Image Encryption Vault

Midhuneshwar Kandasamy Kanivalavan *SUID : 351564889*
Syracuse University
Email ID : mkandasa@syr.edu

Oviyah Sridhar *SUID : 842946163*
Syracuse University
Email ID : osridhar@syr.edu

Rajaraajeshwaran Ramasamy Kannan
SUID : 925189708
Syracuse University
Email ID : rramas01@syr.edu

Work done:

Program Development & Execution	Midhuneshwar Kandasamy Kanivalavan Oviyah Sridhar Rajaraajeshwaran Ramasamy Kannan
Report Preparation	Midhuneshwar Kandasamy Kanivalavan Oviyah Sridhar Rajaraajeshwaran Ramasamy Kannan

This project was a joint effort by all the team members. The team worked together to execute the project and produce the report.

Abstract— **In today's environment, security plays a vital role in communication. To prevent raw data from being stolen, we use encryption. Encryption is the way of encoding plain text with a key by which only authors with that key can securely view the information. Similarly, Decryption is the way of decoding the cipher text with the key. Images are generally stored in the hard drive/internal storage, making it possible for any intruder to access the images when a mobile device gets stolen.**

To overcome this issue, Image Encryption can be implemented. Image Encryption is the method of converting a plain image to a cipher image with a key using various encryption techniques. We propose an Image Encryption method using Arnold map and Henon map which can be used along with a mobile vault, where the author can upload their personal images, which will be encrypted and stored in the mobile device's local storage.

.

I. INTRODUCTION

As we all know we are currently living in a digitally evolved society where vast amounts of information are sent via insecure communication channels. These days, data from all social media servers, military based information and other data of very Important sectors are being stored in enormous databases**.** Given the widespread use of technology in current society, there are several issues. Consequently, one of the obvious concerns is currently the confidentiality and security of electronic documents. One of the significant ways to prevent issues of this nature whenever you store or share important images, start adopting to image encryption technologies. An Image encryption vault keeps our data secure by transforming the data into a format that is incomprehensible to the intrusions, this technique or procedure protects information from unwanted cyberattacks. Data decryption is the counterpart of data encryption and restores the actual information.

Contradictory to text encryption, the majority of conventional and common cyphers, such as AES(Advanced Encryption Standard Algorithm), RSA(Rivest Shamir Adleman), IDEA(International Data Encryption) and DES(Data Encryption Standard) etc. doesn't really works adequate for designing cryptosystems for photographic files as they own intrinsic characteristics of image files, such as large - scale data capacity, high redundancy, significantly positive correlation between consecutive frames, etc. Therefore, the traditional encryption procedure can lead to altering the original data format in the image encryption as visual photos have distinctive coding patterns and significant quantities of information.

Considering the disadvantages of using the traditional algorithm in image encryption system we are suggesting a Image encryption application which is built with the help of chaos-based image encryption techniques. Because of the chaos essential trait of sensitivity to initial circumstances, which results in data sets that are predictable yet appear random, there has been an increase in interest in using chaos in cryptography. Cost, processing power, complexity, vulnerability, computational overhead, regarding speed, etc., chaos-based cryptographic models have been applied to create unique techniques for designing effective image encryption systems. So, basically our paper suggests an image encryption method for digital encryption using Arnold cat map algorithm and Herold map algorithm which are Chaos mapping Technique. The flow of our paper goes as detailed discussion of the Implementation, Literature survey, result and our Conclusion.

II. NOVELTY OF THE WORK

The project aspect is to develop an image encryption technique using Arnold and Henon map algorithm. This image encryption method can be used along with a vault to store the images securely. So that even when an intruder tries stealing the device, it will be impossible for him/her to get the raw image.

III. IMPLEMENTATION

Arnold Map:

Arnold's Cat chaotic mapping of two dimensions can be used to move a pixel within an image without erasing any of the image's data. Assume the following to be the pixel image:

$T=\{(a,b) \mid a,b = 0,1,2,3,..N-1\}$

The 2-D representation of Arnold's Cat map can be expressed as:

$\begin{bmatrix} a' \\ b' \end{bmatrix}$ = X * $\begin{bmatrix} a \\ b \end{bmatrix}$ * (modn)

1 r

s (rs + 1) * $\begin{bmatrix} a \\ b \end{bmatrix}$ * (modn)

Here, r and s are positive integers, the determinant (X) = 1.

When Arnold's Cat Map algorithm is run, the initial pixel position (a, b) moves to the new position (a', b').

Algorithm for Arnold Cat Map:

```
ArnoldCatConvert(image,no):
rows, colm
chn<-image.shape
n<-rows
arnoldimage<-nr.zero([row,col,chn])
for i in range(0,rows):
        for j in range(0,colm):
                arnoldimage[a][b]<-image[(a+b)]
return arnoldimage
ArnoldCatEncrypt(img,key):
Image<-cv2.read(img)
For k in range(0,key):
        Image<-
ArnoldCatConvert(image,k)cv2.write(img.split('.')[0]+"Imag
eName.png",image)
return image
```

Henon Map:

Henon map is a dynamic 2-D system, it produces two distinct chaotic sequences. The original/plain image's row and column permutations are then subjected to these sequences. To create a unimodal skew tent map that diffuses pixel values, XOR models are employed. In the final step of the method, each pixel is changed into a brand-new random pixel using Hussain's substitution box.

Algorithm for Henon Map:

Let's take,

$a(k+1) = b(k+1)+1-pa_k^2$

$b(k+1) = qa_k$

Here, (a_0, b_o) is the initial point and p,q are the initial parameters. A mapping is done with (a_n, b_n) and a new point (a(n+1),b(n+1)) using Henon map.

for k in range of (i^2):

$a(k+1) = b(k+1)+1-pa_k^2$

$b(k+1) = qa_k$

bit =0 when a_k<=0.4 or 1

For Encryption and Decryption = ^(image matrix, bit matrix)

Using the initial values that is applied to the Henon map for key generation, the bit matrix can be formed

IV. RESULTS

Image Encryption provides more security and reliability to the user. Using the proposed encryption method implemented with a mobile vault makes any intruder impossible to steal the raw images. This encryption method can also be used with any type application such as web-based, ios-based, android-based etc providing security to all types of users.

V. CHALLENGES FACED

Since we were using two map to form the algorithm, we felt it more complicated. We were initially trying to encrypt larger images which was too time consuming.

VI. CONCLUSION

WE'D LIKE TO EMPHASIZE IN OUR PAPER'S CONCLUSION THAT WE'RE PROPOSING A METHOD FOR PREVENTING SENSITIVE AND DISTINCT PHOTOGRAPHIC DATA FROM BEING EXPOSED TO INTRUSION. WE HAVE DEVELOPED A IMAGE ENCRYPTION METHOD THAT CAN BE USED ALONG WITH A VAULT THAT HELPS ENCRYPTING REGULAR IMAGES INTO PHOTOGRAPHIC DATA THAT CAN ONLY BE DECIPHERED BY AUTHORIZATION PEOPLE WHO HAS THE KEY. GIVEN THE DRAWBACKS OF CONVENTIONAL ENCRYPTION ALGORITHMS, WE HAVE OPTED TO USE CHAOTIC MAPS IN OUR SYSTEM BECAUSE OF ITS ADVANTAGES, INCLUDING SPEED, HIGH SECURITY, REASONABLE COMPUTE OVERHEADS, AND PROCEDURAL POWER.

REFERENCES

[1] T. Li, B. Du and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," in IEEE Access, vol. 8, pp. 13792-13805, 2020, doi: 10.1109/ACCESS.2020.2966264.

[2] Pan, H., Lei, Y. & Jian, C. Research on digital image encryption algorithm based on double logistic chaotic map. J Image Video Proc. 2018, 142 (2018). https://doi.org/10.1186/s13640-018-0386-3

[3] Khan M, Waseem HM (2018) A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS ONE 13(11): e0206460. https://doi.org/10.1371/journal.pone.0206460

[4] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang and Mengmeng Wang, "Digital image encryption algorithm based on pixels," 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems, 2010, pp. 769-772, doi: 10.1109/ICICISYS.2010.5658790.

[5] P. A. -N. Agbedemnab, E. Y. Baagyere and M. I. Daabo, "A New Image Encryption and Decryption Technique using Genetic Algorithm and Residual Numbers," 2019 IEEE AFRICON, 2019, pp. 1-9, doi: 10.1109/AFRICON46755.2019.9133919.