutation can be performed in different way depending on size key, if size of key is one dimensional then we can perform row permutation and column permutation according to key and if size of key is two dimensional then pixels are place at the position according to the key[10]. Image can be divided into sub blocks. Sub blocks are permuted in block permutation. The process of block permutation is same as pixel permutation. The size of key for pixel and block permutation is not fixed it can be chosen randomly.

IV. ARCHITECTURAL VIEW

The objective of the proposed system is to perform diffusion based encryption/ decryption with respect to bit level encryption/ decryption and chaotic based encryption/ decryption for pixel relocation. The obtained decrypted image will be sent to the noise removal process where a spatial based filtering will be applied for the purpose of noise correction. The PSNR value is considered as a standard of measure for the quality of the noise corrected image and the correlation coefficient is considered as a measure for the performance of the encryption/ decryption methods. The proposed system architecture is shown in below. which involves four modules, they are encryption, key generation, decryption and noise removal.

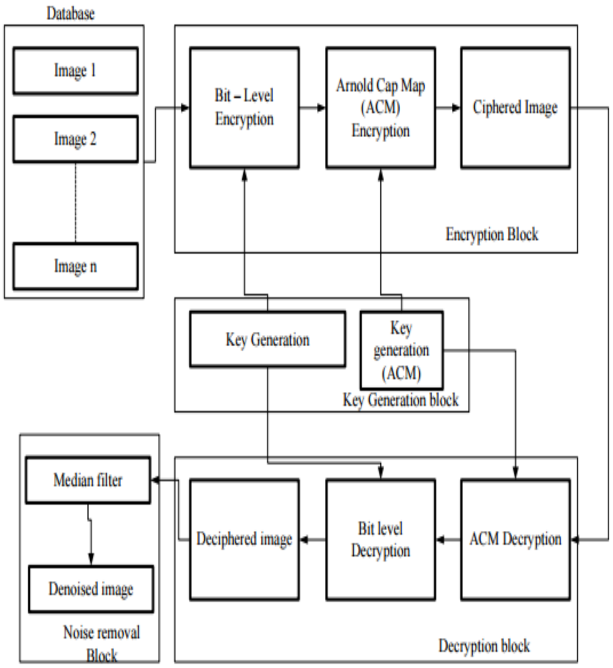
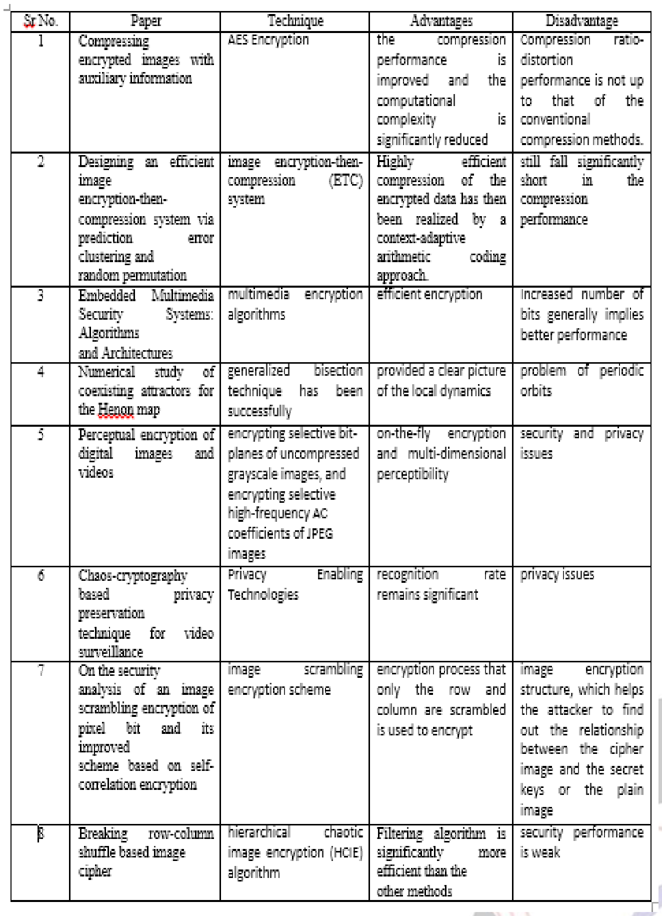


Figure 1 System Architecture

Initially an input image (plain image) is resized to have an equal dimension of square matrix. A bit level encryption is performed where the key is generated having the same number of rows as the number of total bytes and the 1 column. Each bit in the plain image is XORed with the value of the corresponding position of the key. The resulting encrypted image is then sent to the chaotic based mapping encryption which in this case the Arnold Cap map based scrambling method is used to scramble. a number of iteration for the ACM is specified by the user. The key with respect to ACM is generated by first entering a value which in turn produces a random number, the value of this random number is considered as the number of iterations for the ACM encryption method to be performed. The resulting image is the ciphered image which is expected to have a high correlation coefficient with respect to image pixels. The decryption of the image is performed by first considering the ciphered image obtained by the ACM method. The user will be prompted for a key[11], this is the same key which was set during the ACM encryption process. Upon entering the respective key the iteration value is retrieved which will perform the same number of iteration as was performed during the ACM encryption process. The decrypted image from ACM method is then sent to the bit level diffusion based decryption method where the user is prompted for the second key which was created during the encryption process of the bit level encryption method. Upon receiving the key the pixel position of the decrypted image is XORed with the corresponding pixel position of the key. The resulting image is the final decrypted image. The final decrypted image is sent to the noise removal process where a spatial based median filter is applied which in turn improves the quality of the image with respect to its psnr value below table 1 are Show.



Sr No.	Paper	Technique	Advantages	Disadvantage
1	Compressing encrypted images with auxiliary information	AES Encryption	the compression performance is improved and the computational complexity is significantly reduced	Compression ratio-distortion performance is not up to that of the conventional compression methods.
2	Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation	image encryption-then-compression (ETC) system	Highly efficient compression of the encrypted data has then been realized by a context-adaptive arithmetic coding approach.	still fall significantly short in the compression performance
3	Embedded Multimedia Security Systems: Algorithms and Architectures	multimedia encryption algorithms	efficient encryption	Increased number of bits generally implies better performance
4	Numerical study of coexisting attractors for the Henon map	generalized bisection technique has been successfully	provided a clear picture of the local dynamics	problem of periodic orbits
5	Perceptual encryption of digital images and videos	encrypting selective bit-planes of uncompressed grayscale images, and encrypting selective high-frequency AC coefficients of JPEG images	on-the-fly encryption and multi-dimensional perceptibility	security and privacy issues
6	Chaos-cryptography based privacy preservation technique for video surveillance	Privacy Enabling Technologies	recognition rate remains significant	privacy issues
7	On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption	image scrambling encryption scheme	encryption process that only the row and column are scrambled is used to encrypt	image encryption structure, which helps the attacker to find out the relationship between the cipher image and the secret keys or the plain image
8	Breaking row-column shuffle based image cipher	hierarchical chaotic image encryption (HCIE) algorithm	Filtering algorithm is significantly more efficient than the other methods	security performance is weak

Table 1.

Initially an input image (plain image) is resized to have an equal dimension of square matrix. A bit level encryption is performed where the key is generated having the same number of rows as the number of total bytes and the 1 column. Each bit in the plain image is XORed with the value of the corresponding position of the key[10]. The resulting encrypted image is then sent to the chaotic based mapping encryption which in this case the Arnold Cap map based scrambling method is used to scramble. a number of iteration for the ACM is specified by the user. The key with respect to ACM is generated by first entering a value which in turn produces a random number, the value of this random number is considered as the number of iterations for the ACM encryption method to be performed. The resulting image is the ciphered image which is expected to have a high correlation coefficient with respect to image pixels. The decryption of the image is performed by first considering the ciphered image obtained by the ACM method. The user will be prompted for a key, this is the same key which was set during the ACM encryption process. Upon entering the respective key the iteration value is retrieved which will perform the same number of iteration as was performed during the ACM encryption process [8]. The decrypted image from ACM method is then sent to the bit level diffusion based decryption method where the user is prompted for the second key which was created during the encryption process of the bit level encryption method. Upon receiving the key the pixel position of the decrypted image is XORed with the corresponding pixel position of the key. The resulting image is the final decrypted image. The final decrypted image is sent to the noise removal process where a spatial based median filter is applied which in turn improves the quality of the image with respect to its psnr value.

V. Conclusion

In this paper, the security of a class of image encryption schemes has been studied in detail. It has been found that the schemes are not sensitive to the changes of plaintexts or key streams generated by any secret key. There exists a defect in the diffusion function. In addition, the schemes can be broken with a chosen plain-image attack when the number of encryption rounds is one. The cryptanalysis work on one scheme given by another research group has been found to be problematic. Nevertheless, the security of the class of encryption schemes with multiple rounds has not been found to have major problem so far, which still needs further study.

REFERENCES

[1] Announcing the Data Encryption Standard (DES), NIST Standard 46–3, 1999.

[2] Announcing the Advanced Encryption Standard (AES), NIST Standard197, 2001.

[3] D. Engel, T. St¨utz, and A. Uhl, “A survey on JPEG2000 encryption,”Multim. Sys., vol. 15, pp. 243–270, 2009.

[4] H. Cheng and X. Li, “Partial encryption of compressed images andvideos,” IEEE Trans. Sig. Proc., vol. 48, no. 8, pp. 2439–2451, 2000.

[5] D. Engel, E. Pschernig, and A. Uhl, “An analysis of lightweightencryption schemes for fingerprint images,” IEEE Trans. Inf. Foren.Sec., vol. 3, no. 2, pp. 173–182, 2008.

[6] 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. 1327–1336, 2014.

[7] 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. 214–223, 2007.

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

[9] S. Li, G. Chen, and X. Zheng, “Chaos-based encryption for digital images and videos,” in Multimedia Security Handbook, B. Furht and D. Kirovski, Eds. Boca Raton, FL, USA: CRC Press, 2004, pp. 133– 167.

[10] 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 Journal on Information Security, Article ID 179290, pp. 1–18, 2008.

[11] S. Li, “Perceptual encryption of digital images and videos,” in Perceptual Digital Imaging: Methods and Applications, R. Lukac, Ed. Ch. 14, USA: CRC Press, 2012, pp. 431–468.