IJMEIT
IGM Publication
International Journal Of Mechanical Engineering And Information Technology
An Official Publication Of IGM Publication

Development of a New Secure Algorithm for Encryption and Decryption of Images

Authors

Suman Yadav[1], Puneet Garg[2]
[1]M. Tech. Scholar, GITAM, Kablana, Jhajjar, Haryana
[2]Asst. Professor Scholar, GITAM, Kablana, Jhajjar, Haryana
Email-id- *sysumanyadav52@gmail.com*

ABSTRACT

Image encryption plays an important role in the field of information security. Most of the image encryption techniques have some security and performance issues. So there is a need to compare them to determine which method is suitable for the application. Chaos based encryption algorithms are employed nowadays because of their better security and performance aspects. Chaotic behavior of a system is t he sophisticated nature of a nonlinear system that looks random. This work is a review of two novel chaos based image encryption algorithms, namely a secure image encryption algorithm based on Rubik's cube principle and a new chaos-based fast image encryption algorithm in terms of the parameters like NPCR.

Keywords— *Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography.*

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. 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. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed.

The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm [1] (ii) value transformation based algorithm and [2, 3] (iii) visual transformation based algorithm [1]

This paper is organized as follows In Section 1; we present general guide line about cryptography. In Section 2, we survey on already existing research paper. Finally, we conclude in section 3.Plaintext[4]: An original message is known as plaintext. Cipher text [4]: Coded message is called cipher text. Encryption or Enciphering [4]: the process from converting plain text to cipher text is called Encryption or Enciphering. Decryption or Deciphering [4]: Restoring plain text from cipher text is called decryption or Deciphering. Cryptography [4]: The many schemes used for enciphering constitute the area of study known as cryptography.

Types of Cryptography:

There are two main types of cryptography:

- ✓ Secret key cryptography
- ✓ Public key cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, 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 Cryptograph uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of mathed public and private keys. Cryptography technique is used when secret message are transferred from one party to another over a communication line. 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, we need to ensure information security and safety. 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.

II. LITERATURE SURVEY

Modified AES Based Algorithm for Image encryption, 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki[5] 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.

Image Encryption Using Block-Based Transformation Algorithm, 2008

Mohammad Ali Bani Younes and Aman [6] 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, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. 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.

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

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [7] 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 the images with background of same gray level or same colour.

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

Mohammad Ali Bani Younes and Aman Jantan [8] 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.

Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [9] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed

AdvHill cipher algorithm. And it is clearly noticeable that original Hill Cipher can't 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.

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 [10] researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES.Their result show high starting value sensitivity, and high security and the encryption speed.

A Novel Image Encryption Algorithm Based on Hash Function, 2010

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [11] proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses 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.

A Digital Image Encryption Algorithm Based

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab[12]

Introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. In the proposed image encryption scheme, an external secret key of 104 bit and two chaotic logistic maps are employed to confuse the relationship between the cipher image and the plain image. Further, to make the cipher more robust against any attack, the secret key is modified after encrypting of each pixel of the plain image. The robustness of the proposed system is further reinforced by a feedback mechanism, which makes the encryption of each plain pixel depends on the key, the value of the previous cipher pixel and the output of the logistic map (data dependent property).

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

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.

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[14] propose a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation. They redistribute the pixel values to different location using affine transform technique with four 8-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 total key size used in algorithm is 64 bit. Their results proved that after the affine transform the correlation between pixel values was significantly decreased.

Permutation based Image Encryption Technique, 2011

Sesha Pallavi Indrakanti and P.S.Avadhani[15] proposes a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provide confidentiality to color image with less computations Permutation process is much quick and effective. The key generation process is unique and is a different process

Image Security via Genetic Algorithm, 2011

Rasul Enayatifar and Abdul Hanan Abdullah[16] 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.

Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it, 2011

Kuldeep Singh and Komalpreet Kaur[17] are compared four chaotic maps Cross chaotic, Logistic, Ikeda and Henon map and noise effects are observed on image. Firstly, they use the image encryption algorithm to convert original image to encrypted image. Then they apply noise on the encrypted image and then decrypt cipher image with noise back to original image. They have found out that cross chaotic map showed best results than other three chaotic maps.

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

Qais H. Alsafasfeh and Aouda A. Arfoa[18] proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler 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.

Image Encryption Using Differential Evolution Approach In Frequency Domain, 2011

Ibrahim S I Abuhaiba and Maaly A S Hassan[19] present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. They have carried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security of the new image encryption procedure.

Statistical analysis of S-box in image encryption applications based on majority logic criterion, 2011

Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal and Hasan Mahmood[20] 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.

III. CONCLUSION

In the digital world nowadays, the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. In this paper, we have surveyed existing work on image encryption. We also give general guide line about cryptography. We conclude that all techniques are useful for real-time image encryption. Techniques describes in this paper that can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access image which transferring on open network. In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security

IV. REFERENCES

[1] 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.

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

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

[4] William stallings, ―Cryptography and Network Security: Principles & Practices‖, second edition.

[5] 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.

[6] Mohammad Ali Bani Younes and Aman Jantan ―Image Encryption Using Block-Based Transformation Algorithm‖ IAENG International Journal of Computer Science, 35,2008.

[7] 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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[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 (ICEIE), 2010 International Conference.

[14] 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).

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

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

[17] Kuldeep Singh, Komalpreet Kaur,‖ Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it‖, International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, June 2011.

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

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