Abstract: In this paper, we propose a novel cryptographic algorithm namely Symmetric Random Biometric key (SRBK) algorithm. The key for this SRBK algorithm is obtained from two biometric features namely ear and lip. The key generated are flexible and can be altered based on the type of algorithm used. We also consider Advanced encryption standard (AES) algorithm for comparison with SRBK algorithm and finally it was proved that SRBK algorithm is better than AES algorithm on selected parameters.

Key words: Bi-modal biometrics, AES, Key generation.

I. INTRODUCTION

Security plays a vital role in transferring huge amount of data across the internet where the information is not safe guarded by any medium. Cryptography is an eminent component in communication which ensures secure transmission and reception takes place between authorized parties. The proper selection of cryptographic algorithm is important for security, efficiency and other parameters. In this paper, a novel method is proposed to generate keys using biometric features like ear and lip. The detailed generation of key by bi-modal method is discussed in [9]. Biometrics is an analysis from human physical and behaviour characteristics. Though many methods are available, we use human EAR and LIP because of its unique features for generating binary values (keys). The advantage of using this biometric feature is that the key generated is flexible. The bits generated at the final stage can be obtained based on the algorithm we use. In this paper, the biometric key is applied to AES algorithm and also to the novel method proposed. In AES, the key length is 128 bits, whereas in SRBK, the length is 16 bits.

1.1. GENERATION OF BIOMETRIC KEYS

Here the initial set of values for keys in terms of 16 bytes are generated from biometric features (Ear and Lip). Two features are taken as reference and 128 bits are generated from the two features.

The steps followed in key generation are:
- Input image
- Conversion from RGB to GRAY-
- Filtering-various filters were applied and analysed to know the better noise removal filter
- Enhancement- Tonal regularisation
- Image reshaping- Mean level of the pixel are adjusted
- Extraction- concentrating and extracting selective feature on the image
- Concatenation- Gradient calculation
- Gradient image
- Sorting- re-arranging the values
- Key generation- binary value is generated as key.

The detailed method of key generation from Ear feature is discussed in [9].

The most popular standard algorithm which is widely used in today’s scenario is AES algorithm. It is found to be several times faster than the triple-DES algorithm.

The features of AES are as follows
- Symmetric key /block cipher.
- Based on number of rounds, the key length is varied.
- Fast and stronger than triple –DES.
- Gives the entire specification and design details.
- Can be implemented in software tools.

II. BIOMETRIC KEY IN AES

The key obtained from biometric feature is flexible and therefore can be applied to AES based on number of rounds.

The overview of key size and rounds is shown in table 1.

Table 1: Relationship between key size and number of rounds in AES.

<table>
<thead>
<tr>
<th>KEY SIZE</th>
<th>NO OF ROUNDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>10</td>
</tr>
<tr>
<td>192</td>
<td>12</td>
</tr>
<tr>
<td>256</td>
<td>14</td>
</tr>
</tbody>
</table>

Fig 1: The general schematic of AES algorithm [3]
2.1 AES ANALYSIS USING BIOMETRIC KEYS

The keys obtained from ear and lip biometric features are given as input(key) to the encryption /decryption process of AES algorithm. The 128-bit key and 10 round operation is performed. The results are shown below.

2.1.1. Encryption:

Fig 2: biometric key used in AES for Pre-round

Fig 3: Cipher taken for process.

Fig 4: Initial round 1 process

Fig 5: Round 2 process

Fig 6: Round 3 –AES

Fig 7: Round 4 –AES

Fig 8: Round 5-AES
2.1.2. Decryption:
The key and cipher text obtained from the final step of encryption process is given as input to the decryption. Fig 15 shows the first step in decryption and fig 16 shows the final key and plain text obtained.

In today’s scenario, AES is widely used and accepted for hardware and software implementation. Till date, no practical cryptographic attack has been identified or reported. Additionally, AES has built-in key flexibility which improves the overall advantage of the process. However, similar to DES, AES security is assured only if it is correctly implemented with the proper key management techniques. [2]
III. THE PROPOSED NOVEL METHOD: SYMMETRIC RANDOM BIOMETRIC KEY (SRBK) BASED CRYPTOGRAPHY

3.1. ENCRYPTION

![Flow chart of SRBK Encryption](image-url)

Step 1: Initial data of size multiple of 8 is taken, if necessary do padding.
Step 2: Data is divided into 8 characters each.
Step 3: Convert into its corresponding ASCII equivalent.
Step 4: Concatenate the alternate set of binary values
Step 5: Reverse the order of bits from step 4
Step 6: Bringing the concatenated biometric key from ear and lip
Step 7: Ex-or the result of step 5 and step 6
Step 8: Perform 1-bit right shift with result obtained from step 7
Step 9: 1’s compliment the values of step 6
Step 10: Ex-or the result of step 8 and step 9
Step 11: Duplicating each bit once to get 32-bit cipher text

<table>
<thead>
<tr>
<th>PLAIN TEXT</th>
<th>S</th>
<th>U</th>
<th>C</th>
<th>C</th>
<th>E</th>
<th>S</th>
<th>E</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>83</td>
<td>85</td>
<td>67</td>
<td>67</td>
<td>69</td>
<td>83</td>
<td>69</td>
<td>83</td>
</tr>
<tr>
<td>BINARY VALUE</td>
<td>1010011</td>
<td>1010101</td>
<td>1000111</td>
<td>1000011</td>
<td>1001011</td>
<td>1010011</td>
<td>1010011</td>
<td>1010011</td>
</tr>
<tr>
<td>CONCATENATE THE ALTERNATE BITS</td>
<td>101001101000011</td>
<td>101010101000111</td>
<td>100010101000101</td>
<td>101001101001111</td>
<td>101001101001111</td>
<td>101001101001111</td>
<td>101001101001111</td>
<td>101001101001111</td>
</tr>
<tr>
<td>REVERSE THE ORDER</td>
<td>110000011010101</td>
<td>110000110101010</td>
<td>110101010100010</td>
<td>110011101011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
</tr>
<tr>
<td>KEY CONCATENATE FROM EAR AND LIP</td>
<td>100011110011100</td>
<td>0</td>
<td>101001101010010</td>
<td>100010101000101</td>
<td>101001101001111</td>
<td>110001011011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
</tr>
<tr>
<td>KEY’S COMPLIMENT</td>
<td>011000011010100</td>
<td>0</td>
<td>110101101100010</td>
<td>101001101001111</td>
<td>110011101011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
<td>110011101011010</td>
</tr>
<tr>
<td>XOR-ING THE REVERSE BIT WITH KEY</td>
<td>011110111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
<td>111101111111100</td>
</tr>
<tr>
<td>1 BIT RIGHT SHIFT</td>
<td>111111111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
</tr>
<tr>
<td>XOR-ING WITH KEY’S COMPLIMENT</td>
<td>111111111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
</tr>
<tr>
<td>DUPLICATING EACH BIT ONCE TO GET THE CIPHER TEXT</td>
<td>111111111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
<td>11110001111111111</td>
</tr>
</tbody>
</table>
3.2. DECRYPTION:

Step 1: The 32-bit cipher text is obtained, in which the even number of bits are removed.

Step 2: The data is divided into four sets of 16 bit values.

Step 3: The key's compliment value is obtained which is ex-ored with step 2.

Step 4: Perform 1-bit left shift with the result obtained from step 3.

Step 5: Ex-or the key value with the left shifted bits.

Step 6: Reverse the order of bits with the result from step 5.

Step 7: Split into 8 sets of 8-bit binary values.

Step 8: Swap the 2nd and 3rd byte values and 6th and 7th byte values.

Step 9: Convert into corresponding ASCII from the result obtained in step 8.

Step 10: The 8-character plain text is obtained.

---

**Fig 18 : Flow Chart – Decryption**

---

**Table 1**: Decryption Process

<table>
<thead>
<tr>
<th>Cipher Text</th>
<th>11111111111111111111111111111111</th>
<th>11111111111111111111111111111111</th>
<th>11111111111111111111111111111111</th>
<th>11111111111111111111111111111111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removal of even bits</td>
<td>111111111111111111111111</td>
<td>111111111111111111111111</td>
<td>111111111111111111111111</td>
<td>111111111111111111111111</td>
</tr>
<tr>
<td>Key's Compliment</td>
<td>1010001100101</td>
<td>1000110011011</td>
<td>1010011011011</td>
<td>1000110011011</td>
</tr>
<tr>
<td>XORing the obtained bit with the above 1's complement of the key</td>
<td>0100010010101</td>
<td>0100010011011</td>
<td>0100010011011</td>
<td>0100010011011</td>
</tr>
<tr>
<td>1-bit left shift</td>
<td>1000110010101</td>
<td>1000110011011</td>
<td>1110011101100</td>
<td>1110011101100</td>
</tr>
<tr>
<td>XORing the left shifted bits with the key</td>
<td>1100000101100</td>
<td>1100000101100</td>
<td>1100000101100</td>
<td>1100000101100</td>
</tr>
<tr>
<td>Reverse the order</td>
<td>1101000101100</td>
<td>0100011011011</td>
<td>0110011001011</td>
<td>0100011011011</td>
</tr>
<tr>
<td>Split into 8 bits each</td>
<td>0100011011011</td>
<td>0110011001011</td>
<td>0100011011011</td>
<td>0100011011011</td>
</tr>
<tr>
<td>Swapping 2nd &amp; 3rd byte and 6th &amp; 7th byte</td>
<td>0100011011011</td>
<td>0110011001011</td>
<td>0100011011011</td>
<td>0100011011011</td>
</tr>
<tr>
<td>ASCII</td>
<td>83</td>
<td>83</td>
<td>67</td>
<td>67</td>
</tr>
<tr>
<td>Plaintext</td>
<td>S</td>
<td>U</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>
3.3. Symmetric Random Biometric Key- Features

- The proposed algorithm will be several times faster than the existing algorithm.
- This algorithm is safe against unauthorized attacks and runs faster than the popular existing algorithm.
- With this new approach we are implementing a technique to enhance the security level of this algorithm and further reduce the time for encryption and decryption.

IV. RESULTS AND DISCUSSIONS

Comparison is made between the AES algorithm and SRBK algorithm. Memory occupied by SRBK is several times lower than AES algorithm. The encryption time (time taken by the algorithm to convert from plain text to cipher text) is calculated for both the algorithms. Since the number of steps for encryption and decryption is less for SRBK, the overall encryption and decryption time is lesser than AES. The throughput is obtained based on the encryption time. It shows the speed of encryption and decryption. The speed at which the total plain text encrypted divided by encryption time. The throughput is higher for SRBK compared to AES.

V. CONCLUSION AND FUTURE WORK

Thus the proposed algorithm occupies less memory and encryption and decryption time proving it is better than existing encryption algorithm. The biometric key used for encryption and decryption is flexible and the number of bits can be changed based on the plain text used. We also say that the key is secure since it is generated from our own biological trait.
The future work can be extended with the additional novel method with increase number of rounds for better security and the increased key length for encryption and decryption. Additional algorithm can also be used for comparison.

REFERENCES


2. “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”- Ako Muhamad Abdullah-Reasearch gate- Publication Date: June 16, 2017


9. .Formulation of Ear Biometric Key with an Eminent Noise Immune Filter to Provide High Security in Authentication –Ms.S.Pavithra, Dr.P.Muthukannan, Mr.V.Prabhakaran, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018


15. “SURVEY ON DIFFERENT TYPE OF ENCRYPTION ALGORITHMS”- Namdev Choure, Prof. Shrikant Dhamdhere-open access international journal of science