International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Enhanced Security with Minimum Storage in Aadhaar Card

Jyoti
Computer Science Department, IIMT College of Engineering, Greater Noida, Uttar Pradesh, India
Email : jyoti18kataria@gmail.com

ABSTRACT

Aadhaar Card project is one of the most ambitious and controversial project in India launched by government of India. The project issue Unique Identification Number (UID) to each residents of India, which will work as Proof of Identity throughout the country. It collects biometric and demographic data of residents and stores these in a centralised database. However recently there has been a deliberation over the privacy and security issues related to the Aadhaar project. This Project proposes the security of the data stored by the Aadhaar project with the minimum storage of space in the direction of encryption and steganography

Keywords: Aadhaar, Encryption, Embedding, Arnold's Transformation, LSB, Steganography

I. INTRODUCTION

The Aadhaar project is the world's largest national identity project launched by government of India. It collects the biometric and demographic data of residents of India and provide a unique identification number (UID) to them. This number is unique and is linked to an individual's unique biometric and demographic information. This collected data stored in the central database known as Central Identity Data Repository (CIDR). Security of the data is a very important concern [1]. This proposed project "enhanced security with minimum storage in Aadhaar card'' provide two key level security. First of all, encryption is done on the information and generation of first key taken place then embedding process occurs and generates another second Key. So in future if there will be any access from unauthorized person. The person is unable to encrypt the information until or unless he/she can have the two keys.

II. METHODOLOGY

The methodology is proposed in order to assure security for Aadhaar project. This proposed system structured in two phases :-

i. Encryption phase.
ii. Embedding phase.

Encryption Phase

Encryption is a process of encoding the plain text into a cipher text in such a way that only the authorised party can access it. This encoding scheme generates a key, without this key decryption is not possible.

In this project, the encoding can be done by the one of the encrypting algorithm, the Arnold's transformation. Aadhaar deals with the image so when the text is embedded into the image the quality of the image is deteriorated. The application of this algorithm mainly helps in restoring the quality of image. The Arnold mapping ensures that the image pixels are thoroughly scrambled after every step to remove any correlation with the original image contents. Thus it enhances the security of the proposed method [2]

The process of Arnold's transformation is as follows-

i. Read the colour pixel of the image.
ii. Calculate the position (x, y) pixel in the image to be encrypted.
iii. Rotate RGB pixel to the image.
iv. Repeat step 3 until and unless the whole image can convert into a cipher code

Embedding Phase

The embedding can be done by least significant bit (LSB) algorithm. Least significant bit (LSB) is an approach to embed information in an image file in such a way that does not allow any "enemy" to even detect that there is a secret message present in the image. This technique of hiding message in the image is known as steganography [3].

The process of least significant bit is as follows

i. Select an image of size M*N as an input.
ii. The message to be hidden is embedded in RGB component only of an image
iii. Use a pixel selection filter to obtain the best areas to hide information in the image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).

First of all, take the original image and demographic information of the applicant who applies for the Aadhaar card. This is known as Registration process. After that, the original image and information is transformed into a square matrix and encryption phase occurs that convert the information into a cipher text that generates the first key. This cipher text has to be embed in the original image of the applicant and this phase is known as embedding phase and generates second key. The original image after the embedding is known as carrier stegno image. This carrier image has demographic information as well as original image of the candidate taken during the registration process.

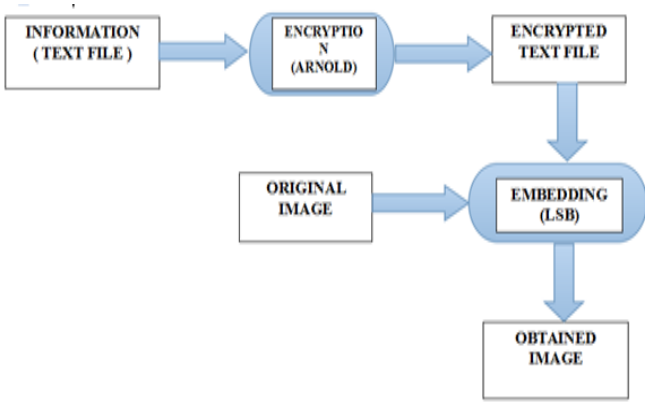

Figure 1. Block Diagram of the Proposed Model

III. RESULTS AND DISCUSSION

The performance of the proposed technique is measured through a series of tests. These tests include entropy measurement, histogram analysis, processing time measurement, histogram deviation, correlation analysis, key sensitivity, SNR, PSNR. The results of these tests showed that the proposed image encryption technique provides an efficient and secure way for encryption. The proposed technique run time is small and hides the data into the image that make less use of memory space as it's save the demographic data and the image of the applicant into a one carrier image.

IV. CONCLUSION

In this paper, a new efficient security model based on the combination of Arnold's transformation and least significant bit is presented that provides two key level securities. These two keys make the system highly secured .It deals with the demographic data not with the biometric data. In this project, no one can find that the information is hidden in the image except the authorized person. If by any chance unauthorized person can knows that information is hidden in the image. He/she cannot decrypt the image until and unless he/she can have the both keys. This project is highly specified for the use in securing data server that is Central Identity for Data Repository. Application of this system can enhance the security of the sensitive information collected for the purpose of making of Aadhaar Card

V. REFERENCES

[1]. https://uidai.gov.in/
[2]. P. Gupta, S. Singh and I. Mangal, "Image Encryption Based On Arnold Cat Map and S-Box," IJARCSSE, vol. IV, no. 8, pp. 807-812, 2014.
[3]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013.