A Survey on Various Encryption Techniques

John Justin M, Manimurugan S

Abstract-This paper focuses mainly on the different kinds of encryption techniques that are existing, and framing all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques, double encryption and Chaos-based encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues.

Keywords-Chaotic Encryption, Double Encryption, Image Encryption, Information Encryption.

I. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the digital images very drastically. Hence it is more vulnerable of duplicating of digital image and re-distributed by hackers. Therefore the images has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use.

Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues. The performance of all those encryption techniques are studied and discussed in later chapters of the paper.

II. LITERATURE SURVEY

To study and analyze more about the encryption techniques, the following literature survey has done and discussed in this chapter.

Manuscript Received January 09, 2012.
John Justin.M, PG Research Scholar,Image Processing Group,Karunya University,Coimbatore,India.(e-mail:johnjuztin@gmail.com)
Manimurugan.S, Assistant Professor,Dept of Computer Science and Technology, Karunya University,Coimbatore,India.
(e-mail: smanimurugan@yahoo.co.in)

A. Encryption

Encryption can 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. 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.

Dahua Xie and Jay Kuo have proposed an encryption technique with enhanced Multiple Huffman Table (MHT) by key hopping method. The previously developed Multiple Huffman Table (MHT) has good desirable properties but it was highly vulnerable to the chosen plaintext attack (CPA). Whereas this enhanced MHT encryption method faces all such limitations. As the result shown, that the algorithm is secure for the chosen plaintext attack and proved mathematically by the key hopping method.[1]

Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor has jointly framed a manuscript for Classifying the Encryption Algorithms in accordance with the Pattern Recognition method. In this discussion the authors focuses on the limitations of the algorithms which are used for encryption scheme and for generating the keys for encryption process. Here the pattern recognition method to identify the block ciphers in encryption process. The block cipher algorithms like AES, DES, IDEA, and RC were used to identify the good classification technique. As the result shown, that the performance of RoFo (Rotaion Forest) classifier has the very good classification accuracy.[2]

A Study on OMAP (Open Multimedia Applications Platform) Digital Fingerprint Encryption technique has done by Zhu Yuxi. In this study the author deals with the identification of the fingerprint and the security in transmission for the embedded systems. Here a digital fingerprint technique was used with the structure of the OMAP (Open Multimedia Applications Platform). The author designed an integrated software structure with an application platform.[3]

Huang Jinga,b Zheng Zhen-zhuc has developed an optical encryption technique for secure real time image transmission. Because of any image hold a huge amount of data or information, which results in very less efficiency of the real time image encryption. The authors has proposed a new scheme for image encryption which is used in optical computing technologies that apparently focuses on images and large amounts of data simultaneously, as the result of this high speed is attained. Hence this scheme was implemented by using a stream cipher on the polarization encoder as the optical logic gates. The

results states very good security for the images with histogram.[4]

Mort Naraghi-Pour and his colleagues have developed a simple encryption standard for secure detection in the wireless sensor networks. Only the authorized user or the ally fusion center (AFC) is aware of the encryption method its features, and no unauthorized or any third party fusion centers (TPFC) are not aware of such encryption features. As the result shown, the exact threshold value was found and the numerical results were evaluated for the error probabilities of the two fusion centers (AFC and TPFC).[5]

An iterative speech encryption scheme basis of subspace method was proposed by Atef Mermoul. Blind source separation (BSS)-based encryption schemes have been built up using the intractability of the under determined BSS problem. In this paper, the author designed a novel encryption scheme that is iterative and based on the idea of subspace technique, by the nonlinear functions and the key signals. It is proved here that only a part of the secret key parameters were used in encryption process is needed for the decryption process. Also this technique gives no contents if no plain-text is fed in the input.[6]

B. Image Encryption

The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

Osamu Watanabe et al have jointly developed a scalable encryption method which comprises of backward compatibility with the JPEG2000 Images. This encryption technique tells the encrypted images to hold the multilevel encryption method also decreases the computational complexity of the encryption process. In this paper the standard JPEG 2000 decoder is used to decode the encrypted images and some parameters of JPEG 2000 were saved after the encryption process. As the result of this, the duration of the encryption process is controlled by selective encryption algorithms to promote faster processing.[7]

Analysis on encryption techniques with JPEG Images was done by W. Puech, and J.M. Rodrigues. This paper mainly focuses on the draw backs of both the selective encryption (SE) and the image compression. The SE (selective encryption) can be made by Advanced Encryption Standard (AES) algorithm incorporate with the Cipher Feedback (CFB) mode. And for the compression, the JPEG algorithm has been used. Here the SE was done in the stage of Huffman coding in JPEG algorithm which does not affects the size of the compressed image. The results shows the application of SE in JPEG compressed images.[8]

Mahmood Al-khassaweneh and Selin Aviyente has put forth a novel image encryption technique based on the concept of Least Square Approximation (LSA) .In this paper, the conversion of the original image into the form of encrypted one by the randomly generating vectors. And on the other hand the original image has been decrypted by using the least square approximation concept on the encrypted image and also on the randomly generating vectors. As the result of this, there is a good range of efficiency in this algorithm and also promotes good enhancement in the security aspects.[9]

Syed Ali Naqi Gilani, M. Ajmal Bangash has developed an enhanced block based image encryption Scheme with Confusion. The authors designed the Block-Based Image Encryption Algorithm (BBIE) which works together with the Blowfish Encryption algorithm. Here the digital image is decomposed into slices, after those two continuous actions that are rotating each 3D true color image slice to 90° which is then follow up by flipping row wise down were done. Also the rendered blocks were then undergo the process of scrambling into the form of converted confused image which is finally follow up by the Blowfish cryptosystem which is actually the process of encryption of the image using a secret key. The result shown that, the correlation between adjacent pixels has been reduced in all the color component.[10]

Seyed Hossein Kamali et al have framed an image encryption algorithm of enhanced model of Advanced Encryption Standard. The authors proposed an enhanced model of Advanced Encryption Standard to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original AES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks.[11]

An encryption technique to embed the watermarking idea to promote the security was proposed by Mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat.In this paper, 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.[12]

B.V.Rama Devi and her colleagues have jointly developed a novel encryption method for securely transmitting of images. Thus the encryption method is called godelization which is follow up by the public key encryption. Here the input image has been transformed to a process called Godel Number Sequence (GNS).as the result of this the encryption string has been transmitted and been reconstructed in the decoding phase by the reverse process.[13]

C. Information Encryption

Xu E, Liangshan Shao, Guanghui Cao, Yongchang Ren, Tao Qu has put forth a new technique for information encryption. The authors proposed a block chaos image scrambling and the chaos encryption. Here the block permutation provides the formula for correlation which also compares the correlation before and after the permutation process. As the result shown that the image encryption algorithm promotes strong resistance towards the statistical attacks and differential attacks.[14].

D. Double Encryption

A new double random phase encryption method has been proposed by Ayman Alfaloul, and Ali Mansour to multiplex and simultaneously encodes multiple images. This method can enhance the level of encryption of a classical "DRP" Double Random Phase encryption system this promotes a very simple implementation, robustness, and can easily apply on various image formats. This technique deals with two tiers. The first tier is multiplexing which performs iterative Fourier transformations together with several encryption key-images. And the second tier is classical DRP system. Both the tiers produces encoding of several target images and reduces the time and storage complexity.[15]

E. Chaotic Encryption

Chaos-based encryption is one of the applications of the nonlinear dynamics of chaotic finder. It meets the issues that are creating the problem of encryption, the different kinds of image encryption techniques that are based on the chaotic schemes are discussed in the following paragraphs.

Qiang Wang et al have undergone a research on the digital image encryption which is based on the DWT (discrete wavelet transform) and Chaos. In this discussion, a digital image watermark algorithm has been developed that is based on the concept of discrete wavelet transform (DWT) and chaos theory. First, the discrete wavelet transform has to be done to retrieve the low frequency part as embedding field; secondly the chaotic sequence has to be done to encrypt the watermark to retrieve the low frequency, and to embed with the original image. As the result of this, this technique promote the resistance on JPEG compression, noise attack, filter and so on.[16]

Yong-Hong Zhanghas designed and developed an image encryption using extended chaotic sequences. In this study, the chaotic cryptography technique is used which is called a key cryptography. Here, the extended chaotic processes are generated by using the *n* -rank rational Bezier curve. Results shows that the high key space and good security level.[17] .

Monisha Sharma and Manoj Kumar Kowar have done a review on image encryption techniques using chaotic schemes. In this manuscript, the chaotic image encryption is made possible by the parameters of chaos which includes the deterministic dynamics, unpredictable behavior and non-linear transform. Which leads to the techniques that provide security features and a complete visual check.[18]

Mintu Philip and Asha Das have jointly done a survey on image encryption process by using the chaotic cryptography schemes. The author states that the cryptography uses the chaotic system features namely the loss of information and the initial condition from sensitive condition. They have concluded the paper with comparisons made out of the performance of the existing chaotic image encryption methods.[19]

Jun Lang, Ran Tao, Yue Wang has proposed an image encryption technique which is based on the concept of multiple parameter discrete fractional Fourier transform and the chaos function. In this paper, the image is encrypted by the position of the images in many arguments of the discrete fractional Fourier block whereas the alignment of the sections is evaluated by chaotic logistic maps. As the result of this, comparison has been made in between the various existing schemes and posses' good or superior robustness [20].

F. Performance Parameters

According to Suhaila O. Sharif et al proposal, eight classifiers were used to identify the cipher text they are Naive Bayesian, Support Vector Machine, neural network ,Instance based learning , Bagging, AdaBoostM1, Rotaion Forest, Decision Tree and its accuracy were calculated. The aim was to find the best classification algorithm with high accuracy for four different block ciphers called DES, IDEA, AES, and RC2. Resulted in, the RoFo (Rotaion Forest) classifier has the highest classification accuracy of (53.33 %) meaning that 128 out of 240 input data were correctly classified.[2]

According to Jolly shah and Dr. Vikas Saxena in a survey manuscript on video encryption defined a set of parameters based on which the performance can be evaluated and compared with the existing video encryption algorithms such parameters are visual degradation (VD), encryption ratio(ER), speed(s), compression friendliness(CF), format compliance(FC) and Cryptographic security (CS)[21].

III. CONCLUSION

In this internet world nowadays, 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. In this paper, it has been surveyed that the existing works on the encryption techniques. 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.

REFERENCES

[1] Dahua Xie and C.-C. Jay Kuo, "Enhanced multiple Huffman table (mht) encryption scheme using key hopping" IEEE Transactions pp. 568-571,2004

[2] Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor ,"Classifying Encryption Algorithms Using Pattern Recognition Techniques" IEEE Transactions pp. 1168-1172,2010

[3] Zhu Yuxi, Ruchun Cui, "Applied Study Based on OMAP Digital Fingerprint Encryption Method" IEEE Transactions pp. 1168-1172,2010

[4] Huang, Jing, Zheng Zhen-zhuc, "A Method for Secure Real-Time Image Transmission Based on Optical Encryption" International conference on the Intelligent Signal Processing and Communication Systems, 2010

[5] Mort Naraghi-Pour, Venkata Sriram Siddhardh Nadendla," Secure Detection in Wireless Sensor Networks Using a Simple Encryption Method" IEEE Transactions, 2011

[6] Atef Mermoul, "An Iterative Speech Encryption Scheme Based On Subspace Technique" IEEE Transactions on Systems, Signal Processing and their Applications, pp. 361-364, 2011.

[7] Osamu Watanabe, Akiko Nakazaki And Hitoshi Kiya," A Scalable Encryption Method allowing Backward Compatibility with JPEG2000 Images" IEEE Transactions pp. 6324-6347,2005.

[8] W. Puech, J.M. Rodrigues," Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images" IEEE Transactions on Image Analysis for Multimedia Interactive Services,2007.

[9] Mahmood Al-khassaweneh, Selin Aviyente,"Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.

[10] Syed Ali Naqi Gilani , M. Ajmal Bangash, "Enhanced Block Based Color Image Encryption Technique with Confusion" IEEE Transactions pp. 200-206,2008.

[11] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard(AES) Based Algorithm for Image Encryption", IEEE Transactions on Electronics and Information Engineering, Vol 1,pp.141-145,2010

[12] Mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat, "A New Encryption Method For Secure Embedding In Image Watermarking" IEEE Transactions on Advanced Computer Theory and Engineering pp. 403-407,2011.

[13] B.V. Rama Devi et. al., " A Novel Encryption Method for the Secure Transmission of Images" International Journal on Computer Science and Engineering, Vol. 02, No. 09, pp.2801-2804, 2010.

[14] Xu E, Liangshan Shao, Guanghui Cao , Yongchang Ren , Tao Qu, "A New Method of Information Encryption" IEEE Transactions pp. 583-586,2009.

[15] Ayman Alfalou and Ali Mansour, "A new double random phase encryption scheme to multiplex and simultaneous encode multiple images" Applied Optics, pp. 5933-5947, 2009.

[16] Qiang Wang, Qun Ding , Zhong Zhang, Lina Ding, "Digital Image Encryption Research Based on DWT and Chaos" IEEE Transactions pp. 494-498,2008.

[17] Yong-Hong Zhang, "Image encryption using extended chaotic sequences", IEEE Transactions International Conference on Intelligent Computation Technology and Automation pp. 143-146,2011.

[18] Monisha Sharma et. al. "Image Encryption Techniques Using Chaotic Schemes: A Review" International Journal of Engineering Science and Technology, Vol. 6,pp. 2359-2363, 2010.

[19] Mintu Philip, Asha Das, " Survey: Image Encryption using Chaotic Cryptography Schemes" International Jounal of Computer Applications,2011.

[20] Jun Lang, Ran Tao, Yue Wang, "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function" Optics Communications, Vol 283, pp. 2092-2096, 2010.

[21] Jolly shah and Dr. Vikas Saxena, "Video Encryption: A Survey" International Journal of Computer Science Issues, Vol. 8, pp. 525-534, 2011.

AUTHOR PROFILE

1. John Justin.M received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2010,and pursuing his M.Tech degree in Software Engineering in Karunya University, Coimbatore, India. His research interests include Image Processing, Software Engineering.

2. Manimurugan.S received the B.E. degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2005, and the M.E. degree in Computer Science and Engineering in 2007. He is currently pursuing the Ph.D. degree in Computer Science and Engineering in Anna University, Coimbatore, India. His current research interests are in Image Processing, Information Security.