IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMAGE ENCRYPTION USING COMBINED CHAOS AND MEMORY CELLULAR AUTOMATA

Rathika A [1], Sibi Pranav K[2], Sanjaay J[3], Soundararajan R[4], Vishnu Priyan.R[5]
Assistant Professor, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India[1]
UG Students, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India [2 - 5]

Abstract:

In this paper, a novel image encryption system is proposed based on a portable mobile automata (RCA) system that incorporates chaos. In this algorithm, an integrated mapping system with complex behaviors and periodically reversible mobile automata is used. We divide each pixel of an image into 4-bit units, and then take the pseudorandom key distribution generated by the integrated layout map to allow these units in the confusion phase. And in the distribution phase, the two-dimensional reversible mobile automata which are different flexible systems are used to repeat multiple rounds to achieve a smaller distribution, when we consider only the top 4 bits per pixel because the top 4 bits hold almost image information. Theoretical analysis and test results show that the proposed algorithm achieves a high level of security and considers effective performance against common attacks such as distinct attacks and statistical attacks. This algorithm belongs to the systematic system.

I. INTRODUCTION

With the advent of the internet, information security is gaining more attention. Usually encryption can besuccessfully protect human information that is broadcast on social media. But traditional encryption methods have limitations on image encryption such as low efficiency, large data, and high correlation between pixels and so on. Chaos, which is a complex indirect system, has flexible structures suitable for encryption as high sensitivity in initial values and system parameters, uncertainty, randomization and periodicity. So chaos theory used in terms of cryptosystems. Over the past decade, more and more researchers have proposed multiple encryption schemes in chaos, many of which are crucifixion. Image encryption is usually divided into two sub-sections, the confusing and diffuse phase. In the confusion phase, image pixels are allowed using the same conversion method baking map, magic square, Arnold map-based, while pixel values remain unchanged. The distribution phase in particular masks each pixel after consecutive approval. In this paper, we combine cellular automata (CA) with chaos to suggest a new image encryption. The default for cell phones is highly compatible and distributed systems can mimic complex behaviors. A large number of CA rules enable it many ways to produce sequences. Moreover, the mobile automata converts by logical calculation only, by pseudorandom. And complex behavior. Cellular automata are also used in symmetric cipher and public cipher. A public cipher based on mobile automata was first proposed by Guan, a stream cellular automata stream cipher was proposed by Wolfram. Later, many experts proposed encryption algorithms based on mobile automata. In the authors use reversible mobile automata to use block chain encryption algorithm. In our work, we use your strongpoint for both chaos and mobile automata to design a new image encryption algorithm. All operations are performed at bit-level. In approving on stage, we use a pseudorandom sequence generated by a chaotic map to shuffle the units that make up each pixel. And converts pixel values without permission. In the distribution phase, the reversible mobile automata is accepted for duplication in pixel bits many rounds instead of pixels. The benefits of mobile automata in encryption are listed below:

(1) Extreme evolution dominates the environment.

(2) Mobile automata contain only complete statistics or logical functions, making calculations easy.

(3) Cellular automata also exhibits complex behavior, and are consistent.

The paper is arranged as follows. In the next section, we give a brief overview of the combined map and description of the RCA we have used and algorithm. In Step 3, the encryption algorithm is presented in detail. Section 4 provides an analysis of the theory and implications of imitation. The last section concludes with a paper.

Literature Review:-

Photo encryption is done using low-level permission and high-resolution mapping. The blank image is converted (M x N) to a gray scale image (M x 3N) and converts the gray image to 8-bit identical members per pixel and the image size is converted to (M x 24N). The lines and columns of the image agree on a small scale and move the map to produce a series of interactive dynamic maps divided into sections and arrange the two identical members in an ascending order to obtain an approved image. After approval the image is converted to a color image. The Chen system is used to confuse and distribute the color components in a photo at the same time. Generate three decimal sequences by finding random numbers through the Chen system. Exclusive OR operation (XOR) is a sequential image that is produced gradually. Repeat the Chen process until all features are encrypted. The encryption process is the opposite of the encryption process. The first encryption process separates the embedded color image from the red, green, and blue images and then scans the pixels from row to column and in addition produces three decimals with the same initial values and parameters used for encryption. Answer algorithm level bit algorithm by PWLCM program. The system used showed that encryption was achieved on a large scale using security analysis and test results. All types of attacks can be prevented from being large enough using the key space used. Implementation of the chaos based cryptographic system to protect the contents of transmitted images. The proposed system consists of a separating layer built using a binary matrix size 32 by 32. The partition layer is followed by a thin layer of permutation that uses pieces to shuffle 5 pixels of abnormal image pixels. method by which byte permission is used. The bit permutation layer is made up of a modified 2-D cat map that improved performance on a standard 2-D cat map. Advantages of using a 2-D modified cat map for efficiency in use, intelligence and arithmetic operation, the process involved in permitting and a small number of lock cycles. It therefore helps to spread the effect of one bit over the other. The system incorporates the same turbulent generation of random and indirect random sequence adjustment control parameters during the entire encryption cycle and the writing process. The results obtained and the security analysis showed that the system requires a single authorization cycle to provide sensitivity to one small change in the blank text and secret key and also the system prevents image from various types of attacks and is suitable for hardware use. Implementation of a riot-based encrypted encryption system that uses perceptron to detect encrypted output to withstand security threats and attacks. The high-intensity chaotic system produces three different random sequence sets from two standard .The perceptron is a single-layer network feed that can change its weight dynamically with the help of a high-level random system by creating random random sequence -cipher as output. The flexible nature of the turmoil system parameters will extend the system time and solve problems related to the different turmoil system cycle. The test results of the system used showed increased durability and high key sensitivity .The algorithm showed high security.

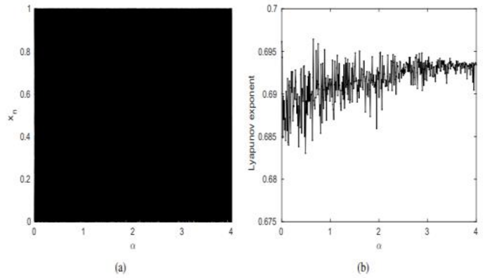
Keywords:
RCA,Encryption

Methodology:-

In this section, we explain in detail your proposed scheme for both encryption and decryption. The encryption / decryption system includes a series of outstanding cryptographic strategies including MCA, hash functions, complex systems, and random variables. The hash function is used in the proposed scheme to obtain a unique original image signature. The hash value associated with the first image is used for the acquisition of system parameters and keys required for different encryption / encryption phases. Generation details of these keys are also discussed in this section. In our algorithm, SHA-256 is used, a custom cryptographic hash function that generates a 256-bit hash value. Initially, a hash unit of character value is produced, and its first 212 bits are divided into four strands of unequal length in terms of (8) - (11). These lowercase letters are then converted to their corresponding decimal values, h1−52, h53−106, h107−158, and h159−212. The system parameters and the seed of (7) are obtained using these decimal numbers as follows

x 0 0 = 1 2 (x0 + h1−52),
α 0 0 = 1 2 (α0 + h53−106),
x 0 1 = 1 2 (x1 + h107−158),
α 0 1 = 1 2 (α1 + h159−212),

Where x0, α0, x1, and α1 are the first secret key and hi − j indicates the decimation of a small series that takes from i the to j the hash value.

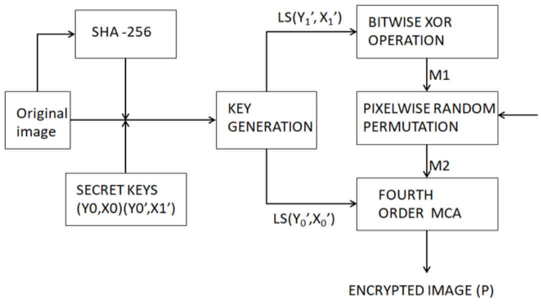


A. Important Generation

The deferred MCA of the k the system requires k - 1 rules of change and k pre-configuration in order to achieve the following configuration. As we use the MCA for the fourth order, three rules of change are required for the operation of the MCA. These rules are defined using a set of small keys generated by the system parameters tested using. The detailed process is described as follows. Keys use a logistic sine map. The deferred MCA of the fourth program requires three rules of current configuration to obtain the following configuration. The rules of change are defined using a set of small keys generated by the operation of the MCA using the control $Y0'$ control and $X0'$ seeds. First repeat the sine logistic sine map (l) at $l \geq 500$ to avoid the temporary effect using $Y0$ ' $andX0$ ', then repeat 48 times to get the e sequence. Map e [0,1] to [0,255] using the formula given below showing the sequence of n. $\boldsymbol{n} = (\boldsymbol{e} + \mathbf{1015})\ \boldsymbol{mod25}$ 384 bits and these bits are divided into three smaller series equals and used as rules of change to make the MCA. Next 128 bits where $K = [K1, K2, K3]$

B. The Encryption Process

At this stage the process that follows the steps of the proposed encryption process, shown in Fig. 4, described in detail. The whole process is made up of three stages in one round. First, the turbulent matrix M × N is generated using (7), M and N are the lines and columns of the first image. This matrix is then mapped to the right distance and slightly clever XOR with the first image. The resulting image is then approved by pixel intelligence. Finally, the MCA for the fourth reversed order is applied to the approved image, which displays the encrypted image. Bit-Wise Chaotic Diffusion: The first image is a little clever with XORed with a chaotic matrix. Pixel-Wise Random Permutation: In this step, a clever random pixel conversion where your pixels are allowed using PRNG. The pixel positions are updated according to the random sequence w obtained using the Algorithm.



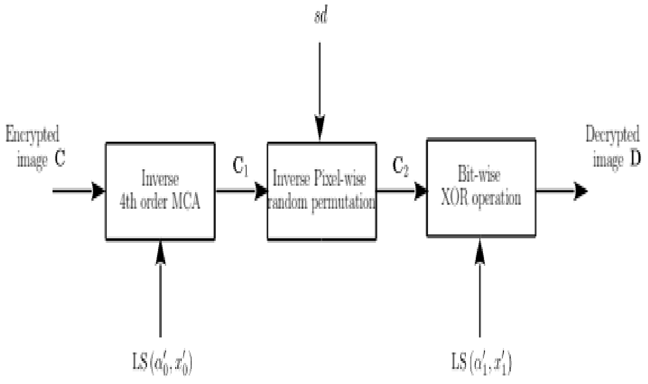
Encryption phase

C. The Crucifixion Process

In order to properly restore the original image, a total of six parameters must be transferred to the encryption side. These parameters include the seeds and system parameters of the LS map (cf. x0, α0, x1, and α1), the PRNG seed (cf. sd), and the 256-bit hash value of the first image. The encryption removal process, shown in Fig. 5, performed in the order of the encryption process. The C-shaped image can be found as

$$\mathbf{D} = \mathcal{F}^{-1}_{\alpha_1',x_1'}\left(\overbrace{\mathcal{G}^{-1}_{sd}\left(\underbrace{\mathcal{H}^{-1}_{\alpha_0',x_0'}(\mathbf{C})}_{\mathbf{C}_1}\right)}^{\mathbf{C}_2}\right)$$

Where D is the decrypted image



Novelty of the Work:-

Information security plays an important role when confidential information is shared between two or more parties. Stunning maps are used to deal with security issues. The current task is to compile a variety of dynamic maps to provide chaotic behavior between images. Conflict systems are widely used in image encryption because their initial conditions and control parameters are sensitive to the environment. The proposed encryption system incorporates a fourth-order mobile automata and diffusion-complication architecture. The blocks resulting from this decay strategy are considered to be the initial configuration of the MCA and an integrated chaos system is used to obtain transformation rules. Test and result analysis shows that the encryption is strong enough to survive all types of attacks while maintaining low complexity.

Recommendation of the department:

Nowadays, with the rapid emergence of the Internet in the digital world, the security of digital photography is becoming more important than ever. Many different methods of encryption have been suggested. Due to the other natural features of the image one needs to improve the tension in each image encrypted to provide high quality encryption. Factors such as high entropy or low pixel correlation are measures of interest in image encryption.

Reference:-

1. Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Optics Communications, 284(16- 17), 3895-3903.
2. Beniani, R., &Faraoun, K. M. (2018). A Mixed Chaotic-cellular Automata Based Encryption Scheme for Compressed Jpeg Images. JMPT, 9
3. 88-101. [3] Seredynski, M., &Bouvry, P. (2004, October). Block encryption using reversible cellular automata. In International Conference on Cellular Automata (pp. 785-792). Springer, Berlin, Heidelberg.
4. Chen, R. J., & Lai, J. L. (2007). Image security system using recursive cellular automata substitution. Pattern Recognition, 40
5. 1621-1631. [5] Wang, X. Y., Yang, L., Liu, R., &Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics, 62(3), 615- 621.
6. Souyah, A., &Faraoun, K. M. (2016). Fast and efficient randomized encryption scheme for digital images based on

quadtree decomposition and reversible memory cellular automata. Nonlinear Dynamics, 84(2), 715-732.

7. El Assad, S., &Farajallah, M. (2016). A new chaos-based image encryption system. Signal Processing: Image Communication, 41, 144-157.
8. Tralic, D., &Grgic, S. (2016). Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation. Radioengineering, 25(3), 549.
9. Bakhshandeh, A., &Eslami, Z. (2013). An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering, 51(6), 665-673.
10. Zhang, Y., & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19(1), 74-82. 27.