ISSN:0975-9646

A Survey On Different Image Encryption and Decryption Techniques.

Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya

Dept. of Computer Science
Lakshmi Narain College of Technology, Bhopal(India)

Abstract – **This paper focuses mainly on the different kinds of image encryption and decryption techniques. 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. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. This paper presents a survey of over 25 research papers dealing with image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. 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.**

Keywords- **Image Encryption, Image Decryption**.

I. Introduction

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging .Tele-medicine and military Communication, etc. The evolution 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 will be defined as the conversion of plain message into a form called 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 into its original plain text, so that it can be read [1].

Encryption of data [2] has become an important way to protect data resources especially on the internet, intranets and extranets. 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.

The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm [3] (ii) value transformation based algorithm and [4, 5] (iii) visual transformation based algorithm [3].

II. Literature Survey

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

Jiun-In Guo and Jui-Cheng Yen [3] have presented an algorithm which was mirror like. 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.

2. Lossless Image Compression and Encryption Using SCAN.

S.S. Maniccam and N.G. Bourbakis [4] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

3. New Encryption Algorithm for Image Cryptosystems.

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [6] 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.

4. Technique for Image Encryption using Digital Signatures.

Aloka Sinha and Kehar Singh [4] 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.

5. Technique for Image Encryption using multi-level and image dividing technique.

Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, and SmJmng Kim[7] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures is regenerate to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation.

6. Technique for Image Encryption using 1D chaotic map.

Fethi Belkhouche and Uvais Qidwai [8] used the method that can be used for binary images encryption with the possibility of using several keys ex: initial state, the external parameters and iterations' number.

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

They presented a method [09] for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real-time situations. 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.

8. Technique for Image Encryption using chaos technique.

Guosheng Gu and Guoqiang Han [10] made a new highly optimised image algorithm using permutation and substitution methods. It was done in order to enhance the pseudorandom characteristics of chaotic sequences, an optimized treatment and a cross-sampling disposal is used.

9. Technique for Image Encryption using chaos technique.

Huang-PeiXiao , Guo-ji Zang[11] made an algorithm using two chaotic systems . One chaotic system generates a chaotic sequence, which was changed into a binary stream 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 pixel values of the images was modified. Then, the modified image was encrypted again by permutation matrix.

10. Color Image Encryption Using Double Random Phase Encoding.

Shuqun Zhang and Mohammad A. Karim [12] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted 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. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods.

11. Modified AES Based Algorithm for Image encryption.

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [13] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (W7,A5/1) to AES for ensuring the encryption performance.

12. Image Encryption Using Block-Based Transformation Algorithm.

Mohammad Ali Bani Younes and Aman [14] 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 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.

13. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption.

Mohammad Ali Bani Younes and Aman Jantan [15] introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

14. Novel Image Encryption Algorithm Based on Hash Function.

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [16] proposed an algorithm based on SHA-512 hash function, which was novel algorithm. It had two sections. Firstly does pre-processing operation to shuffle one half of image then hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.

15. Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps.

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab [17] proposed chaos-based stream cipher, composing two chaotic logistic maps and external secret key for encryption of image. In this an external secret key of 104 bit and two chaotic logistic maps are used to differentiate between the encrypted image and the plain image. Further, the secret key is modified after encrypting of each pixel of the plain image which makes the encrypted image more robust. Then there is a feedback mechanism which increases the robustness of the proposed system.

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

Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M.[18] presented a modification to the Advanced Encryption Standard (MAES) to provide a high level security and better image encryption. The result shown by them was higher than that of original AES encryption algorithm.

17. Image Encryption Using Affine Transform and XOR Operation.

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [19] introduced a new algorithm using affine transform and was based on shuffling the image pixels. It was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

18. Permutation based Image Encryption Technique.

Sesha Pallavi Indrakanti and P.S.Avadhani[20] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provide confidentiality to colour image with less computations.

19. Image Security via Genetic Algorithm.

Rasul Enayatifar and Abdul Hanan Abdullah [21] proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

20. Image Encryption Based on the General Approach for Multiple Chaotic Systems.

Qais H. Alsafasfeh and Aouda A. Arfoa[22] proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rossler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed.

21. Statistical analysis of S-box in image encryption applications based on majority logic criterion.

Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal and Hasan Mahmood [23] propose a criterion to analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi Sboxes.

22. Image Encryption Using Differential Evolution Approach in Frequency Domain

Ibrahim S I Abuhaiba and Maaly A S Hassan [24] present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. In order to demonstrate the security of the new image encryption algorithm, key space analysis, statistical analysis, and key sensitivity analysis was carried out by them.

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

Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma [25] general random scrambling method was designed which has more stable scrambling degree than the classical method Arnold transform. At first, they decomposed a gray image into several bit-plane images. Then we shuffled them by a random scrambling algorithm separately. Lastly, we 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 located at the same coordinates in different bit-planes are almost not stay on the original positions when each bit-plane being scrambled separately. For each pixel, its 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. It is obvious that our method can do both positions exchange scrambling and gray level change scrambling at the same time.

CONCLUSION

This internet world nowadays, the security of images is very important. In this paper I have surveyed different image techniques and decryption in the span of 13 years (1999-2012). The security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently .Those encryption techniques are studied and 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 techniques and also enhance the security level by introducing more than one chaotic scheme for image encryption algorithms. A new algorithm for encrypting color images was also analyzed.

REFERENCES

[1] John Justin M, Manimurugan S , "A Surve on Various Encryption Techniques ", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.*

[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] 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.*

[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", *Pattern Recognition 34,1229- 1245,2001.*

[6] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", *The Journal of Systems and Software 58 , 83-91,2001.*

[7] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", *IEEE Proceeding in the year 2003.*

[8] Fethi Belkhouche and Uvais Qidwai , "Binary image encoding using 1D chaotic maps", *IEEE Proceeding in the year 2003.*

[9] 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.*

[10] Huang-Pei Xiao Guo-Ji Zhang, "An Image Encryption Scheme Based On Chaotic Systems", *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", *IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.*

[12] 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.*

[13] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption", *World Academy of Science, Engineering and Technology 27, 2007.*

[14] 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*

[15] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" , *IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.*

[16] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function*", 6th Iranian Conference on Machine Vision and Image Processing, 2010.*

[17] Ismail Amr Ismail, Mohammed Amin, Hossam Diab ,"A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", *International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.*

[18] 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 .*

[19] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation *",International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).*

[20] Sesha Pallavi Indrakanti,P.S.Avadhani, "Permutation based Image Encryption Technique", *International Journal of Computer Applications (0975 – 8887) Volume 28 ,No.8, 2011.*

[21] Rasul Enayatifar , Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", *2011 International Conference on Computer and Software Modeling IPCSIT vol.14.*

[22] Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", *Journal of Signal and Information Processing, 2011.*

[23] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion", *International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011.*

[24] Ibrahim S I Abuhaiba , Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach In Frequency Domain" , Signal & Image Processing An *International Journal (SIPIJ) Vol.2, No.1, March 2011.*

[25] 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***.**