IJCSEInternational Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-1 E-ISSN: 2347-2693

Improving Image Encryption and Decryption Using WU's Algorithm

Simy Mary Kurian[1*], Nimmymol Manuel[2], Neena Joseph[3], Neema George[4]

[1,2,3,4]Department of Computer Science & Engineering, Mangalam College of Engineering, Kerala, India

[*]*Corresponding Author: simy.kurian@mangalam.in, Tel.: +91 9656294800*

Available online at: www.ijcseonline.org

Received: 04/Jan/2018, Revised: 12/Jan/2018, Accepted: 23/Jan/2018, Published: 31/Jan/2018

Abstract— In this advanced world, pictures are generally utilized in various cycles. Along these lines, the security of picture and information from unapproved utilizes is significant. Presently, data security is turning out to be progressively significant in information capacity and broadcasting. It is fundamental for getting picture, either on the way or store on gadgets. Nonetheless, some picture encryption calculations actually have numerous security issues and can be effortlessly gone after by assailants. This proposed framework plays out the cryptanalysis of a recently proposed variety picture encryption scheme utilizing Wu's algorithms. For encryption plot, typically utilizes a pseudo-irregular encryption key created by a calculation and which makes the picture safer. An approved recipient can without much of a stretch unscramble the message with the mystery key given by the originator to recipient however not to unapproved clients.

Keywords— Encryption, Wu's algorithms

I. INTRODUCTION

Encryption is the most common way of encoding information utilizing a mystery key so it can stay covered up or difficult to reach to unapproved clients. This safeguards individual data and touchy information and builds the security of correspondence between client applications and servers. Today all utilization social, the unapproved clients are hack our own information. We are not fretted over that kind of wrongdoing. However, today the digital violations are increment. After increment the digital wrongdoing we are consider it.

That time is give more significance digital protection. In friendly Medias give heaps of safety highlights. In early day's kin are utilizing social Medias and which are utilized for associating various people groups. Yet, today its utilized for business. So this time the digital wrongdoings are increment. The encryption method is utilized to forestall the digital wrongdoings.. In this strategy is profoundly validated and give greater security of our own information. The singular mystery keys are utilized the information move and it is exceptionally private.

II. RELATED WORK

The accessible symmetric key calculations like DES, AES and public key calculation RSA as found in [1] for the most part include more number of calculation or activity. Tumult hypothesis is a piece of science and utilized in a few propelling regions like nervous system science for EEG investigation, cardiology for early stage chick heart cells [2], climate prediction[3], correspondence, control and hypothesis of circuits[4], Direct succession Code Division Multiple Access framework [4,9]. Numerous scientists have shown mayhem groupings can be utilized for encryption of pictures [4,10].

Calculated work is one disarray work which has a property of high aversion to introductory condition, created arrangement is pseudo arbitrary non intermittent and flighty for appropriate decision of bifurcation boundary 'r'. Benefits of utilizing Chaos hypothesis explicitly for scrambling the pictures are straightforward in execution, computationally quicker and invulnerable. Early use of tumultuous succession to encode instant messages key arrangement was produced utilizing calculated map. As of late, aside from calculated map other tumultuous capacities are additionally used to create key arrangement in encoding the pictures. A portion of the tumultuous guides utilized in picture encryption plans are standard map[5,11], Baker map[6], Cat map [7,8] and multi-turbulent framework based scheme[5][6][7].

By utilizing this model, it can tie down our private information's effectively and stays away from assailants to go after our information's. Data sets are progressively used to store an assortment of touchy information from by and by recognizable data to monetary records basic applications. Network administrations are currently open to the public private information may not be secure over the organization. Along these lines, it is essential on the off chance that somebody recovers/catches information since it is scrambled, he can't decode the organization and the first messages. The fundamental issues that emerge in picture encryption process are regarding its security level. Sharing and trade have expanded enormously; generally data move is finished utilizing open channels.

The principle issues that emerge in picture encryption process are as for its security level. Sharing and trade have expanded colossally; typically data move is finished utilizing open channels. The survivor of interruption. Presently, data security is turning out to be an ever

increasing number of significant in information sharing and broadcasting. Pictures are utilized diversely various cycles. Henceforth, the security of picture and record information from unapproved utilizes is significant. Picture encryption is a method for safeguarding information.

III. METHODOLOGY

The primary issues that emerge in picture encryption process are regarding its security level. Sharing and trade have expanded enormously; typically data move is finished utilizing open channels. The casualty of interruption. Presently, data security is turning out to be an ever increasing number of significant in information sharing and broadcasting. Pictures are utilized contrastingly various cycles. Subsequently, the security of picture and archive data from unauthorized uses is important. Image encryption is a way to protect data.

In encryption process, it comprises of two stages, that is the permutate pixel positions and the encode pixel values. In the cryptanalysis, an encryption plot is same as encryption apparatus. Can make sense of the entire course of the encryption hardware as follows. The encryption hardware's feedback port have a variety plaintext picture with size of m×n×3 is input and in the result port contains the encoded variety picture with size and has the size of m×n×3 is yield. In the encryption hardware incorporates disarray and dissemination handling stages. In disarray process comprises of:

1) Color plaintext image will be transformed into 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 ofPm×n×3 andasRPm×n=[RP(i, j)],GPm×n=[GP(i, j)]and BPm×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 asPRTm×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, Bto 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, Bin 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.

The proposed model named Cryptanalyzing and Image Encryption utilizing WU's calculation. It has an enlistment page, login page, record transferring page, and a page for administrator to see client subtleties, additionally a page to realize which all documents are utilized and its subtleties. Enlistment, login and record transferring pages are completely associated/connected, so one page can prompt another. After the client enlisting, client can login and begin transferring the necessary picture record; from that point it will part the given picture in to 3 blend of red, green and blue picture.

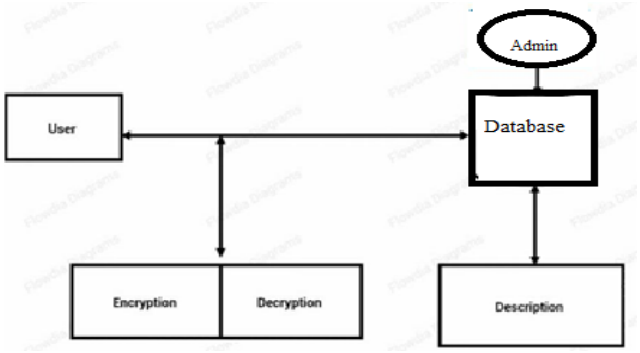

Figure 1 .System Architecture

These pictures are then scrambled utilizing wu's algorithm. Then, at that point, the 3 pictures are consolidated. A sepulcher dissecting is done to track down any downsides in the right now utilized encryption calculation, after that a reasonable key is created for the encryption utilizing SHA-3 hash value algorithm. Then, at that point, this encoded picture is shipping off the individual the client needs to send. The sent picture (encrypted picture) contain key that is produced. The individual gets the encoded picture and it is decrypted utilizing the key gave.

Picture encryption is characterized as the most common way of scrambling secret picture with the assistance of some encryption calculation so unapproved clients can't get to it and picture encryption is the technique where pictures are encoded by the source to make the information greater security thus that the scrambled pictures can't be gotten to by the unapproved individuals. In this proposed framework client can login after the enrollment and begin transferring the expected picture document; from that point it will part the given picture in to 3 blend of red, green and blue image. These images are then encrypted using wu's algorithm.

Then, at that point, the 3 pictures are combined. In our site, there is a choice to transfer the pictures and the source can without much of a stretch transfer the pictures. Then this encoded picture is shipping off the individual the client needs to send. The sent image (encrypted image) contain key that is produced. The individual gets the encoded picture and it is decrypted utilizing the key gave.

IV. RESULT ANALYSIS

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

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

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.

In this segment is to introduce trial results. To assess a framework continuously, the framework must be sent in the genuine climate. The framework proposed by utilizing Python structure Django and this application give greater security to the information's like pictures and reports.

By utilizing RBG variety mix and it can give the encryption interaction to the variety pictures and2D grid and by utilizing SHA calculation can take the hash values. And afterward need to permute the dim codes. which makes safer the information. The created framework demonstrated that it gives greater security for the information's and Test Description Input Expected Result Actual Result P/F Login Enter the necessary subtleties of client.

V. CONCLUSION

A variety picture encryption algorithm is dissected and broken by utilizing picked plain text assaults. Further, proposed a better variety picture encryption calculation. The better calculation incorporates the accompanying three significant enhancements. At first, another turbulent framework called Logistic-tent map(LTM) is proposed, which has great tumultuous execution than tent guide. Also, the new tumultuous framework is applied to the better encryption plot. Thirdly, by further developing the key age technique encryption plot Thirdly, by, further developing the key age strategy encryption plan can conquer the security imperfections of the first encryption conspire. The exploratory and scientific outcomes demonstrate the way that the calculation can essentially work on the security of encryption pictures while as yet having every one of the

benefits of the Wu's calculation. 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.

REFERENCES

[1] W. Stallings, **"***Cryptography and Network Security***",**Fourth Edition, Prentice Hall, Vol. **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,Vol. **8**, Issue **3**, pp**. 41-45,1998.**

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

[4] 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. pp. **447-451,2002**

[5] 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, pp. **67-69,2010**

[6] 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, Vol.**2**, pp**. 508-511,2002**

[7] 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, Vol**. 343**, pp. **432-439,2005**

[8] 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), pp.**41-46,2009**

[9] Juby Joseph, Vinodh P Vijayan**"** *Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression usingLonger Path Protocol"* International Journal of Advanced Research in Computer Science and Software Engineering, Vol **4**, Issue **7**, pp. **825-829,2014**

[10] V P Vijayan, Biju Paul **"***Multi Objective Traffic Prediction Using Type-2 Fuzzy Logic and Ambient Intelligence***"**,IEEE International Conference on Advances in Computer Engineering, Published in IEEE Computer Society Proceedings, **2010**

AUTHORS PROFILE

Ms.Simy Mary Kurian Assistant Professor , Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2011.She has completed B.Tech in Computer Science and Engineering from Mahatma Gandhi University and M.Tech in Software Engineering from Karunya Institute of Technology and Science. Her research interest include Image Processing, Data Science, Artificial Intelligence and Bio-inspired Computing .She has associated with many number of undergraduate and research projects.

Ms.Nimmymol Manuel is working as Assistant Professor in the Department of Computer Science & Engineering of Mangalam College of Engineering ,Kerala ,India since 2008.Shecompleted her B.Tech in Computer Science & Engineering in 2006 from Mahatma Gandhi University with First Class and M.Tech in Computer Science & Engineering from M.S University Tirunelveli in 2012. Her research interest include Wireless Sensor Netwok, Artificial Intelligence, Computer Architecture and IoT. She has taught both undergraduate and post graduate topics and guided several projects. She has a teaching experience of 13 years. She is a member of Computer Society of India.

Ms.*Neena Joseph* has completed her master's degree in Computer Science & Engineering from Manonmaniam *Sundaranar University* and bachelor's degree in Computer Science & Engineering from Mahatma Gandhi University. She has qualified UGC NET in Computer Science and Applications and has more than 10 years of under graduate teaching experience and 8 years of post-graduate teaching experience. She has to her credit several research papers, published in reputed National and International journals. She has presented many research papers in various conference of International repute. Her areas of interest include Theoretical Computer Science, Natural Language Processing and Compiler Optimization.

Ms.Neema George Assistant Professor , Department of Computer Science and Engineering, Mangalam College of Engineering, Kerala, India since 2008. Her research interest include Image Processing, Machine Learning, Artificial Intelligence Cloud Computing .

