ISSN 2320 -2610
Volume 9, No.3, May - June 2020
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis01932020.pdf
https://doi.org/10.30534/ijmcis/2020/01932020

Crypt analyzing and Image Encryption Using WU's Algorithm

[1]Pooja Jayan,[2]Pretty Sara Fredy,[3]Rintu Joseph,[4]Roshni P S,[5]Ms.Nimmymol Manuel
[1] Department of Computer Science& Engg, India,poojakannankunnel2016@gmail.com.
[2]Department of Computer Science& Engg, India, prettysarafredy98@gmail.com.
[3]Department of Computer Science& Engg, India, rintu712@gmail.com.
[4]Department of Computer Science& Engg India, psroshni1996@gmail.com.
[5]Faculty Department of Computer Science, India, nimmymol.manuel@mangalam.in

ABSTRACT

In this modern world, images are widely used in different processes. Therefore, the security of image and data from unauthorized uses is important. Now, information security is becoming increasingly important in data storage and broadcasting. It is essential for securing image, either in transit or store on devices. However, some image encryption algorithms still have many security issues and can be easily attacked by attackers. This proposed system performs the cryptanalysis of a newly proposed color image encryption scheme using Wu's algorithms. For encryption scheme, usually uses a pseudo-random encryption key generated by an algorithm and which makes the image more secure. An authorized beneficiary can easily decrypt the message with the secret key provided by the originator to beneficiary but not to unauthorized users

Key words: Encryption, Decryption, Wu's algorithms.

1. INTRODUCTION

Encryption is the process of encoding data using a secret key so it can remain hidden or inaccessible to unauthorized users. This helps protect personal information and sensitive data and increases the security of communication between client applications and servers. Today all use social, the unauthorized users are hack our personal data. We are not bothered about that type of crime. But today the cyber crimes are increase. After increase the cyber crime we are think about it. That time is give more importance cyber security. In social Medias give lots of security features. In early day's people are using social Medias and which are used for connecting different peoples. But today its used for business. So this time the cyber crimes are increase. The encryption technique is used to prevent the cyber crimes.. In this technique is highly authenticated and provide more security of our personal data. The individual secret keys are used the data transfer and it is highly confidential.

2. RELATED WORKS

The available symmetric key algorithms like DES, AES and public key algorithm RSA as found in [1] generally involve more number of computation or operation. Chaos theory is a part of mathematics and used in several advancing areas like neurology for EEG analysis, cardiology for embryonic chick heart cells [2], weather prediction[3], communication, control and theory of circuits[4], Direct sequence Code Division Multiple Access system [5,12]. Many researchers have shown chaos sequences can be used for encryption of images [5,13]. Logistic function is one chaos function which has a property of high sensitivity to initial condition, generated sequence is pseudo random non periodic and unpredictable for proper choice of bifurcation parameter 'r'. Advantages of using Chaos theory specifically for encrypting the images are simple in implementation, computationally faster and impregnable. Early application of chaotic sequence to encrypt text messages key sequence was generated using logistic map. Recently, apart from logistic map other chaotic functions are also used to generate key sequence in encrypting the images. Some of the chaotic maps used in image encryption schemes are standard map[8,15], Baker map[9], Cat map [10,11] & multi-chaotic system based scheme[8][9][10]. In [8]

encryption scheme was divided into two phases. In [6,14] they used 2D discrete chaotic system for row and column scrambling for each pixel on the original image. By using this model, it can secure our private data's efficiently and avoids attackers to attack our data's. Databases are increasingly used to store a variety of sensitive data from personally identifiable information to financial records critical applications. Network services are now open to the public confidential data may not be secure over the network. Therefore, it is necessary if someone retrieves / captures data because it is encrypted then he cannot decrypt the network and the original messages**.** The main problems that arise in image encryption process are with respect to its security level. Sharing and exchange have increased tremendously; usually information transfer is done using open channels. The victim of disruption. Now, information security is becoming more and more important in data sharing and broadcasting. Images are used differently different processes. Hence, the security of image and document data from unauthorized uses is important. Image encryption is a way to protect data.

A. Python

Python is an easy and powerful programming language to learn. Python's elegant syntax and dynamic typing, and its interpreted nature, make it an ideal language for scripting and rapid application development across many platforms and in many areas

B. Django

Django is a python based web framework and used to create efficient web applications. It is also called as batteries included framework because django provides built-in features like django admin interface ,default database SQLite3,etc ...It's based on MVT (model view template)architecture. MVT is a software design pattern for developing webpage. It’s helps to eliminate repetitive tasks making the development process very easy and Time saving.

3. METHODOLOGY

The main problems that arise in image encryption process are with respect to its security level. Sharing and exchange have increased tremendously; usually information transfer is done using open channels. The victim of disruption. Now, information security is becoming more and more important in data sharing and broadcasting. Images are used differently different processes. Hence, the security of image and document data from unauthorized uses is important. Image encryption is a way to protect data.

THE WU’S ALGORITHM

In encryption process, it consists of two phases, that is the permutate pixel positions and the encrypt pixel values. In the cryptanalysis, an encryption scheme is same as encryption machinery. Can explain the whole process of the encryption machinery as follows. The encryption machinery's input port have a color plaintext image with size of m×n×3 is input and in the output port contains the encrypted color image with size and has the size of m×n×3 is output. In the encryption machinery includes confusion and diffusion processing stages. In confusion process consists of:

1) Color plaintext image will be transformed into a gray image.
2) The gray image is permutated by using the 2D Arnold transform.

In diffusion process consist of:

i. The permutated gray image will be transformed into 3 color images.
ii. 3 color images are encrypted by CTM.
iii. The 3 encrypted color images components are merged into a color image, then get an encrypted image.

The steps can be described briefly as follows:

Step (1): Firstly, choose the secret keys (a, b, c, d, rm, rn, t) and (μ1, μ2, μ3, x10, x20, x30).

Step (2): Read the m×n×3 sized color plaintext image i.e, Pm×n×3=[P(i, j, k)]. Let N = m×n, and which denote the three components of$Pm\times n\times 3$ and as$RPm\times n=[RP(i, j)]$,$GPm\times n=[GP(i, j)]$and $BPm\times n=[BP(i, j)]$,where i=1, 2,…, m, j = 1, 2,…, n, k=1, 2, 3.

Step (3): Stitch the three components, that are RPm×n, GPm×n and BPm×n and are together to form a gray image as PSm×3n=[PS(i, l)], where
i=1, 2,…, m, l=1, 2,…, 3n.

Step (4): To permutated the gray image PSm×3n=[PS(x, y)] by using the Eq.(2) for the t rounds, and get a permutated image and the permuted image as$PRTm\times 3n=[PRT(x', y')]$ where, PRT(x’, y’) = PS(x, y).

Step (5): Split PRTm×3n into three matrices, and the three matrices are RRTm×n, GRTm×n, and BRTm×n with a size of m×n. Then RRTm×n, GRTm×n, and

BRTm×n converted to three 1D vectors RN×1, GN×1, and BN×1 where N=m×n.

Step (6): Iterate Equ (1) for N+1000 times with these parameters (μ1, x10), (μ2, x20) and (μ3, x30) and then take the final N values and to form three chaotic sequences X1, X2, X3 of length N.

Step (7): And then calculate the three key streams S1, S2, S3 with X1, X2, X3 by

S1 = [X1×10^10] mod 256,

S2= [X2×10^10] mod 256,

S3 = [X3×10^10] mod 256.

Step (8): Encrypt RN×1, GN×1, and BN×1 to obtain corresponding cipher text images R'=[R'(i)], G'=[G'(i)], and B'=[B'(i)].

The conditions expressed by the above formulas must be satisfied.

$R'(i) = (R(i)+ G'(i-1))+ B'(i-1))\bmod 256 \oplus S1(i)$

$G'(i)= (G(i) + R'(i-1)+ B'(i-1) \bmod 256 \oplus S2(i)$

$B'(i) = (B(i)+ R'(i-1)+ G'(i-1) \bmod 256 \oplus S3(i)$,

where i = 1, 2, …, N, when i=1, R'(i − 1), G'(i − 1), B'(i − 1) can be replaced by three parameters denoted by

R'0, G'0, and B'0.

Step (9): Reshape the three 1D vectors R', G',B' to the three matrices RCm×n,GCm×n,BCm×n, by using these three components to compose to get final color cipher image C. The decryption algorithm is the method in which it is an opposite operation of the encryption algorithm. The two key operation of the decryption algorithm are to mark out as follows.:

Firstly, the formula for recovering R, G, and B from R', G', B'in the reverse diffusion processes as:

$R(i) = (R'(i) \oplus S1(i) - G'(i-1) - B'(i-1) \bmod 256.$

$G(i) = G'(i) \oplus S2(i) - R'(i-1) - B'(i-1) \bmod 256.$

$B(i) = B'(i) \oplus S3(i) - R'(i-1) - G'(i-1) \bmod 256.$

Where i = 1, 2, …, N, when i=1, R'(i − 1), G'(i − 1), B'(i − 1) these are replaced by the some parameters

R'0 , G'0 , B'0.

The first pixel values of R(1), G(1) and B(1) cannot be decrypted, this is because the R'0, G'0, B'0 these three parameters values are unknown and for decryption these values are needed to calculate by pixel values of the plain image.

Secondly, the formula for the recovery of the unpermitted gray image PSm×3n from the permutated gray image PRTm×3n in the reverse confusion formula.

4.PROPOSED SYSTEM

The proposed model named Cryptanalyzing and Image Encryption using WU's algorithm. It has a registration page, login page, file uploading page, and a page for admin to view user details, also a page to know which all files are used and its details. Registration, login & file uploading pages are all connected /linked, so one page can lead to another. After the user registering, user can login and start uploading the required image file; from there it will split the given image in to 3 combination of red, green & blue image.

These images are then encrypted using wu's algorithm. Then the 3 images are joined together. A crypt analyzing is done to find any drawbacks in the currently used encryption algorithm, after that a suitable key is generated for the encryption using SHA-3 hash value algorithm. Then this encrypted image is sending to the person the user wants to send. The sent image (encrypted image) contain key that is generated. The person receives the encrypted image and it is decrypted using the key provided.

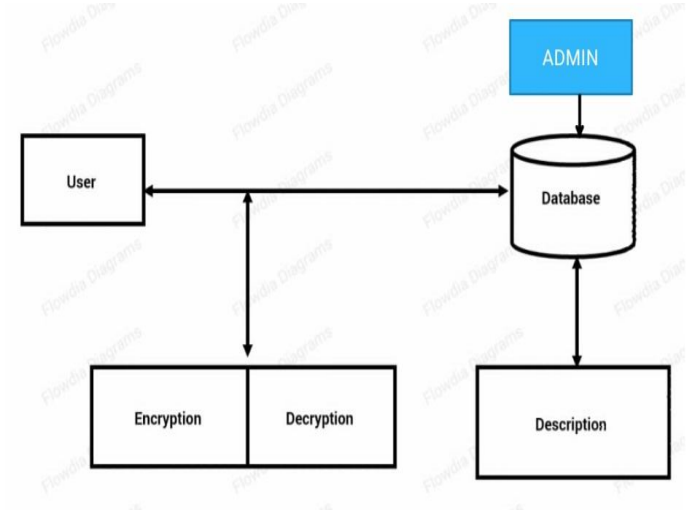

Figure 1: System Design

Encryption Process

Image encryption is defined as the process of encrypting secret image with the help of some encryption algorithm so that unauthorized users cannot access it and image encryption is the method in which images are encrypted by the sender to make the data more security and so that the encrypted images cannot be accessed by the unauthorized people. In this proposed system user can login after the registration and start uploading the required image file; from there it will split the given image in to 3 combination

of red, green and blue image. These images are then encrypted using wu's algorithm. Then the 3 images are joined together. In our website, there is an option to upload the images and the sender can easily upload the images. Then this encrypted image is sending to the person the user wants to send. The sent image (encrypted image) contain key that is generated. The person receives the encrypted image and it is decrypted using the key provided.

Decryption Process: The authorized user can decrypt the data because decryption requires a secret key or password. After the sender sends encrypted images he also shares a secret key to decrypt it. When the receiver receives the encrypted data, he login to website and there will be a decryption 4 option to decrypt the data or images. So he will decrypt it by using the secret key shared by the sender.

5.RESULT

In this section is to present experimental results. In order to evaluate a system in real time, it is very important that the system be deployed in the real environment. The system proposed by using Python framework Django and this application provide more security to the data's such as images and documents. By using RBG color combination and it can provide the encryption process for the color images and2D matrix and by using SHA algorithm can take the hash values. And then need to permute the grey codes. which makes more secure the data. The developed system proved that it gives more security for the data's and Test Test Description Input Expected Result Actual Result P/F Login Enter the required details of user.

Table 1: Result Table

Test ID	Test Description	Input	Expected Result	Result	P/F
Login	Enter the required details of user	Username and Password	Display Homepage	Success	P
Registration	Checking the details entered	Username and password is verified	Registration Complete	Success	P
Message	Giving the desired input	Images are encrypted and sent	Receiver can decrypt the data's	Success	P
Feedback	Store the feedback	Messages	Messages are stored	Success	P

6.CONCLUSION

A color image encryption algorithm is analyzed and cracked by using chosen-plain text attacks. Further, proposed an improved color image encryption algorithm. The improved algorithm includes the following three major improvements. Initially, a new chaotic system called Logistic-tent map(LTM) is proposed, which has good chaotic performance than tent map. Secondly, the new chaotic system is applied to the improved encryption scheme. Thirdly, by improving the key generation method encryption scheme Thirdly, by, improving the key generation method encryption scheme can overcome the security defects of the original encryption scheme. The experimental and analytical results show that the algorithm can significantly improve the security of encryption images while still having all the merits of the Wu's algorithm. It has a better potential for different applications. The improved image encryption algorithm proposed in this is suitable for encryption of color images with high security requirements, and is also suitable for Gray images encryption.

REFERECES

[1] W. Stallings, **"Cryptography and Network Security",** Fourth Edition, Prentice Hall, November 16, 2005.

[2] **.** Eberhart, R. C. **"Chaos theory for the biomedical engineer"** IEEE engineering in medicine and biology magazine: the quarterly magazine of the Engineering in Medicine & Biology Society 8.3, 1998, pp. 41-45.

[3] Lorenz, Edward N. **"Deterministic non-periodic flow"**. Journal of the Atmospheric Sciences 20 (2), 1963, pp.130-141.

[4] **.** J. A. Maldonado, J. A. Hernandez" **Chaos Theory Applied to Communications-Part I: Chaos Generators"** Proceedings of Electronics, Robotics and Automotive Mechanics Conference, 2007, pp. 50-55.

[5] Zouhozr Ben Jemaa, Safya Belghzth **"Correlation properties of binary sequences generated by the logistic map-application to DSCDMA."** Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Hammamet, Tunisia. 2002, pp. 447-451.

[6]. Zhang D., Gu Q. , Pan Y. and Zhang X. "**Discrete Chaotic Encryption and Decryption of Digital Images",** Proceedings of International Conference on Computer Science and Software Engineering, 2008, pp. 849-852.

[7]. Xiang Di, L. X. , Wang P., **"Analysis and improvement of a chaos image encryption algorithm"** Chaos, Solution and Fractals, Volume 40, Issue 5, 15 June 2009, pp. 2191-2199.

[8]. Jin-mei Liu, Qiang Qu, **"Cryptanalysis of a substitution-diffusion based image cipher using chaotic standard and logistic map"** Proceedings of Third International Symposium on Information Processing,2010, pp. 67-69.

[9].M. Salleh, S. Ibrahim, I. F. Isnin, **"Enhanced chaotic image encryption algorithm based on Baker's map."** Proceedings of IEEE Conference on Circuits and Systems, 2003, vol.2, pp. 508-511.

[10].K. Wang, W. Pei, L. Zou, A. Song, Z. He, **"On the security of 3D Cat map based symmetric image encryption scheme,"** Physics Letters A, 2005, vol. 343, pp. 432-439.

[11] Vinodh P Vijayan, Deepti John, Merina Thomas, Neetha V Maliackal, Sara Sangeetha Varghese **"Multi Agent Path Planning Approach to Dynamic Free Flight Environment"**, International Journal of Recent Trends in Engineering (IJRTE), ISSN 1797-9617 Volume 1, Number 1, May 2009, Page(s): 41-46.

[12] Juby Joseph, Vinodh P Vijayan**" Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol"** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014, pp. 825-829, ISSN: 2277 128X

[13] V P Vijayan, Biju Paul **"Multi Objective Traffic Prediction Using Type-2 Fuzzy Logic and Ambient Intelligence"** International Conference on Advances in Computer Engineering 2010, Published in IEEE Computer Society Proceedings, ISBN: 978-0-7695-4058-0, Print ISBN: 978-1-4244-7154-6

[14] Vijayan V P, Gopinathan E **"Improving Network Coverage and Life-Time in a Cooperative Wireless mobile Sensor Network "** Fourth International Conference on Advances in computing and communications (ICACC) Aug, 2014. Published in IEEE Computer Society Proceedings. Print ISBN: 978-1-4799-4364-7, INSPEC AccessionNumber:14630874,DOI:10.1109/ICACC.2014.1 6 PP 42-45.

[15] Vinodh P Vijayan, Biju Paul **" Traffic scheduling for Green city through energy efficient Wireless sensor Networks "** International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.4, July – August 2019, ISSN 2278-3091, https://doi.org/10.30534/ijatcse/2019/81842019.