SECURE IMAGE SHARING WITH CHAOS BASED ENCRYPTION

Vanitha A,

Master of Computer Application,

Dhanalakshmi Srinivasan Engineering College,Perambalur,Tamilnadu

Ass Prof..,Vijayakumar D,

Master of Computer Application,

Dhanalakshmi Srinivasan Engineering College,Perambalur,Tamilnadu

ABSTRACT

Image privacy is a serious issues now a days.A chaos based image encryption is added to secure the image. The image will be divided into odd and even pixels.XOR based encryption and decryption is enhanced for the selected pixels. This paper introduces a security analysis of a chaos- based image encryption scheme. An attack system is proposed to discover the security weaknesses of the chaotic encryption scheme. Convergence of the attack system is proved using master- slave synchronization. Future evaluation are the structure of the encryption scheme and a scalar time series observed from the chaotic system. Simulation and numerical results verifying the feasibility of the security analysis method are given.

INTRODUCTION

Securing image from server is a tedious process now-a -days.So, encryption is enhanced in image to secure in a efficient manner.Image can be securely stored in server with a pixel based encryption. Chaotic systems have several applications in nowadays evolving technology such as in electrical circuits, cryptology, engineering, etc. [1], [2]. Because of their diverse applications in these areas, chaotic systems have been extensively investigated and analyzed by many researchers. These complex dynamic systems are generally modeled by chaotic or hyper- chaotic phenomena.

EXISTING SYSTEM

Chaotic maps are generally continuous and can be discredited as per requirement for application in encryption schemes. There exist several well-known one dimensional and multi-dimensional chaotic maps like logistic map (1-D), tent map (1-D), Arnold’s cat map (2-D), Lorenz map (3-D) etc. To improve on the chaotic properties researchers have been proposing improvements in chaotic maps or hybridization of more than one chaotic maps to create new chaotic maps with enhanced properties. Thus the chaotic maps has been placed with a two types of pixel division is employed. The pixels are divided as odd pixel and even pixel with a chaotic map implementation. A probabilistic based cipher is implemented with the encryption and protection of the 2D image. This paper describes how such an even-odd encryption. The even and odd number of pixel is added by the pixel division methodology where the image can be splits and add to the distributed storage as multiple shares and the shares get encrypted. Thus the implementation system provides a resistance over the statistical attacks. The encryption placed as the AES based encryption system where the key based enhancement is produced. Thus the encryption reduces the security attacks over the third party attacks over the server. The accuracy of the encryption and the protection against the third party access and the attacks is high.

DISADVANTAGES

- Encryption and decryption time changes according to the dimension of the image.
- Need large key space to encrypt the image and to resist against brute force Attack.
- If any bit is altered then the encryption scheme will be different.
- Both odd and even pixel image need to be encrypted.
- Only brute force attack and statistical attack can be reduced.

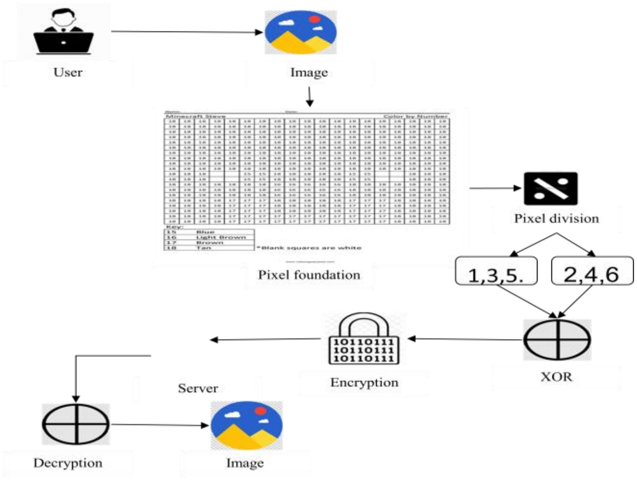
PROPOSED SYSTEM

Picture encryption utilizing change is picking up its notoriety over common encryption plans like AES, DES, RSA etc., due to its tall security, less time complexity utilizing sensible computational overheads. Mainly chaotic capacities are utilized in stage based procedures to characterize a grouping, based on which the pixels or bits of a picture are permuted. In parallel, investigates are too carried out to define permutation utilizing non chaotic methods. In this paper, a novel non-chaotic picture encryption technique is proposed. The properties of cyclic bunch are utilized as the spine of the proposed strategy and using these properties a few sequences/permutations are characterized. These changes are utilized for row/column level change of pixels and bit-level stage. Iterative pixel expansion operation with bit shifting using a ‘Transform array’ changes the pixel esteem of the bit permuted picture. Test comes about show that the proposed conspire is secure against measurable and vary. The steps are followed as two phase: confusion and diffusion phase later carried by the XOR encryption algorithm. The process carried out with two diffusion where BLP and BLT which adds more secured accuracy to the image. In confusion stage the pixels are repositioned and diminish the relationships among the pixels. But, the histogram remains same as the unique picture and thus there's a chance to figure the initial picture from the histogram. In dissemination stage, more security is suggested utilizing Bit level Change and Bit level Transformation. This stage moreover guarantees that a slide adjustment in unique picture comes about a totally distinctive encrypted image. These bit level operations are outlined with the assistance of produced permutation by the cyclic gather. Test comes about on a few standard images are very palatable. In this work, the standard measurements and tests are utilized to degree the security and vigor of the proposed method. Proposed strategy gives way better comes about in most of the cases while comparing with a few existing techniques.

ADVANTAGES

- Differential attacks can be overcome by the proposed system
- The execution of the proposed method is very great compared with the existing strategies
- The image will be restored without any distortion
- This helps one to securely safeguard the image from unknown attacks.

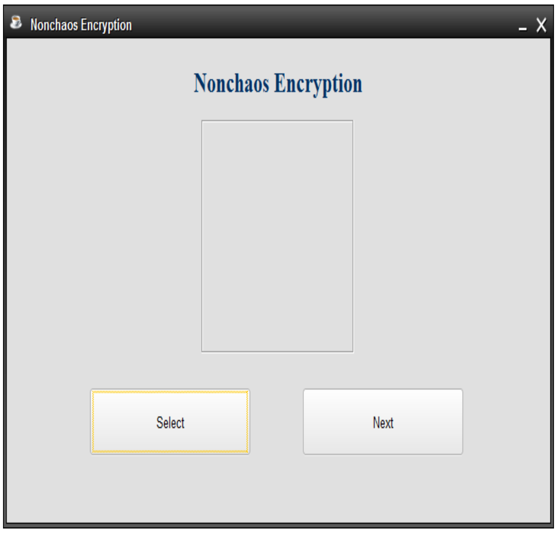
SYSTEM ARCHITECTURE

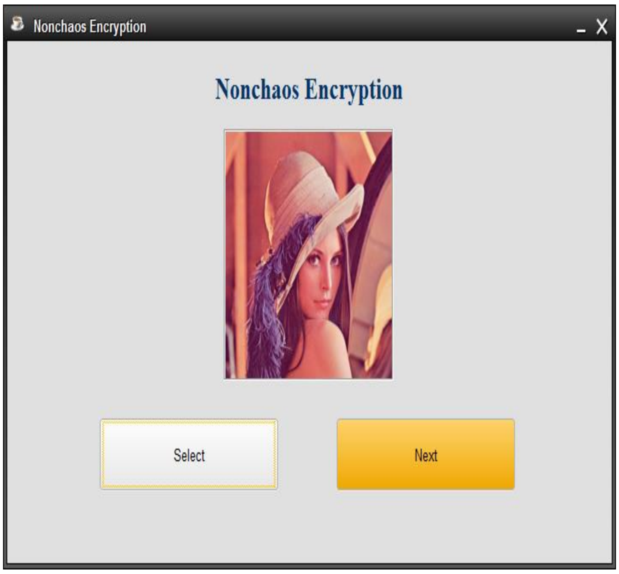


Various organizations define systems architecture in different ways, including:

- An allocated arrangement of physical elements which provides the design solution for a consumer product or life-cycle process intended to satisfy the requirements of the functional architecture and the requirements baseline.

- Architecture comprises the most important, pervasive, top-level, strategic inventions, decisions, and their associated rationales about the overall structure (i.e., essential elements and their relationships) and associated characteristics and behavior.
- If documented, it may include information such as a detailed inventory of current hardware, software and networking capabilities; a description of long-range plans and priorities for future purchases, and a plan for upgrading and/or replacing dated equipment and software.





CONCLUSION

An encrypted image with confusion diffusion pixels.The encrypted image needs a restoration of intensity level and the correlated values to be placed.This helps one to securely safeguard the image from unknown attacks.Thus a secure image transfer is achieved using this non chaos based implementation.In propose a security analysis method for chaotic encryption schemes. An attack system is introduced to discover the security weaknesses of the chaos-based image encryption system and its convergence is proved using master- slave synchronization scheme. Although the only information available are the structure of the chaos-based encryption scheme and a scalar time series observed from the target chaotic system, identical synchronization of target and attack systems is achieved and hence output bit streams are syn- chronized. Keys generated for the target chaos-based image encryption scheme does not fulfill NIST 800-22, Big Crush and Diehard statistical test suites, the previous and the next bit can be predicted, while the same output bit sequence can be reproduced.

REFERENCES

1. Shyamalendu Kandar , Dhaibat Chaudhuri , Apurbaa Bhattacharjee , Bibhas Chandra Dhara, “Image encryption using sequence generated by cyclic group”, Journal of Information Security and Applications”, PP: 117-129, 2019.
2. Avinash Ray , Anjali Potnis , Prashant Dwivedy , Shahbaz Soofi , Uday Bhade, “Comparative Study of AES, RSA, Genetic, Affine Transform with XOR Operation, And Watermarking for Image Encryption” International conference on Recent Innovations is Signal Processing and Embedded Systems, pp: 27-29, October 2017.
3. Devaney, R., An introduction to Chaotic Dynamical Systems, Second edition, Addison-Wesley, Reading MA, 1989. Abel, A. and Schwarz, W. “Chaos communications principles, schemes, and system analysis”, Proc. of IEEE, vol. 90, no. 5, pp. 691-710, May 2002.
4. Bucolo, M., Caponetto, R., Fortuna, L., Frasca M. and Rizzo, A., “Does chaos work better than noise?”, IEEE Circuits and Systems Magazine, vol. 2, no. 3, pp. 4-19, 2002. Small, M. and Tse.
5. C. K., “Detecting determinism in time series: The method of surrogate data”, IEEE Transactions on Circuits and Systems I, vol. 50, pp. 663-672, May 2001. Stojanovski, T., Kocarev, L. “Chaos-Based Random Number Generators- Part I: Analysis”, IEEE Transactions on Circuits and Systems I, Vol. 48, 3 (2001) 281-288.