International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 07, July 2017
ISSN: 2455-3778
http://www.ijmtst.com

A Review on Various Encryption Techniques and Quality Metrics for Images

Arunpandian S[1] | Dr. K. Mahesh[2]

[1]M.Phil., Scholar in Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.
[2]Professor, Departmentof Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India.

To Cite this Article
Arunpandian S and Dr. K. Mahesh, "A Review on Various Encryption Techniques and Quality Metrics for Images", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 07, July2017, pp. 72-76.

ABSTRACT

In the competitive modern world, the entire transactions and communications are converted into electrically. Off course all transactions are being done with in a period of time to decrease the man power process. One important and hectic thing is needed here to enhance the perfect transaction is called as "security". Recent day's security assumes an essential part for whole electrical exchanges. For, most of the online business, interaction between websites and servers uses cryptography concepts to maintain their secrets in secured manner. In cryptography, lot algorithms were designed for working with text, image as well as video. These types of cryptographic encryption algorithms are entirely working against hacker's knowledge. Encryption techniques are considered by two varieties that are, public and private. The main difference between public and private algorithm is, in public system, need 3000 bit key to achieve the same level of security of a 128 bit private system. Asymmetric algorithms are incredibly slow and it is impractical to us them to encrypt large amounts of data. Symmetric algorithms are about 1000 times faster than Asymmetric ones. This article shows the collection of encryption techniques particularly for image and evaluates these techniques based on the performance metrics.

KEYWORDS:*Cryptography, electrical communication, image encryption, online transaction, performance metrics, website security.*

I. INTRODUCTION

A. Why Cryptography is needed still

Nowadays people wants to survey their life with electrical techniques and components, one of these technique is cryptography. Cryptography allows the people to enrich the electrical world (like secret transactions) with more confidence. Lot of techniques is designed by cryptography concepts to recover the secrets from the harmful hackers. There are millions of computers are interconnected on the internet to do the transactions, to start a secret communication cryptography is needed today. Based on the internet the role of cryptography is to secure websites and provides safe transmissions. In the today's modern world, cryptography allows people to do their purchases through the online banking and a credit card without worrying their account data is being theft. In our daily works cryptography is used in the following fields,

1. Remote keyless system in car
2. Provide secure Wifi network using WPA security(Application of cryptography algorithm)
3. RFID Smart cards
4. In entertainment equipment using broadcast encryption

5. In Whatsapp, developers use cryptographic algorithm to secure the end users personal data
6. In mobile phone, communication between mobile and base station is encrypted using cryptographic techniques.

To encrypt both text and image data, lot of cryptographic techniques areapplicable. These crypto techniques are considered by two main metrics, which are, Symmetric crypto technique and Asymmetric crypto technique. In Asymmetric system, two distinct keys are used for encryption and decryption. In Symmetric systems, the similar key is used for encryption as well as decryption. The research in image encryption is peak today. The collection of secrets bundled on encrypted image is considerable as more secure. There are plenty of cryptography techniques are available for image encryption. In this paper provides entire survey on cryptographic techniques which has been used for image encryption.

II. RELATED WORK

K.Berlin, A.Padmapriya [1], authors designed new encryption scheme for color images named as A Novel Threshold based Image Encryption for bitmap Images. Here, the color images are converted into gray to proceedtheir preprocess. In this, the working process is divided into two parts, one is threshold calculation based on the 16 × 16 matrix values that are computed from the converted gray image. Second one is encryption based on the symmetric key encryption cipher. Through their research, authors achieved highest encryption entropy.

New encryption method was designed by K.Kanagalakshm and M.Mekala [2] named as Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key. Here, the enhanced Blowfish algorithm and Supplementary key also used for increase the security strength. The performance factors are analyzed such as time and space.

Xiaofeng Li and Yinhui Zhang [3] developed cryptographic technique for digital images that research was entitled as Digital Image Encryption and Decryption Based on Wavelet Transform and Chaos System. Here the 2-D Discrete Wavelet Transform and Chaos system used for encryption and for decryption the Wavelet reconstruction method is obtained. Finally the author says their proposed digital image encryption technique gives high security with encrypted image and small distortion has made with decrypted image.

The new cryptographic based method "Performance Analysis of Threshold Based Image Encryption" was designed by K. Berlin and A. Padmapriya [4]. Here authors had done their image encryption with the help of threshold computation. Factors are analyzed to justify the security of the concern encryption technique. Through their research, the authors increased the image entropy and reduced the encryption time too.

Yashpalsingh Rajput and A K. Gulve [5], the authors proceed their encryption for images with Extended Hill Cipher. This image encryption method was known as An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher. The entire encryption technique done through three different phases, first one is the input image converted into digits. Second one is, bit rotation, reversal and randomization techniques are proceed with images. Third part is the extended Hill Cipher technique is applied on the images. Through their work, authors achieved decreased amount of correlation among the pixels that are obtained by the encrypted images.

III. SUITABLE ENCRYPTION TECHNIQUES FOR COLOR IMAGES

In color image, which has more number of intensity values (RGB) based on the resolution of an image. When the color image encryption, stream cipher could provide the standard methods for encryption and decryption process. Stream cipher is a secret key cipher where plaintext digits are mutually with key streams. Stream cipher works on byte-at a time basis using an input stream. A key stream is a stream of unequal or pseudorandom characters that are consolidated with a plaintext message to generate a scrambled message.

Following Stream cipher techniques are used in image encryption and decryption.

A. Rc4 Stream Cipher

RC4 encryption algorithm is shared key stream cipher, which is needed to secure exchange the content. Symmetric key algorithm usually works as identically for encryption and decryption such as the data stream is typically ex-ored with generated key sequences. Wireless encryption protocol 802.11 also used RC4 stream cipher for an encryption.

B. Four Feistal Structure

Feistel cipher is symmetric structure which can help to build the block ciphers. Normally fiestal development is an iterative procedure which makes actualizing the cryptosystem in equipment less demanding. In feistal cipher, the encryption process is dividing into halves. The round capacity is connected in one half utilizing sub key and another half is utilized restrictive than two parts are swapped. Every round pursue the similar pattern exclude for the final proceeding round where there is no swap

C. Rubik cubes

Rubik cube is a one of the image encryption technique. This is 3-D Combination Puzzle. It comprises the two major techniques such as encryption and watermarking, which is used to increase the data protection. While use the rubik cube algorithm, scramble the pixel values by changing the position of a pixel and pick the two random numbers. XOR operation performed on the odd rows and columns. After the above operation has done the original image converted into an encipher form. This gives high security and quick encryption for constant web transmission.

IV. SUITABLE ENCRYPTION TECHNIQUES FOR GRAY IMAGES

Gray scale image is a collection or the range of monochromic shades. Range means lightest end consist pure white, and opposite end has pure black. It contains only luminance information whereas digital image contains the RGB and luminous information. When compare to the color image, gray scale picture consist of less intensity values. It doesn't have RGB values. In color image encryption, this has to be change into the gray scale image and then add the key value to encipher process.

A. Hill cipher

Hill cipher is a traditional cryptography technique and polygraphic substitution cipher depends on the linear algebra which comes under the block cipher algorithm. According to hill cipher, it has matrix computation which is needed to encrypt and decrypt the information. In image encryption, R, G, B pixel values are extracted from the original image respectively. RGB values are required to build the Matrix form. Then hill cipher algorithm has applied on it to scrambled information.

B. Genetic Algorithm

Genetic Algorithm is a one more model for computation and search based optimization technique. Typically, it is needed to solve the huge optimization problem. It consists of major properties such as Crossover, Mutation, Fitness function and selection. Few image encryption and decryption has done by the genetic algorithm and iterative process to make the standard security for optimization.

V. PERFORMANCE ANALYSIS BASED ON QUALITY METRICS

A. MSE (Mean Square Error)

MSE is the Error metric technique to measure the encrypted and compressed of an image, which is closely related to regression line. It represents the set of points(x, y value) and squaring them. The squaring is needed to eliminate the any negative sign. It gives huge weight also to larger difference.

B. Find the Regression Line

Insert the x values into the linear regression equation to find the y values.
Subtract the new y value from original to get the error.
Square the error & add up the error
Find the mean value using following formula

$$MSE = 1/MN \sum_{Y=1}^{M} \sum_{X=1}^{N} [I(X,Y) - I(X,Y]\ 2 \quad (1)$$

It is a consolidate squared Error between the original and encrypted image.

C. Peak Signal to Noise Ratio

PSNR is often used as a quality measurement in between the encrypted and compressed image. It measures the peak value error, which is the better quality of encryption or reconstruct the image.

$$PSNR = 10 \log10(R2/MSE) \quad (2)$$

R is the maximum fluctuation in the input image.

D. Signal to Noise Ratio

SNR is used as a physical measures the sensitive of an image. Calculate the p signal as the mean of pixel value then p noise and the standard deviation or error value of pixel value and take the ratio of an image.

$$SNR = 10 \log10(P\ signal/P\ noise) \quad (3)$$

Above equation is helped to express the results in decibels.

E. Structural similarity Index

The Structural similarity index (SSIM) is an observation metric that Quantify the image quality degradation, which is affected by processing such as losses and Data compression in the data transmission. It has three changes such as Luminance, Contrast, and Structural Change.

Luminous Change

$(x, y) = 2\mu x\mu y+c1/\mu x2+ \mu y2+c1$ (4)

Contrast Change

$2\sigma x\ \sigma y+c2/\ \sigma x2+\ \sigma y2+c2$ (5)

Structural Change

$s(x, y)= \sigma xy+c3/\ \sigma x\ \sigma y+c3$ (6)

VI. PERFORMANCE ANALYSIS

S No	Nam e of the paper	Process of Encryption and Decryption	Major Technique and algorithm	Result of the method
1	Digital image encryption and decryption algorithm based on wavelet transform and chaos system	1. Wavelet Decomposition process for Encryption 2.Chaos Sequences for Decryption 2D discrete wavelet transform	Wavelet Transform and Chaos System, Symmetric Key Encryption	Strong Ability, Small Distortion to Resist the Noise Attacks
2	Image encryption and Decryption using Image Gradient Technique	Two process has done to encrypt the image Level: 1. Intensity variation 2. Pixel value swapping	Gradient Technique, Secret Key Cryptography	Avoid the Brute Force Attack, provide the same pixel value of image after encryption and decryption process of other methods
3	Image encryption technique using improved A/5 Cipher on Image bit planes for Wireless Data Security	1. ID Data Streams 2. Gray Scale Image 3.XOR with Key Streams 4.Clock Controlling unit 5. Non –Linear Function	A5/1 Cipher, Image Bitplane, Symmetric Key. Stream Cipher	High Quality Encryption, Fast Computation, Lossless Encryption and Decryption
4	Image encryption Scheme with key sequence based on chaotic Function	1.Threshold Function 2.Shift Register 3. Binary Bits 4. Histogram Band	Key Sequence, Chaotic Function, Symmetric Key Encryption Addictive Stream Cipher	Offline key generation and storage process, Currently Used in Real time Applications
5	Image Encryption and Decryption in public key Cryptography Based on MR	1.Control Parameters 2. Byte Values and Numeral values 3.Byte Array	Magic Rectangle, Asymmetric Key Encryption	Difficult to Identify the Original message whether text or image file. Increase the efficiency and security
6	Image Encryption and Decryption using Combined key sequence of Logistic map and Lozi map	1.Logistic Function 2. Single Key Sequence 3. xor Function	Logistic Map, Lozi Map, Combined Key Sequence, Asymmetric Key Encryption with Lozi and Logistic Map	Gray scale image medical images. Security Analysis applied in MSE, Correlation, Coefficient, Visual Analysis
7	Image Encryption and Decryption RNS Domain Based On $2^n,2^{n+1},2^{n+1},\ldots2^{N-1}$ Modular List	1.Combinational Logic 2.Modular Conversion 3.Integer Stream 4.Forward Convertor 5.Reverse Convertor	RNS Domain, $2^n,2^{n+1},2^{n+1},\ldots2^{N-1}$ Modular List, Symmetric Key Encryption AES with Residue Number System	Two Dimensional Securities Achieved.
8	FPGA Implementation of image encryption and Decryption using AES 128 bit core	1.Hexadecimal Format 2.FPGA using UART method	AES 128 Bit Core, Symmetric Key AES Algorithm	Ether net speed is high and avoid the loss of data packets while transmission Time

9	A Novel Threshold Based Image Encryption for Bitmap Image	1.Threshold 2.Matrix Transposition	Bit Map Images, Symmetric Key Stream Cipher	Lowest Correlation, Highest Encryption Entropy
10	Enhanced Blowfish Algorithm for image encryption and decryption with supplementary key	1. Key Generation 2. Encrypted Image	Blowfish Algorithm, Symmetric Key	Security is more high, supplementary key provides the efficiency

VII. CONCLUSION

Today's world is entirely depends on the science and electrical mode. The people are not ready to proceed their man power for daily exchanges. For transactions and communications, they want to use internet at all for save their time. For the internet transactions, high securityis needed here. Lot of cryptographic techniques was developed more and more by the various researchers. In this paper review the various research in different approach that list out what are all the encryption techniques best suited for color images and which of the cryptographic technique is suited for gray images. Finally, this paper is having the collection of quality metrics, which are needed to test the image quality. This paper is more useful for peer researchers.

REFERENCES

[1] Kanagalakshm, K., and M. Mekala. "Enhanced Blowfish algorithm for image encryption and decryption with supplementary key." *International Journal of Computer Applications* 146.5 (2016).

[2] Berlin, K., and A. Padmapriya. "A NOVEL THRESHOLD BASED IMAGE ENCRYPTION FOR BITMAP IMAGES." (2014).

[3] Li, Xiaofeng, and Yinhui Zhang. "Digital image encryption and decryption algorithm based on wavelet transform and chaos system." *Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE*. IEEE, 2016.

[4] Berlin, K., and A.Padmapriya. "Performance Analysis of Threshold based Image encryption".International Journal of Computer Applications 99.12 (2014):30-33.

[5] Rajput, Yashpalsingh, and A.K. Gulve." An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher". International Journal of Computer Applications 83.13(2013).

[6] Naveen, Ch, and Vishal R. Satpute. "Image encryption technique using improved A5/1 cipher on image bitplanes for wireless data security." Microelectronics, Computing and Communications (MicroCom), 2016 International Conference on. IEEE, 2016.

[7] Shruthi, K. M., S. Sheela, and S. V. Sathyanarayana. "Image encryption scheme with key sequences based on Chaotic functions." Contemporary Computing and Informatics (IC3I), 2014 International Conference on.IEEE, 2014.

[8] Amalarethinam, DI George, and J. SaiGeetha. "Image encryption and decryption in public key cryptography based on MR." Computing and Communications Technologies (ICCCT), 2015 International Conference on. IEEE, 2015.

[9] Rohith, S., and B. K. Sujatha. "Image encryption and decryption using combined key sequence of Logistic map and Lozi map." Communications and Signal Processing (ICCSP), 2015 International Conference on.IEEE, 2015.

[10]Priyanka, M. P., E. Lakshmi Prasad, and A. R. Reddy. "FPGA implementation of image encryption and decryption using AES 128-bit core." Communication and Electronics Systems (ICCES), International Conference on.IEEE, 2016.

[11]Reddy, P. VenkataNarasa, and RajasekharKarumuri. "Image encryption and decryption in RNS domain based on {2 n, 2 2n+ 1-1, 2 n+ 1, 2 n-1} moduli set." Communication and Electronics Systems (ICCES), International Conference on.IEEE, 2016.

[12]Sadan, ShettyDeepesh, and AnushaKarkala. "Image encryption and decryption using image gradient technique." (2013).