

## Encrypting Demographic Information to 2d Image

<sup>1</sup>S. Arunpandian, <sup>2</sup>Dr.S.S Dhenakaran

*Ph.D Research Scholar, Department of Computer Science Alagappa University, Karaikudi.*

*spandiyan01@gmail.com*

*Professor, Department of Computer Science, Alagappa University, Karaikudi.*

*ssdarvind@yahoo.com*

**Abstract:** Nowadays, communication depends on radio waves for sharing information at distant place where wireless technology is popularly used for short communication and most of the applications are executed by mobile phones and people are facing problems in operating mobile apps by opening many apps knowingly or unknowingly and hence their data are stolen by hackers. Though applications have features to protect data by encryption mechanisms, it seems insufficient to protect vital information. Perpetrator hacks personal information of others which is the main task of cyber space attacks since the information relates to money and Business confidential data. It is seen that the personal information is structured data which use insufficient encryption technique in applications like Aadhar and Banking systems. In this paper, a new approach is designed for text encryption to secure the information that may be difficult to access the personal information. Generally, text encryption is done by replacing original character by some other symbols using emojis, extended Ascii key, different languages which are not fulfilling standards of encryption. Here an innovative strategy has proposed for text encryption. Initially the given text is converted to a 2D image. The image encryption is employed for encryption giving another form of image. The hackers have the intuition of image processing principles to find out facts of the image. Hence the proposed method may fulfill the need of requiring innovative principle to hide the sense of data.

**Keywords:** Encryption, Decryption, Security, 2D image, Applications,

### I. INTRODUCTION

Due to the rapid growth of technology, digital information security is becoming an important issue for breaching data [2]. Data breaches are occurring by lack of security, which are the chances for hacking or altering the precious information by intruders. To reduce the security issues, cryptography plays a vital role for avoiding the problems of security issues. The two basic synonyms in cryptography are encryption and decryption, which enable data protection in unpredictable form. The encryption techniques are classified as symmetric and asymmetric encryptions based the method and approach of using keys. Symmetric key techniques are implemented in many applications. Among the symmetric key encryptions, AES (Advanced Encryption Standard) provides the exponential security for data than other mechanisms because it includes different manipulation functions viz, subBytes, ShiftRows, Mix column, AddRoundKey which makes iteration 10 times for 128 bit, 12 times for 192 bit, 14 times for 256 bit[4]. AES algorithm uses substitution and permutation rule which are the basic steps to form a encryption block. On the other hand, RSA and Elliptic curve cryptography are efficient techniques in asymmetric encryptions. In these techniques public and private key are used for encryption. In RSA algorithm, computational process is difficult since it uses 1024 bit and 2048 bit keys [5]. In Elliptic curve cryptography (ECC), keys are generated by properties of elliptic curve equation and it works efficiently due to faster key creation. Finally, the key size is smaller which gives the equivalent security with lower computing power and these features are suitable for mobile applications [5]. The proposed work uses the symmetric key algorithm for encrypting the original data by transform text into image form. The outcome of encryption is a graph which is an innovative approach to implement the ciphertext.

### II. LITERATURE REVIEW

Information security is an important science which could be managed by cryptography. In secure information and communication system, cryptography is a significant component protecting information. It is the main alternative for protecting the text data as well as image data. Text information are transformed and reformatted by the cryptography technique, which makes safe to travel information data between computers. There are number of relevant works which are briefed here.

Sourabh Singh, Anurag Jain has proposed text to image for encryption which is entitled as "An Enhanced Text to Image Encryption Technique using RGB Substitution and AES". Text data is converted to image in encryption process which is accomplished by RGB substitution with the help of a key by AES

algorithm [6]. In this approach text information is shared easily without any scaring and if the intruder steals the encrypted image then downloaded another image instead of original encrypted image.

Amal Joshy, Amitha Baby K X, Padma S, Fasila K A et.al, The paper entitled as “Text to Image Encryption Technique using RGB Substitution and AES” mainly for making an android application. In this work [7], text is converted into image. RGB substitution technique produces image which is encrypted by the AES encryption algorithm. A pixel added in addition to the encrypted image which gives the additional security. Generally image consists of rgb values in an image. When extracting RGB value, extra value is added randomly with R and G by mapping scheme. B is a constant which does not have any additional value. The key was used by the AES algorithmic by altering the corresponding rgb value.

Anjali suresh, Remya Ajey A S, has proposed a work titled “VLSI Implementation of Text to Image encryption algorithm based on private key encryption”. Cryptography algorithms not only proposed for software applications but also used in hardware implementations. Reprogrammable devices such as Field Programmable Gate Arrays are the cryptography hardware applications [1]. In this work, algorithm generates different random value for R, G and B for every letter in text. When these values are combined, a color image is formed and generated and keys are generated from letters of text. This mechanism is used in offline machine as well as reliable for email security.

### Proposed Work

The proposed work is a novice encryption for the security of plain-text. In this work, plain-text is inverted into interlaced objects with jpeg format by the mathematical manipulations. This approach contains plain-text module, encryption module and image module. Based on the plain text the encrypted data is changed dynamically. The plain text module reads text information which holds demographic information of name, address, mobile number, father and mother name, date of birth and identification number of particular person. The second module deals with encryption and decryption process which works with mathematical strategies of ASCII value conversion, subtraction, divide, modulo and concatenation to complicate the encryption process.. Finally, an image is generated by RGB values and 2D parameters height, width of image.

### Functional Block Diagram of Proposed Work

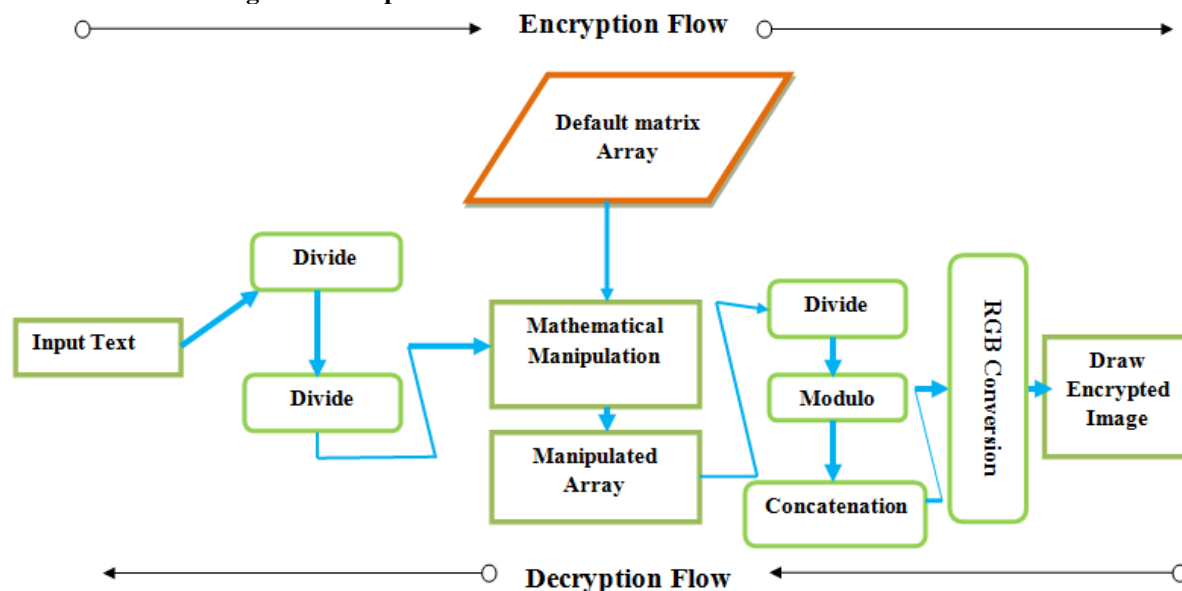


Figure 1: Functional Block Diagram

### Encryption Algorithm

- Step 1:** Read the demographic information of person.
- Step 2:** Take the characters of demographic information.
- Step 3:** Characters are replaced by ASCII values
- Step 4:** Dynamically create Default array filled with 255 values in each position based on input characters
- Step 5:** Subtract the ASCII values from Default Array and results are stored
- Step 6:** Results are manipulated with divide, modulo, concatenation operations to get the RGB values
- Step 7:** Finally, Draw interlaced Square image for RGB values.

### Decryption Algorithm

**Step 1:** Read the Interlaced square image.

**Step 2:** Extract RGB values from that Image with mathematical manipulation operations.

**Step 3:** Add the RGB values with Default Existing value (255).

**Step 4:** Resultant is converted into ASCII values.

**Step 5:** ASCII values are changed to characters.

**Step 6:** Character are inverted to String (Which is a Personal Details of Particular Person)

### Sample Plain Text Encryption Algorithm

In this section, the intermediate results of the proposed work are shown in seven steps.

**Table 1: Intermediate Results of Encryption**

Step 1: Plain-Text	-	welcome
Step 2: Separate Characters	-	w, e, l, c, o, m, e
Step 3: Equivalent ASCII value	-	119, 101, 108, 99, 111, 109, 101
Step 4: Create an Default Array Depends on input with default value	-	255
Step 5: Subtract ASCII value from Default Array	-	136, 154, 147, 156, 144, 146, 154
Step 6: Divide, Modulo and Concatenation Operation. Here n is a quotient, r – red, g-green, b- blue, s-sum. sum is consider to be an width and height. Note: when result of value divide by 3	-	If remainder is 0, $r=n$ , $g=n$ , $b=n$ , $s=r+g+b$ . If remainder is 1, $r=n$ , $g=n+1$ , $b=n$ , $s=r+g+b$ If remainder is 2, $r=n$ , $g=n+1$ , $b=n+1$ , $s=r+g+b$
Step 7: Draw an square Object x, y co-ordination, s is height and width of an object	-	Write an encrypted Interlaced Square image

### Decryption Algorithm

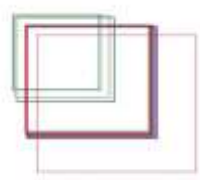

**Table 2: Intermediate Results of Decryption**

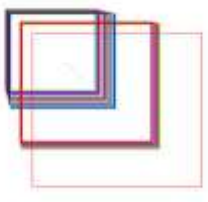
Step 1: Read the image with x,y coordination with height and width of on object	-	Encrypted Interlaced Square Image
Step 2: Mathematical manipulation	-	Quotation, Remainder, $r=n$ , $g=n$ , $b=n$ , $s=r+g+b$ . $r=n$ , $g=n+1$ , $b=n$ , $s=r+g+b$ $r=n$ , $g=n+1$ , $b=n+1$ , $s=r+g+b$
Step 3: Subtract s values from 255 matrix array	-	119, 101, 108, 99, 111, 109, 101
Step 4: Equivalent Character	-	w, e, l, c, o, m, e
Step 5: Together the String	-	Welcome (Plaint Text)

## III. RESULT AND DISCUSSION

The proposed work is experimented for several text inputs. 3 separate plaint text of different personal information are taken as inputs. Each one doesn't have same length of characters. Here, First 70,125,205 characters of plain text are taken and their encrypted file is shown in an image. Depends on the characters, shift image are changed. Parameters of 2d object are height and width defined by the summation of red, green, blue values with x and y coordination. These parameters are used by this work and text to another image by encryption.

**Table 3: Result of Proposed Encryption**

S.No	Length of the Plain Text	Encrypted Image
1	70 Characters	
2	125 Characters	

3	205 Characters	
---	----------------	--

#### IV. CONCLUSION

Nowadays personal information is stored either in hand-held devices or computer by the end-users. Information is considered important and securing information is vital for preserving information from adversaries or intruders. The proposed work is designed for protecting the personal information by new encryption algorithm. In this work, the personal information is converted into an image that contains 2d objects than ciphertext information. This method can perplex hackers in hacking information.

#### REFERENCES

- [1]. Suresh, Anjali, and AS Remya Ajai. "VLSI implementation of text to image encryption algorithm based on private key encryption." *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on*. IEEE, 2016.
- [2]. Saraf, Kundankumar Rameshwar, Vishal Prakash Jagtap, and Amit Kumar Mishra. "Text and image encryption decryption using advanced encryption standard." *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 3.3 (2014): 118-126.
- [3]. Singh, Virendra Pal, et al. "A New Symmetric Key Encryption Algorithm Based on Jumbling Binary Sequence of Message." 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE). IEEE, 2018.
- [4]. <https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption>
- [5]. <https://searchsecurity.techtarget.com/definition/asymmetric-cryptography>
- [6]. Singh, Sourabh, and Anurag Jain. "An enhanced text to image encryption technique using RGB substitution and AES." *International Journal of Engineering Trends and Technology (IJETT)-Volume4Issue5-May* (2013).
- [7]. Joshy, Amal, et al. "Text to image encryption technique using RGB substitution and AES." *Inventive Computing and Informatics (ICICI), International Conference on*. IEEE, 2017.

#### Authors Profile



**S.Arunpandian**, received her M.Phil degree in Alagappa University, Tamil Nadu. Now he is pursuing his Ph.D (Computer Science) research in the same university. The field of his research is Biometric Security in cryptography.



**S.S.Dhenakaran**, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.