International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012)

A survey report on Different Techniques of Image Encryption

Abhinav Srivastava[1]
[1]CSE Dept, IT-GGV, Bilaspur, India

***Abstract*— In the present world when whole web is now coming on from text data to multimedia data, one of the major security concerns is the protection of this multimedia data. Image, which covers the highest percentage of the multimedia data, its protection is very important. This can be achieved by Image encryption. There are so many different techniques should be used to protect confidential image data from unauthorized access. In this paper, I had done the literature review on existing work which is used different techniques for image encryption from 1999 to 2011 and also given general introduction about cryptography and encryption.**

***Keywords*— Cryptography, Image, Encryption, Security, chipper.**

I. INTRODUCTION

Today web is going towards the multimedia data in which image covers the highest percentage of it. But with the ever-increasing growth of multimedia applications, security is an important aspect in communication and storage of images, and encryption is the way to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand and to keeps the image confidential between users, in other word, it's important that without decryption key no one can access the content. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication; etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the old system takes more time for encrypting the image data directly. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Thus to do the encryption of the images various algorithms are proposed. (i) position permutation[1] , (ii) value transformation [1] and (iii)visual transformation[1]

This paper is organized as follows In Section 1; I am presenting general guide line about cryptography and encryption. In Section 2, I have presented literature review on existing research paper. Finally, I conclude in section 3.

Cryptography (or cryptology; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively)is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. [2]

Plain Text [3]: Plaintext is information a sender wishes to transmit to a receiver.

Cipher text [4]: Cipher text (or cypher text) is the result of encryption performed on plaintext using an algorithm, called a cipher.

Encryption is the process of transforming the image into some other image using an algorithm so that any unauthorized person cannot watch it. Only the person who has a key (anti of that algorithm) can watch that image5.

Types of Cryptography:

There are two main types of cryptography:

1. Secret key cryptography
2. Public key cryptography

Secret key cryptography (symmetric key cryptography): In this, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called asymmetric key cryptography. It used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys.

A technique in which secret messages are transferred from one person to another over the communication line, the process is called Cryptography. Cryptography technique needs some algorithm for encryption of data.

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, security and safety of information should be ensured. Image is also an important part of our information. Therefore it's very important to protect our image from unauthorized access. There are so many algorithms available to protect image from unauthorized access which is described in next section.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012)

II. Literature Review

A. New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture (1999)

Jiun-In Guo and Jui-Cheng Yen [7] 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.

B. Lossless Image Compression and Encryption Using SCAN (2001)

S.S. Maniccam and N.G. Bourbakis [8] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based 2D spatial-accessing methodology generate a wide range of scanning paths or space filling curves

C. New Encryption Algorithm for Image Cryptosystems (2001)

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [9] 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. Technique for Image Encryption using Digital Signatures (2003)

Aloka Sinha and Kehar Singh [10] 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.

E. Technique for Image Encryption using multi-level and image dividing technique, 2003

Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, and SmJmng Kim[11] 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 images is converted to binary phase encoding and then these images are encrypt with binary random phase images by binary phase XOR operation

F. Technique for Image Encryption using 1D chaotic map, 2003

In 2003 Fethi Belkhouche and Uvais Qidwai [12] 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.

G. New Chaotic Image Encryption Algorithm , 2004

Zhang Han, Wang Xiu Feng [13], Firstly permutation transform and then nonlinear map to circularly iterate pixel values. Failure of encryption owing to self-similarity and visional psychological characteristics of image.

H. Technique based on T-matrix, 2004

M.-R. Zhang, G.-C. Shao and K.-C. Yi [14] used a T matrix for image scrambling. The T-matrix has a simple conformation and a period twice of the Arnold matrix. This can be applied to image encryption and pre-processing in image processing such as image watermarking algorithms and etc.

I. A Chaotic Neural System based encryption scheme, 2005

Deng Shaojiang [15] completed an image encryption by a chaotic neural system and the cat map. In this, for making the technique chaos, the neural networks was used.

J. Technique for Image Encryption using chaos technique, 2006

Guosheng Gu and Guoqiang Han [16] 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.

K. Technique for Image Encryption using chaos technique, 2006

Huang-PeiXiao , Guo-ji Zang[17] 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012)

L. Modified AES Based Algorithm for Image encryption, 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [18] 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.

M. Image Encryption Using Block-Based Transformation Algorithm, 2008

Mohammad Ali Bani Younes and Aman [19] 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.

N. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [20] 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 colour images. Their algorithm works well for all types of gray scale as well as colour images except for those images which have background of same gray level or of same colour.

O. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008

RijnDael was introduced by Mohammad Ali Bani Younes and Aman Jantan [21] using the combination of image permutation. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then RijnDael algorithm was applied on the generated image for encryption. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

P. Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [22] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption.

They proposed AdvHill cipher algorithm using the old one. And it is clearly seen that original Hill Cipher is unable to do its working properly as it did not encrypt the images properly if the image consists of large area covered with same colour or gray level. But their proposed algorithm works for any images with different gray scale as well as colour images.

Q. Digital image encryption algorithm based on chaos and improved DES, 2009

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [23] researches on the combination of image encryption algorithm like chaotic encryption, DES encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used, it carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. This algorithm had high security and the encryption speed.

R. Novel Image Encryption Algorithm Based on Hash Function, 2010

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [24] proposed an algorithm based on SHA-512 hash function, which was novel algorithm. It had 2 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.

S. Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, 2010

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab [25] 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.

T. New modified version of Advance Encryption Standard based algorithm for image encryption, 2010

Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M.[26] 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012)

U. Image Encryption Using Affine Transform and XOR Operation, 2011

Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar[27] 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.

V. Permutation based Image Encryption Technique, 2011

Sesha Pallavi Indrakanti and P.S.Avadhani[28] 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.

W. Image Encryption Based on the General Approach for Multiple Chaotic Systems, 2011

Qais H. Alsafasfeh and Aouda A. Arfoa [29] proposed a new algorithm by adding the Lorenz chaotic system and the Rössler chaotic system. From analysis through experiment, they shown the advantages of image encryption algorithm which was high obscure level and high speed, large key space and high-level security.

X. Image Encryption Using Differential Evolution Approach In Frequency Domain, 2011

Ibrahim S I Abuhaiba and Maaly A S Hassan[30] 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.

III. Conclusion

In today's world where nothing is secure, the security of images is very important. In this paper I have surveyed different image techniques in the span of 12 years (1999-2011).

I conclude that all techniques are good for image encryption and have their own advantages and disadvantages and give a security so that no one can access the image which is in the open network.[32]

REFERENCES

[1] http://www.waset.org/journals/waset/v3/v3-7.pdf Analysis and Comparison of Image Encryption Algorithms by Ismet Öztürk and Ibrahim Soukpinar.

[2] http://en.wikipedia.org/wiki/Cryptography

[3] http://en.wikipedia.org/wiki/Plaintext

[4] http://en.wikipedia.org/wiki/Ciphertext

[5] http://en.wikipedia.org/wiki/Encryption

[6] Image Using Different Technique A Review: Komal D Patel, Sonal Belani (ISSN 2250-2459, Volume 1, Issue 1, November 2011).

[7] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

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

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

[10] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[11] 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.

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

[13] 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

[14] M.-R. Zhang, G.-C. Shao and K.-C. Yi, " T-matrix and its applications in image processing", IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25

[15] Shaojiang Deng, Linhua Zhang, and Di Xiao, "Image Encryption Scheme Based on Chaotic Neural System", J. Wang, X. Liao, and Z. Yi (Eds.): ISNN 2005, LNCS 3497, pp. 868-872, 2005.

[16] 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.

[17] 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.

[18] 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.

[19] Mohammad Ali Bani Younes and Aman Jantan ImageEncryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,2008.

[20] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008

[21] 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.

[22] 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

[23] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[24] 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.

[25] 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.

[26] 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.

[27] 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).

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

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

[30] Ibrahim S I Abuhaiba , Maaly A S Hassan, Image Encryption Using Differential Evolution Approach In Frequency Domain

[31] Revised for accepted but unpublished paper of min Different Techniques of Image encryption : A literature Review at IJETAE

[32] Fews texts taken as reference from the papers : http://www.waset.org/journals/waset/v3/v3-7.pdf Analysis and Comparison of Image Encryption Algorithms by Ismet Öztürk and Ibrahim Soukpinar , Image Using Different Technique A Review: Komal D Patel, Sonal Belani (ISSN 2250-2459, Volume 1, Issue 1, November 2011) and http://www.ijest.info/docs/IJEST10-02-06-142.pdfThey are in edited language and I give thanks to those writers.