A Survey Report on Image Encryption Techniques

Nitin Rawal
Shri Vaishnav Instt. Of Tech and Sc. Indore

Manoj Dhawan
Astt. Prof. Shri Vaishnav Instt. Of Tech. and Science. Indore

Abstract

In these days as multimedia data transferred over insecure channel, it becomes an important issue to encrypt image with a suitable image encryption algorithms. An image encryption is different from text due to large processing, pixels definition, time to encrypt and size. This is also a different approach due to different type of attacks possible on text and image data. In this paper we study some encryption technique on the basis of their classification. Major technique are classified in different categories are, (I) Pixel Position permutation based algorithm, (II) value transformation based algorithm and (III) visual transformation based algorithm. We aim to frame this paper as literature survey of these classifications.

Keywords: *Image encryption, cipher, Block based image encryption, position permutation based encryption, value transformation algo, visual transformation based algo, Map based algo.*

1. Introduction

Image encryption means to prepare an image from an image that is difficult to understand, and recognize. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Basically there are three major classification of image encryption, Pixel Position permutation based, pixel value transformation based and visual transformation based technique are surveyed in this paper.

This paper is organized as follows In Section 1; we present general guide line about Image encryption. In

Section 2, we survey on already existing research paper Based on 2.1 pixel position permutation techniques. 2.2 Value transformation based techniques. In Section 2.3 Visual transformation based techniques. Finally, we conclude in section 3

2. Literature Survey

In this literature we collect some previous techniques and classify their working on the basis of three classification and frame under this heading.

2.1. Pixel Position Permutation based image encryption techniques.

Sesha Pallavi Indrakanti, P.S.Avadhani [2] proposes an image encryption technique based on all three classifications but the major task in this image encryption technique is related to shifting. This technique is performed in three steps, the first phase is image encryption where the image is split into blocks and these blocks are permutated. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is

generated with valid information about the values used in the encryption process.

Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das,[3] Has presented an image encryption algo based on permutation with the help of a chaotic map. This is a chaotic image cipher using logistic map. In the algorithm, permutation of image pixels was made on the basis of index position of generated chaotic sequence.

Ji Won Yoon and Hyoungshick Kim,[4] Proposes a new image encryption algorithm using a large pseudorandom permutation which is combinatorial generated from small permutation matrices based on chaotic maps. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix. They use chaotic image cipher, in which initially a small matrix was generated using chaotic logistic map. Authors constructed a large permutation matrix from generated small matrixes. The constructed permutation matrix was used to permute plain image pixels.

T. Gao and Z. Chen [5] This paper presents image encryption scheme, which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image.

M.A.B. Younes and A. Jantan,[6] proposed a new image encryption algo in which an image is encrypted using pixel position permutation. In this algo image is divided into a random number of blocks that are then shuffled within the image. A transformation table is constructed with the help of that shuffle, which will use at decryption phase to regenerate original image. After transformation this image encrypted with blowfish algo to increase level of security.

A. Mitra, Y V. Subba Rao, and S. R. M. Prasanna [7] have proposed an image encryption algo in this method the order of the bit, pixel and block permutations is random. It is an Image encryption using combination of different permutation techniques. They present an approach for a random combination of the aforementioned permutations for image encryption. From the results, it is observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information. So they use three different permutations, bit level permutation, pixel permutation and then block permutation.

2.2. Value Transformation based permutation

SD-EI is presented by Somdip dey [8] by using three steps, this image encryption scheme has bit rotation and reversal scheme on the basis of password length followed by extended hill cipher. Bit length of a password is taken up to 8 bit. This image encryption scheme has converted a pixel into the 8 bit binary number. In first number of bit (password length mod by 7) is rotated towards left and then reversed. Finaly used extended hill cipher [7] to get final image.

An advance version of SD EI, named as SD-AEI [9] has an advance stage with cyclic bit rotation policy. He added a new stage in which 8 continuous pixel of 8 bit put together in a matrix and then perform multi-directional matrix cyclic operation on that matrix “code” number of times, where code is the number generated by a string password. This step

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [10] Modified AES Based Algorithm for Image encryption, they analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance.

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [11] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption.

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [12] present image encryption technique using the Hill cipher. They are generating self-invertible matrix for Hill Cipher algorithm. Using this key matrix they encrypted gray scale as well as color images. Their algorithm works well for all types of gray scale as well as colour images except for the images with background of same gray level or same color.

Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M.[13] analysis Advance Encryption Standard(AES) algorithm and present a modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. Their result so that after modification image security is high. They

also compare their algorithm with original AES encryption algorithm.

Aloka Sinha and Kehar Singh [14] have proposed a new technique in which the digital signature of the original image is added to the encoded version of the original image. A best suitable error code is followed to do encoding of the image, ex: Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the image.

Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt [15] present a novel way of encrypting digital images with password protection using 1D SHA-2 algorithms coupled with a compound forward transform. A spatial mask is generated from the frequency domain by taking advantage of the conjugate symmetry of the complex imagery part of the Fourier Transform. This mask is then XORed with the bit stream of the original image. Exclusive OR (XOR), a logical symmetric operation, that yields 0 if both binary pixels are zeros or if both are ones and 1 otherwise.

An image encryption technique based on a combination between Arnold's cat map algorithm and the international data encryption algorithm (IDEA) is presented by Amr M. Riad, Amr H. Hussein, Hossam M. Kasem and Atef Abou El-Azm[16] . The proposed technique follows four steps; first, the IDEA accepts a 128 bits secret key which is used to generate an encryption key. The encryption key length equals the image width (w). Second, the encryption key is used to generate the encryption matrix. The rows of the encryption matrix are formed by making successive (N-decimal) rotations from the encryption key. Third, the encryption matrix is simply XORed with the original image to produce a primary encrypted image. Finally, the Arnold cat map is used to shuffle the positions of the primary encrypted image pixels to produce the final encrypted image.

Ajit Singh1 and Rimple Gilhotra's [17] technique is based on the concept of arithmetic coding in which a word of text is converted into floating point number that lie in range between 0 and 1. This floating point number is converted into binary number and after that one time key is used to encrypt this binary number. Finally after encryption, result is again a binary number; this number is converted into decimal number again and sends to the receiver.

A.B.Abugharsa, A.s.b.h.Basari, H.Almangush [18], proposed a new encryption technique based on the integration of shift image blocks and basic AES, here the shifted algorithm is used to divide the image into blocks .Each block consists of number of pixels and these blocks are shuffled by using a shift method that's move the rows and columns of the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image. The main idea is that an image can be encrypted by shifting the rows and columns of original image and not to change the positions of the blocks but by shifting all the rows a number of times depending on the shift table, and then the same number of times for the columns for an arrangement of blocks.

2.3. Visual transformation based algorithms

Xiaowei Xu, Scott Dexter and Ahmet M. Eskicioglu [19] present a hybrid image protection scheme to establish a relation between the data encryption key and the watermark. This schemes completes in three steps, 1. Generate shares of the image, and then embade watermark to this image share. Finally this embedded image has to be encrypted with any cipher scheme to get final encrypted image.

Sang-Su Lee [20] Proposed a method for a visual cryptography scheme that uses phase masks and an interferometer. To encrypt a binary image, we divided it into an arbitrary number of slides and encrypted them using an XOR process with a random key or keys. The phase mask for each encrypted image was fabricated under the proposed phase-assignment rule. For decryption, phase masks were placed on any path of the Mach-Zehnder interferometer. Through optical experiments, we confirmed that a secret binary image that was sliced could be recovered by the proposed method.

Mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat [21] proposed a scheme, a secure watermarking technique is used which is based on the idea of coding the fractal image and applying the chaos function. Here rearranging the position of image pixels were carried out by using the Arnold's Cat Map method to possess a good range of security.

Also the chaotic images are divided into range of blocks and domain of blocks to identify the self-similarity feature. The process promotes a set of contractive transformations, for approximating the value of every block of the image to the larger block. Which resulted in proving Chaos Fractal Coding algorithm has good range of capacity and better invisibility?

3. Conclusion

Image encryption is a technique in which either a pixel is converted to another pixel (value transformation based encryption) or replaced by other pixel in same image (position permutation) or visual transformation based algorithm (Image on image i.e. image as a key, or watermark, based encryption). Here we surveyed some of these algorithms. There are so many technique to make an image secure. Each technique has its own suitability area. Each technique has its own limitations.

4. References

[1] Komal D Patel, Sonal Belani, "*Image encryption using different techniques: A review*", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011

[2] Shesha pallavi, "Permutation based Image Encryption Technique", *Journal of Computer Applications (0975 – 8887)* Volume 28– No.8, August 2011, pp.236-247.

[3] Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das, *"*Image encryption using an enhanced block based transformation algorithm*" International Journal of Research and Review in Computer Science, Vol. 2, No. 2*, 2011 pp. 275-279**.**

[4**]** Ji Won Yoon and Hyoungshick Kim, *"*An image encryption scheme with a pseudorandom permutation based on chaotic maps*", Communication in Nonlinear Science and Numerical Simulation, Vol. 15, No. 12*, pp. 3998-4006.

[5] T. Gao and Z. Chen, *"*Image encryption based on a new total shuffling algorithm*", Chaos, Solitons and Fractals, (2008) Vol. 38*, pp. 213-220.

[6] M.A.B. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm", *IAENG International Journal of Computer Science*, 35:1, IJCS_35_1_03

[7] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," *Journal of computer Science*, vol. 1, no. 1, p.127,

[8] Somdip Dey, "SD-EI: A Cryptographic Technique To Encrypt Images", Proceedings of "*The International Conference on Cyber Security, CyberWarfare and Digital Forensic (CyberSec 2012)*", held at Kuala Lumpur, Malaysia, 2012, pp. 28-32

[9] Somdip Dey, **"**Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2". *International Journal of Cyber-Security and Digital Forensics (IJCSDF), The Society of Digital I nformation and Wireless Communications (SDIWC)* Nov. 2012 (ISSN: 2305-0012) 1(3): 221-225

[10] M. Zeghid, M. Machhout, L. Khriji, A.Baganne, R. Tourki. "A modified AES based algorithm for image encryption (2007)**".** *Proceeding of the World Academy of Science, Engineering and Technololgy, May, WASET Organization, USA.*

[11] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", *International Journal of Recent Trends in Engineering*, Vol. 1, No. 1, May 2009, pp. 663-667.

[12] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", *1st International Conference on Advances in Computing*, Chikhli, India, 21-22 February 2008.

[13] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M.,"A new modified version of Advance Encryption Standard based algorithm for image encryption,Electronics and Information Engineering*" (International Conference on Electronics and Information Engineering* . Date 1-3 Aug. 2010

[14] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", *Optics Communications, ARTICLE IN PRESS*, 2003, pp.1-6

[15]Abbas Cheddad, Joan Condell , Kevin Curran , Paul McKevitt, *"A Novel Image Encryption Algorithm Based on Hash Function" Optics Communications 283 (2010) 879–893.*

[16] Amr M. Riad, Amr H. Hussein, "A New Efficient Image Encryption Technique Based on Arnold and IDEA Algorithms"**.** *International Proceedings of Computer Science & Information Tech*; September 2012, Vol. 46, p140

[17]Ajit Singh1 and Rimple Gilhotra2, "Data security using private key encryption system based on arithmetic coding." *International Journal of Network Security & Its Applications (IJNSA)*, Vol.3, No.3, May 2011

[18] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush. "A New Image Encryption Approach using the Integration of a Shifting Technique and the AES Algorithm". *International Journal of Computer Applications*. March 2012

[19] Xiaowei Xu,1a Scott Dexter2b and Ahmet M. Eskicioglu "A hybrid scheme for encryption and watermarking".

[20] Sang-Su Lee, Jung-Chan Na, Sung-Won Sohn, Cheehang Park, "Visual Cryptography Based on an Interferometric Encryption Technique", *ETRI Journal*, Volume 24, Number 5, October 2002 pp. 373-380

[21] Keyvanpour, M.R. Farnoosh, M. "A New Encryption Method for Secure Embedding In Image Watermarking" Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on (Volume:2) 20-22 Aug. 2010 ISSN : 2154-7491 Print ISBN: 978-1-4244-6539-2 INSPEC Accession Number: 11537707 Conference Location : Chengdu Digital Object Identifier : 10.1109/ICACTE.2010.5579305

[22]. http://en.wikipedia.org/wiki/RSA_(algorithm) [ONLINE]

[23]. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography [ONLINE]

[24]. Cryptography & Network Security, Behrouz A. Forouzan, TataMcGraw Hill Book Company