DIFFERENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES AND KA IMAGE CRYPTOGRAPHY

KRISHAN GUPTA

TIT&S College, Bhiwani, Haryana, India
Email:-Krishan57gupta@gmail.com

Abstract– In addition focuses on image encryption techniques, As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. This paper focuses mainly on the different kinds of image encryption and decryption techniques and a new technique to encrypt image so that image can become secure. There are various techniques which are discovered and developed from time to time to encrypt/decrypt the images to make images more secure. In this paper a Survey of Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques and a KA encryption technique. KA Image cryptography is new approach In image cryptography which will be very helpful to improve image encryption. KA Technique Encrypt the image in two steps. First apply different operation on image rows and column wise pixels. And then divide whole image in Different parts and then apply different operation.

Keywords-KA Technique, Image Encryption, Image Decryption, Cryptography, ASCII, Symmetric Key, Asymmetric Key, Different parts of image

I. INTRODUCTION

The image encryption is to transmit the image securely over the network so that no unauthorized or any unknown user can able to decrypt the image. Image encryption, video encryption have applications in many fields including the internet communication, transmission, military Communication, etc. The progression of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Encryption defined as the conversion of plain message into a cipher text that cannot be read by any people without decrypting the encrypted text [1]. Decryption is the reverse process of encryption which is the process of converting the encrypted text in to original plain text, so that it can be read [1].Encryption of data [2] has become an important way to protect data resources especially available on the internet, intranets and extranets and at any kind of network. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. This paper focuses also on KA Technique which can secure image data over network and in storage media. KA Technique works on two steps for both encryption and decryption. For Encryption First of all simply apply different operation on image rows or column wise. Secondly divide whole image in 7 parts. And then one bits from every parts takes and make a equivalent ASCII code and then apply operation on all the bits of every parts and then apply different operation. And in case of Decryption first of all second step in reverse order than first step in reverse order. KA technique can works on both symmetric key cryptography and asymmetric key cryptography depends upon what technique used internally here in KA technique and also IN KA technique both symmetric and asymmetric cryptography can be used to gather.

II. LITERATURESURVEY

A. Lossless Image Compression and Encryption Using SCAN.

S.S. Maniccam and N.G. Bourbakis [3] have presented a new algorithm which based on two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

B. New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture.

Jiun-In Guo and Jui-Cheng Yen [4] have presented an algorithm which was same as mirror. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. Then, the chaotic sequence is generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

C. New Encryption Algorithm for Image Cryptosystems.

Chin-Chen Chang, Min-Shian Hwang, and Tung-ShouChen [5] used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

.

D. A New Digital Image Scrambling Method Based on Fibonacci number.

They presented a method [6] for new digital image scrambling method related to Fibonacci numbers. The standardization and periodicity of the scrambling transformation are mentioned. The scrambling effect is very sensible, the data of the image is re-distributed randomly across the whole image. The method can endure common image attacks, such as compression, noise and loss of data packet. They developed a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

E. Technique for Image Encryption using chaos technique.

Guosheng Gu and Guoqiang Han [7] made a new highly optimized image algorithm using substitution and permutation methods. It was done in order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used.

F. Technique for Image Encryption using chaos technique.

Huang-PeiXiao, Guo-ji Zang[8] made an algorithm using two chaotic systems . One chaotic system generates a chaotic sequence, which was changed into a binary representation using a threshold function. The other chaotic system was used to construct a permutation matrix. . Firstly, using the binary stream as a key stream, randomly the values of pixel of the images was modified. Then, the modified image was encrypted again by permutation matrix.

G. Color Image Encryption Using Double Random Phase Encoding.

Shuqun Zhang and Mohammad A. Karim [9] have come a new method to encrypt color images using existing optical encryption systems for gray-scale images. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods The color images are translating to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green- Blue) formats.

H. New modified version of Advance Encryption Standard based algorithm for image encryption.

Kamali S.H., Shakerian R.,Hedayati M. and RahmaniM.[10] presented a changing to the Advanced Encryption Standard (MAES) to provide a very high level security and better image encryption. The result shown by them was higher than that of original AES encryption algorithm.

I. Image Encryption Using Block-Based Transformation Algorithm.

Mohammad Ali Bani Younes and Aman [11] introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original whole image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

J. Permutation based Image Encryption Technique.

Sesha Pallavi Indrakanti and P.S.Avadhani[12] introduced an algorithm like random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the encryption process. The phase one was the image encryption. The phase two was the phase of key generation. And the phase three was the identification process. This provide confidentiality two-color image with less computations.

K. Image Encryption Based on Bit-plane Decomposition and Random Scrambling.

Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma[13] general random scrambling method was proposed which has stable scrambling degree than the classical method Arnold transform. At first, it decomposed a gray image into several bit-plane images. Then this technique shuffled them by a random scrambling algorithm separately. Lastly, this technique merged the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image. Due to each bit-plane image is scrambled by using different scrambling random sequences, the bits situated at the same coordinates in different bit-planes are almost not stay on the original positions when each bit-plane being scrambled separately. For every pixel, it's all bits of gray level, therefore, may be come from those pixels

located different positions. Consequently, the reconstructed gray levels of image are changed ineluctable. Method can do both positions exchange scrambling and gray level change scrambling at the same time.

III. PROPOSED CRYPTOGRAPHY TECHNIQUE

In the KA technique Cryptography will be based on two steps. First Step is apply different operation on images as rows or column wise here. And another step is divide whole image in 7 equal's length parts but remember that these 7 parts come from image from different side not as only row or column wise. In first steps XOR operation will be better to apply rows wise and column wise in two ways first way from left than top than left top than right top. Than in second ways right then bottom then right bottom then left bottom. Here both way well be apply four time one by one. After that second steps will be follow where whole image after first step will be divide in 7 equals parts and then I bit from every part will be selected and than generates a ASCII code from these 7 bits. We apply this operation for all bits in 7 parts of the image. And then apply different encryption operation to encrypt these ASCII code. Here both type of symmetric and asymmetric cryptography algorithm can be applied to change whole ASCII code. Finally originally image data will converted in to ASCII code data or Cipher text data. As shown in firg1 image can be dividing in 7 parts. In fig 1 image divided in typical scenario so that it will be very difficult to anyone who is unauthorized person or any unknown person to detect from where image is divided. Here image will be divided in 7 equal's bits length parts but position of every part is very difficult to in image to detect. That's one scenario here a lot of scenario can be applied to divide whole image in different equal length parts.

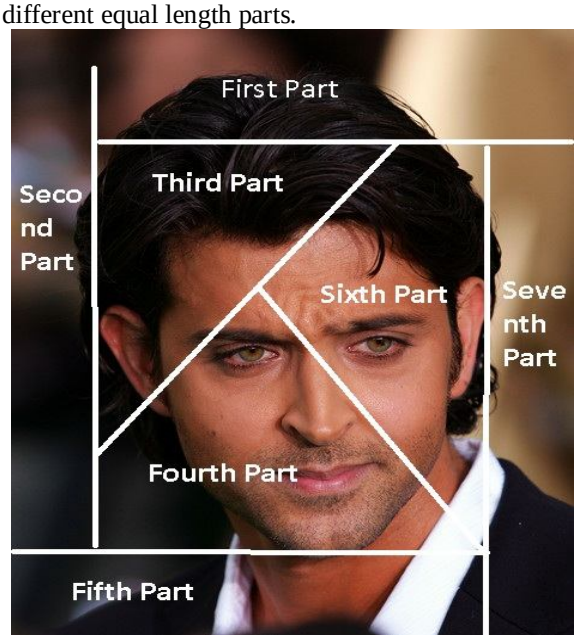

Fig1 shows 7 different parts of image with equal bits length

IV. KA ENCRPTION ALGORITHM

First Step:

(i) First of all select whole image and give named as I.
(ii) Then stored all the pixels value of I in two dimensional array named as P like every image have rows or column wise pixels.
(iii) Apply below operation A to H 4 times.
  A. Firstly row wise XOR all the bits of pixel from top to bottom like as firstly XOR first and second row and then store first row as XOR Result and second rows as it is than XOR second and third rows and store as according to previous operation and then apply to all the rows.
  B. Then apply above XOR operation (A) column wise to every column form left to right.
  C. Then apply above XOR operation (A) diagonally wise from left-top to right-bottom.
  D. Then apply above XOR operation (A) diagonally wise from right-top to left-bottom.
  E. Then apply above XOR operation (A) row wise to every row form bottom to top.
  F. Then apply above XOR operation (A) column wise to every column form right to left.
  G. Then apply above XOR operation (A) diagonally wise from right-bottom to left-top.
  H. Then apply above XOR operation (A) diagonally wise from left-bottom to right-top.
(iv) End.

Second Step:

(i) First of all divide whole image in two 7 equals' length parts.
(ii) Then select one bit from every parts and generates a ASCII code corresponding to selected 7 bits from 7 parts of images.
(iii) Then apple above (ii) operation on every bit of seven parts of image and convert whole image in ASCII code data.
(iv) Then apply different symmetric and asymmetric key encryption algorithm to encrypt that ASCII code data and finally makes the cipher text data.
(v) End.

V. KA DECRYPTION ALGORITHM

First step:

(i) First of select the whole Cipher data.
(ii) Then apply decryption operation of symmetric and asymmetric key according to as applied in encryption operations.

(iii) Then convert whole data into blocks of 7 bits length.
(iv) Then generates 7 one dimension arrays.
(v) Then add first bit of first block in first array and second bit of first block in second array and so on for all seven bits of first block.
(vi) Then apply (v) operation for all block bur in order as first of all first block then second block then so on for every block.
(vii) Now from these seven array makes two dimension array by storing all the bits in order that will be apposite as encryption process(dividing of whole image in 7 equals parts) hence a image come in two dimensions arrays.
(viii) End.

Second step:
(i) Apply below operation A to H 4 times.
A. Firstly diagonal wise XOR all the bits of pixel from right-top to left-bottom like as firstly XOR first and second diagonal and then store first diagonal as it is and second rows as XOR Result than XOR second and third diagonal and store as according to previous operation and then apply to all the diagonals.
B. Then apply above XOR operation (A) diagonally wise from left-top to right-bottom.
C. Then apply above XOR operation (A) column wise to every column form left to right.
D. Then apply above XOR operation (A) row wise to every row form top to bottom.
E. Then apply above XOR operation (A) diagonally wise from left-bottom to right-top.
F. Then apply above XOR operation (A) diagonally wise from right-bottom to left-top.
G. Then apply above XOR operation (A) column wise to every column form right to left.
H. Then apply above operation (A) row wise to every row from bottom to top.
(ii) Then store this two dimensional array in one dimensional array named as I as according to reverse of encryption operation(stored all the pixels value of I in two dimensional array named as P like every image have rows or column wise pixels).
(iii) Hence finally original image will be get without any loss.
(iv) End.

VI. RESULT

KA technique is a power full technique to encrypt image. In KA technique encryption process accrue in two different step first as image and second as ASCII code data. Hence KA technique secures the image more than other technique because its process is very difficult and also different operation of encryption accrue in two different steps which are totally different to each other and also complex to obtain second step from first step. Hence KA technique is very strong and power full technique to secure images over network as well as in storage media.

VII. FUTURE WORKS

KA technique can be use in video encryption hence in future video encryption algorithm can be proposed. KA technique works on two steps hence reverse of these two steps can be apply on the encryption of text data where text data will be converting in image data. Hence in future a lot of work can be done in KA technique like designing of algorithm for video, graphs, text any kind of data and in reverse for design of decryption algorithms.

CONCLUSION

Nowadays world is of internet, the security of images is most important. this paper have surveyed different image techniques and decryption technique. The security for the digital images has become most important since the communication by transmitting of digital products or data or images over the open network occur very frequently .Those encryption techniques which are discussed in this paper and laso analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. Newly proposed image encryption KA techniques is very useful technique because here mainly image data convert in to text data according to ASCII code hence whenever unauthorized person if decrypt this cipher text data than it is very difficult to know by him that it is image data or text data. Because here whole image data is send over network in text data. And different cryptography techniques applied on both image as well as text data which is generated after conversion of image in text data.

REFERENCES

[1] John Justin M, Manimurugan S , “A Survey on Various Encryption Techniques ”,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March2012.
[2] Ephin M, Judy Ann Joy and N. A. Vasanthi, “ Survey of Chaos based Image Encryption and Decryption Techniques ” ,Amrita International Conference of Women in Computing (AICWIC’13)Proceedings published by International Journal of Computer Applications (IJCA).

[3] .Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I8 (2203),229-234.[5]
[4] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN",
[5] Pattern Recognition 34,1229- 1245,2001.
[6] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.
[7] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems ",The Journal of Systems and Software 58 , 83-91,2001.
[8] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number, "Proceeding of the IEEE Inter Symposium On Circuits and Systems, Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.
[9] Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems",
[10] IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.
[11] Guosheng Gu ,Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm",
[12] IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control(ICICIC'06) in 2006.
[13] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.
[14] 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(ICEIE), 2010 International Conference.
[15] Wang Ying, Zheng DeLing, Ju Lei, et al., "The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004.
[16] Sesha Pallavi Indrakanti,P.S.Avadhani, "Permutation based Image Encryption Technique", I international Journal of Computer Applications (0975 – 8887) Volume 28 ,No.8, 2011.
[17] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University ,vol. 09 IEEE, 2012.

★★★