Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

# *A Novel Key Generation Approach Based on Facial Image Features for Stream Cipher System*

Sannidhan M S
*Department of CSE*
*NMAM Institute of Technology*
Nitte, Inida
sannidhan@nitte.edu.in

Sudeepa K B
*Department of CSE*
*NMAM Institute of Technology* Nitte, Inida
sudeepa@nitte.edu.in

Jason E Martis
*Department of ISE*
*NMAM Institute of Technology*
Nitte, Inida
jason1987martis@nitte.edu.in

Abhir Bhandary
*Department of ISE*
*NMAM Institute of Technology*
Nitte, Inida
abhirbhandary@nitte.edu.in

***Abstract*—Security preservation is considered as one of the major concerns in this digital world, mainly for performing any online transactions. As the time progress, it witnesses an enormous amount of security threats and stealing different kind of digital information over the online network. In this regard, lots of cryptographic algorithms based on secret key generation techniques have been implemented to boost up the security aspect of network systems that preserve the confidentiality of digital information. Despite this, intelligent intruders are still able to crack the key generation technique, thus stealing the data. In this research article, we propose an innovative approach for generating a pseudo-pseudo-random key sequence that serves as a base for the encryption/decryption process. The key generation process is carried out by extracting the essential features from a facial image and based on the extracted features; a pseudo-random key sequence that acts as a primary entity for the efficient encryption/decryption process is generated. Experimental findings related to the pseudo-random key is validated through chi-square, runs up-down and performs a period of subsequence test. Outcomes of these have subsequently passed in achieving an ideal key.**

***Keywords— Pseudo random number, stream cipher system, feature extraction, linear feedback shift register, secret key generation***

## I. INTRODUCTION

Information security is one of the primary concerns in data transmission over an online network[1], and cryptography is one of the best-adopted technique meant for the secure transmission of digital information by ensuring the protection against fraudulent intruders. Any cryptographic method provides data protection by converting actual data into a ciphertext (encrypted data) that is difficult to understand. An encrypted data can be transformed back to an actual data by those possessing a secret key. Hence a cryptographic method is a package of encryption, decryption and secret key generation algorithms. A cryptographic method is considered secure if an intruder fails to identify the properties of a plain text or a secret key through ciphertext. Thus, it is essential to have a powerful secret key for a cryptographic method so that it becomes impossible for an attacker to break the secret key. In this regard, researches have proved that a secret key of more substantial length considerably provided better security and hard to break. Recent past, several innovations were carried out in the area of the secret key generation algorithm and came up with a variety of techniques to generate the secret key. Out of all the methods random key generator proved to be one of the versatile secret key generation techniques [2].

Random key generators came out as an essential part of secret key generation techniques in modern cryptography. A tremendous amount of research work has done a remarkable job in the design of random key generators. Still, the research work in the design of random key generators continued making its impact in implementing a variety of random number generators causing the secure production cryptosystems. As it is already known, randomness property neither has a rule nor has an identical probability of occurrence. Since random numbers possess this aspect, they are proving as an essential part of a key generation that can generate a very secure key. Any cryptosystem using random number generators for secret key generation depends on the randomness factor of the number generated. Hence the primary focus of the random number generator is to create a massive series of numbers that are not dependent on each other under a range that is defined. As the usage of sensitive data over the communication channel is getting increased day by day, it is essential to produce an unpredictable secret key. In this direction, a robust random number generator plays a compelling role in preserving the quality of a secret key generated. A good random number generator also has a vital contribution in strengthening the cryptographic algorithms meant for encryption and decryption. Researches carried out in the area of secret key generation explored a type of a random number generator termed as Pseudo-Random Number Generator (PRNG) [3]. A PRNG uses mathematical models for producing a very long pseudo-random number sequence from a selected short series of number known as a seed value. A seed value can be derived from any source that is invariant and hard to predict. Modern researches in the area of cryptography stressed on the importance of a kind of PRNG known as Linear Feedback Shift Register (LFSR) for effective generation of a quality secret key.

Cryptosystems use an essential variant of encryption algorithm called stream cipher. A stream cipher is a symmetric key cipher system were a stream of digits representing an actual data is combined with a stream of numbers representing the symmetric key to generate an encrypted data called cipher digit stream. Stream cipher technique predominantly employs the usage of a pseudo-random key generation which encrypts one digit of plain text at a time with a conforming number of key sequence to generate a corresponding digit of the stream cipher [4]. Practically, every bit of keystream is mathematically

combined with every bit of actual data to derive a bit representing cipher data.

Facial feature extraction is a technique used in image processing meant for extracting the interest points (features) of the facial image. Recent past image processing has offered a range of feature extraction techniques based on the approaches of geometric based and appearance-based methods[5,6]. Facial feature points typically range between 48 to 64 features depending on the image considered. Extracted interest points represent some value corresponding to the region of the face like eyes, nose, mouth etc. This technique has great importance in the area of computer vision that deals with various problems corresponding to the digital images representing a face. A feature extraction technique is designed in such a way that it extracts only notable interest points discarding the irrelevant features. Research observations carried out under feature extraction techniques have shown that the extracted feature values are unique and random[7,8]. Due to this property, a feature extraction technique can be considered as one of the better methods for deriving a seed value required for the formation of a pseudo-random number of extensive lengths.

Plenty of research work has been carried out in the area of visual cryptography using a standard key generation algorithm that concentrated on image encryption as a part of data protection. But none of them attempted using the features of image for pseudo-random key generation. Hence under this research article, we propose a novel pseudo-random key generation technique for encryption/decryption that uses the features extracted from the facial image as a seed value which then fed into the designed LFSR for generating asymmetric pseudo-random key of enormous length. To validate the working criteria of the proposal, actual data on the sender side is encrypted by the stream cipher technique using the combination of an actual data stream and pseudo-random keystream to achieve a cipher data stream. Later cipher data stream on the receiver side is decrypted using the combination of a cipher data stream and the pseudo-random key to achieve original data. In this work, we have considered an audio file for testing the working of an entire encryption/decryption process.

## II. RELATED WORK

Sudeepa, K. B., & Aithal, G. (2017) in their article [9] stressed upon the generation of a pseudo-random key sequence of a long length for the stream cipher generation and successfully proved the strength of the key. In an article [10], researchers have implemented a word-oriented random key sequence using the LFSR technique and successfully tested the power of the generated key by statistically examining it for randomness. Kokila, R et al. in an article [11] presented a survey on comparative analysis various extraction techniques and concluded that SURF extracts more number of relevant features and performs the extraction faster than any other extraction methods. Authors, in their research paper [12] implemented a novel technique for feature extraction using the combination of SIFT and SURF. In this article, they have successfully proved that interest points produced of SURF are more accurate and random for classification than the interest points provided by SIFT. Sannidhan, M. S., & Chaitra, K. M. presented a research article [13] dealing with various enhancement procedures for increasing the classification accuracy of matching digital photo images with composite sketches. In this work, they have used SURF for feature extraction because they produce a more significant number of random interest points faster that helps to achieve the classification accuracy. Experimental results presented in this research paper has successfully proved the strength of SURF in feature extraction.

## III. METHODOLOGY

The entire working procedure of the encryption/decryption process using a pseudo-random key generation process is implemented as illustrated in Fig. 1. The whole working methodology comprises four major phases: 1) Feature extraction using SURF 2) pseudo-random key generation using LFSR 3) Encryption Process 4) Decryption process. To perform the method of feature extraction, a facial image is considered as input, and the process of encryption and decryption is validated considering an audio file as input.

As depicted in Fig. 1, the working procedure initially begins by extracting facial features from the facial image using the SURF technique. In the second stage, extracted features are fed into the designed LFSR to generate a symmetric pseudo-random key. Generated pseudo-random key in the third stage is used to encrypt an audio (original audio) file using stream cipher technique resulting in an audio stream cipher data. Later in the last step, initially generated pseudo-random key is used to decrypt the stream cipher data to derive the original audio stream. The detailed working of each of the phase involved in the proposed system is discussed in the following subsections.

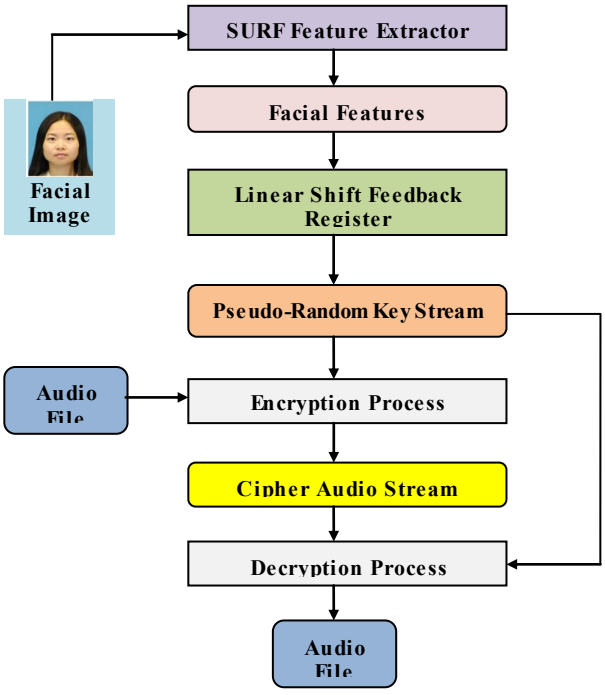



Fig. 1. Working Methodology of the proposed system

### A. *Feature extraction*

Under this phase of the proposed system, facial image features are extracted using notable Speeded Up Robust Feature (SURF) algorithm. SURF is a combination of detector and descriptor that detects the feature (interest) points of an image and describes the detected features with some values. Several research studies have claimed that the extractor is faster as well as robust for any transformations on the image and is applied in the area of object detection, object tracking, facial recognition etc. [14,15]. Fig. 2 represents a snapshot of the result achieved through SURF feature extraction process applied to the sample image of standard CUHK dataset [16] depicting the extraction of 64 interest points on the face.

Fig. 2. Feature points extracted using SURF

Two essential phases of SURF feature detector and feature descriptor are discussed in subsections in detail.

- *Detector phase*

SURF performs feature detection process by breaking up of an image into a collection of square shape Gaussian filters of size 9X9. This filtering is relatively fast with an integral image. The mathematical formulation of Gaussian filtering is depicted as sum expression in equation (1)

$$S_c(X,Y) = \sum_{p=0}^{X}\sum_{q=0}^{Y} I_m(p,q) \quad (1)$$

Parameter $S_c$ represents the coordinate, X and Y represents the corner points of the square. $I_m$ Represents the image p & q represents the sum of pixels along X & Y, respectively.

Once after applying the filter, in the next step SURF uses a Hessian matrix concept by computing the determinant of each of the matrix and combining it with a constant scale factor represents a point P(X, Y) which is considered as an interest point. Computation of Hessian matrix represented by $H(P,\sigma)$ were $\sigma$ is constant with value 1.2 for a square matrix of 9X9 is depicted as in equation (2)

$$H(P,\sigma) = \begin{pmatrix} l_{XX}(P,\sigma) l_{XY}(P,\sigma) \\ l_{YX}(P,\sigma) l_{YY}(P,\sigma) \end{pmatrix} \quad (2)$$

Parameter $l(P,\sigma)$ is the second-order derivative of Gaussian filter.

- *Descriptor phase*

Under this phase, the algorithm describes the previously detected interest points with unique values based on the intensity distribution concerning neighbouring pixels. Very often uses integral values for fast processing.

### B. *Pseudo-random key generation using LFSR*

This step of the proposed system deals with the generation of a pseudo-random key by designing a new pseudo-random generator known as a Linear Feedback Shift Register (LFSR). LFSR is a shift register that shifts the bit value serially upon receiving an input [17-19]. Fig. 3 presents the overall working methodology of LFSR designed for generating a pseudo-random key sequence for the proposed research work.

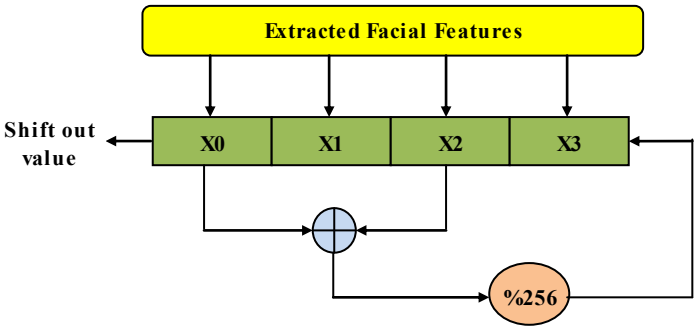



Fig. 3. Design of Linear Feedback Shift Register

As presented in Fig 3, an LFSR operates on a sequence of four facial features extracted at a time, and each element is stored in a separate registers X0 to X3 sequentially. Each sequence of four features represents the seed value for a long series of pseudo-random key generation. The working concept of the model begins by adding the contents of register X0 and X2. Modulo of 256 is obtained from the resulting sum and is termed as Xnew. Parameter Xnew is then shifted into the last register and performing the left shift operation from register X3 to X0 shifting out the previous value of X0 to generate a new sequence of four values. If the generated sequence is not repeated previously, then the sequence is recorded in a separate stream buffer, and the process is iteratively carried until the occurrence of a repeated sequence. On repetition of the sequence, a new sequence of four features are fetched, and the actions of LFSR is repeated until it completes bringing all the features extracted. Once after ultimately bringing all the features, the first value of every non-repeating sequence is fetched from the stream buffer and are arranged sequentially to generate a long sequence of the pseudo-random key. Following equations describes the working concept of LFSR mathematically.

$$X_{new} = (X_0 + X_2)\%256 \quad (3)$$

$$X_3 = X_{new} \quad (4)$$

$$X_2 = X_3 \quad (5)$$

$$X_1 = X_2 \quad (6)$$

$$X_0 = X_1 \quad (7)$$

Equation (3) represents the operation of deriving $X_{new}$ and equation (4) to equation (7) represents the left shift operation performed by LFSR to generate a new sequence.

### B. *Encryption process*

Under this step of the proposed system, it performs the process of encryption where a stream of actual information is encoded using a pseudo-random key to generate a stream of cipher information. The core functionality of this module involves the usage of standard addition operation that encrypts a byte of actual information by adding it with a byte of the pseudo-random key. Entire working model of this stage is presented in Fig. 4.

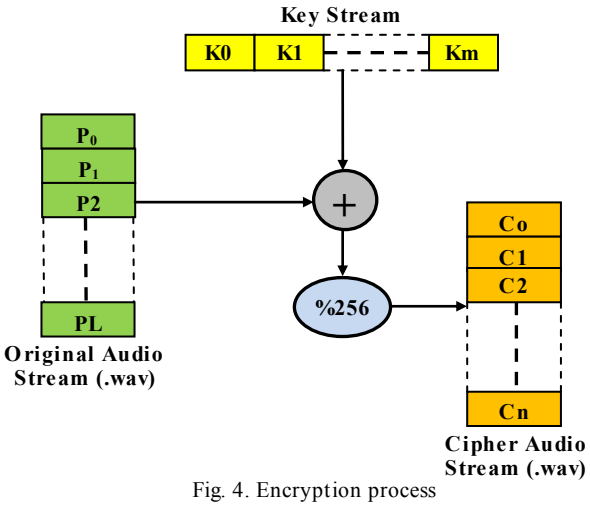



Fig. 4. Encryption process

In Fig. 4, we have considered encoding an uncompressed (.wav format) original audio file stored in a stream of byte array where P0, P1, P2….PL is the stream of bytes representing an audio file. The generated sequence of the pseudo-random key is deposited in a byte array where K0, K1…. Km represents a byte of the pseudo-random key sequence. Working principle of encryption process involves sequential addition of modulus 256 bytes of the original audio stream with modulus 256 byte of keystream. The resultant sum of the sequential addition represents the stream of cipher audio where C0, C1, C2…. Cn is a sequence of bytes representing cipher audio stream. In the process, to preserve attributes of an audio file, we have ensured that the header information of an audio file is not altered. Equation (8) mathematically describes the working procedure of the encryption process.

$$C_i = (P_i + K_i) mod 256 \quad (8)$$

In equation (8), $C_i$ represents a byte of cipher audio stream, $P_i$ represents a byte of the original audio stream and $K_i$ represents a byte of pseudo-random keystream.

### C. *Decryption process*

The proposed research work has implemented decryption as a reverse procedure of encryption which operates decoding the encoded information. A reverse process of encryption involves the application of the subtraction procedure on encrypted information to extract the decrypted data, as illustrated in Fig. 5.

The working concept of the decryption process begins with a cipher stream of an audio file stored in a byte array. Here in the case of decryption, modulus 256 bytes of a cipher audio stream is sequentially subtracted with modulus 256 of the byte of the keystream to achieve a stream of the decrypted audio file. Entire working methodology of the decryption process is depicted in fig 5 where C0, C1, C2…. Cn is a sequence of bytes representing cipher audio stream.

K0, K1…. Km is a sequence of bytes of the pseudo-random keystream and P0, P1, P2….PL denotes the sequence of bytes corresponding to the decrypted audio stream.

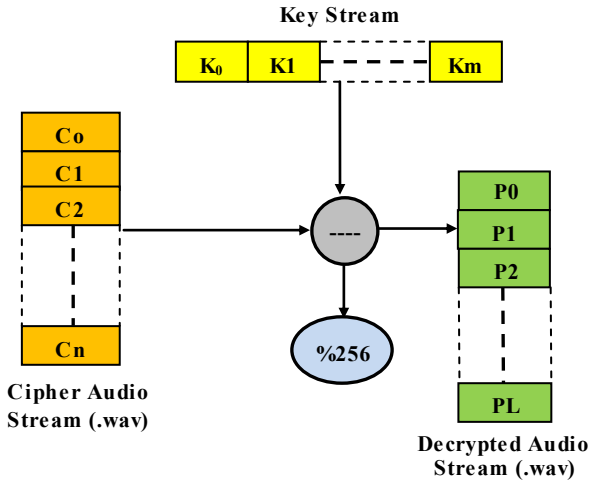



Fig. 5. Decryption process

Equation (9) presents the mathematical formulation describing the working concept of the process

$$P_i = (C_i - K_i) mod 256 \quad (9)$$

Where $P_i$ represents a byte of the decrypted audio stream, $C_i$ signifies a byte of cipher audio stream and $K_i$ represents a byte of keystream.

## IV. RESULTS AND DISCUSSION

Experimental observations concerning the proposed system are discussed in this section. Significant findings of the suggested procedure concentrated on evaluating the strength of the pseudo-random key concerning to encryption process. For feature extraction required for key generation, we have considered images from CUHK dataset, which is open to the research community. Further to carry out the process of encryption and decryption, we have utilized an uncompressed audio file of .wav format having a timeline of 3 seconds with irregular variation and frequency.

Initially, a sample picture is considered from the data set, and the features are extracted out of it using a SURF algorithm as presented earlier in Fig. 2. Here for the recognized image, SURF extracted 59 nonzero elements. Extracted feature values are fed into LFSR, which generated a pseudo-random key sequence with a length of 10460 keys which is approximately 175 times the 59 features extracted. Extracted feature values

and the produced series of pseudo-random key value is graphically presented in Fig. 6 and Fig. 7 respectively.

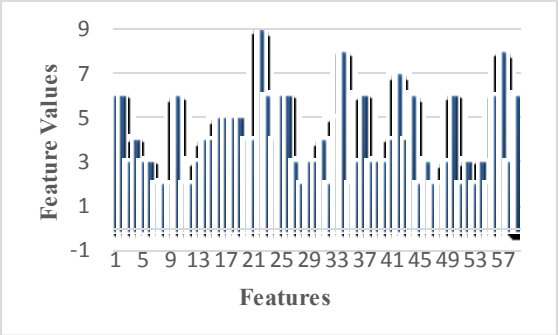



Fig. 6. Snapshot of feature points located in a facial image

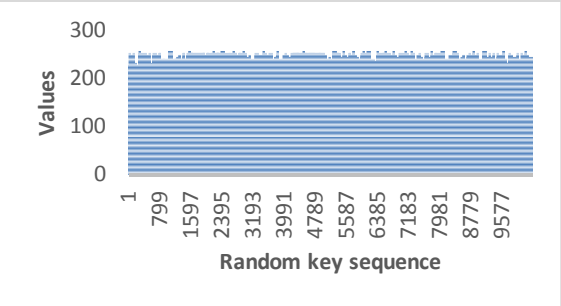



Fig. 7. Generated pseudo-random key sequence using LFSR

The focus of this research work aims in evaluating the strength of the pseudo-random key generated, and the power of the pseudo-random key depends on the randomness factor. Hence following subsections discussed focuses on assessing the randomness of the key by performing various tests

### A. *Chi-Square Test*

We used a this test to trial the randomness factor of the generated key [20]. The mathematical formulation presented in equation (10) describes the procedure of performing the Chi-Square analysis on a random sample of size 'n.' with a set of 'k' class intervals

$$\chi_0^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \tag{10}$$

In equation 10, parameters $O_i$ is an observed frequency ith class interval and $E_i$ is expected frequency under the same interval. where $E_i$ is calculated as $np_i$. $p_i$ Is a probable theoretical value associated with the ith class interval. On substitution, if the calculated value is smaller than or identical to a standard value, then the randomness test is considered as pass. Table 1 depicts the experimental results of Chi-Square test samples conducted for the generated pseudo-random key values as presented in Fig. 7.

TABLE I. CHI-SQUARE TEST RESULTS UNDER VARIOUS SAMPLES

| Total Samples | Intervals | Calculated value | Standard value |
|---|---|---|---|
| 100 | 100 | 92.0 | 124.3 |
| 200 | 100 | 118.0 | 124.3 |
| 300 | 50 | 49.14 | 55.8 |
| 500 | 10 | 14.25 | 16.9 |

Results presented in table I proves that the generated key passes Chi-Square test for a reasonable length of samples with better interval numbers as the calculated values are less than the standard values.

### B. *Runs Up-down Test*

This test investigates the arrangement of numbers in a series to trial the hypothesis of independence. We have applied this test in our research work to find out the run count of a pseudo-random key sequence [21]. More striking the value of run count, higher is the difference in the value of the series, which strengthens the likeliness to be a random number [22]. Formulae presented in equation (11) and equation (12) describes the computation mean and the variance of the run test, respectively.

$$\mu_a = \frac{2N-1}{3} \tag{11}$$

$$\sigma^2 = \frac{16N-29}{90} \tag{12}$$

Where $\mu_a, \sigma^2$ is the mean and the variance of the sequence under a total number of runs $a$, N represents the number of samples. For larger values, $a$ follows a standard curve having the mean and the variance as shown in equation (13) and equation (14)

$$Z_0 = \frac{a - N_a}{\sigma_a} \tag{13}$$

$$\sigma_0 = \frac{a - \left(\frac{2N-1}{S}\right)}{\sqrt{\frac{(16N-29)}{90}}} \tag{14}$$

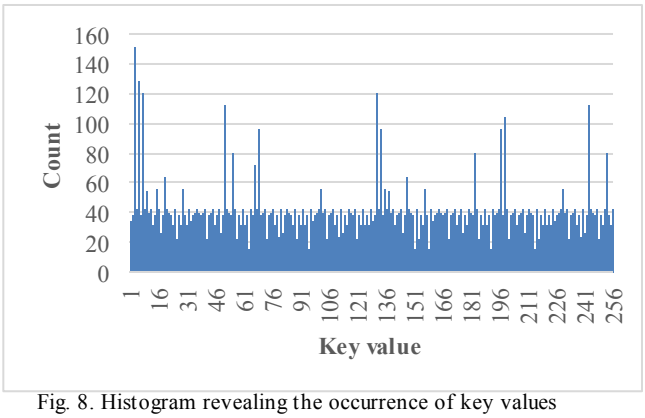



Fig. 8. Histogram revealing the occurrence of key values

We performed our runs up-down test on 10369 samples which fetched a run count of 6817 with $\mu_a$=6912 and $\sigma^2$=1843.055. Comparing this to a standard value of normal curves principals us to -2.2206 under 99% confidentiality in a two-tailed test. It specifies that the values engendered in the series are entirely random. The histogram corresponding to the test sample is presented in Fig. 8.

### C. Period of Subsequence

Under this section, we have computed the number of subsequences generated by the LFSR without repetition. The graph plotted in Fig. 9 presents the total non-repeating period of random subsequences for each of the series of 4 seed values fetched at a time. In the figure, we have represented 15 samples of the subsequences for the extracted 59 features.

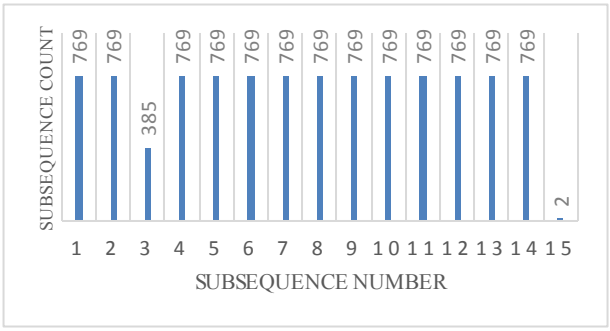
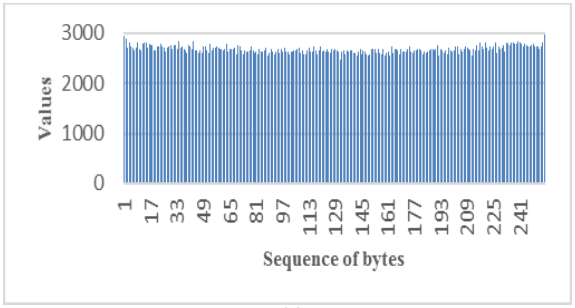



Fig. 9. Histogram representing the period of subsequence

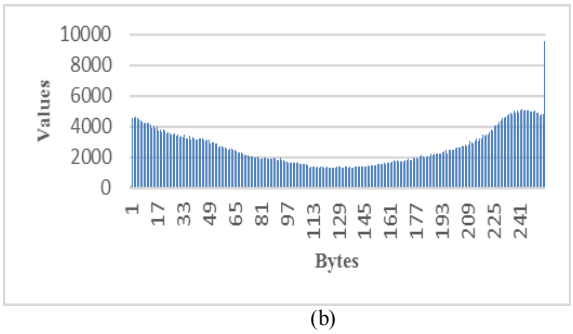
Graphical representation in Fig. 9 confirms the generation of an enormous random sequence value for the series of 4 seed values. Values of subsequent count achieved prove that most of the times, LFSR generated 769 random sequence values for each seed series of seed value without repetition, which is approximately 190 times the sequence of seed value. Hence it proves that LFSR is efficient in generating a robust pseudo-random key.

### D. Comparative Analysis of Encryption & Decryption

Fig. 10 presents the histograms of the encrypted audio and decrypted audio with the bytes of an audio file along the horizontal axis and their values along the vertical axis leaving out their header information. In Fig. 10a, we have achieved histogram for encrypted audio and Fig. 10b depicts the histogram of decrypted audio. Since the histogram in Fig. 10b has a potential difference in comparison with the histogram in Fig. 10a, it confirms that the proposed encryption technique is efficient and hard to break




(a)




(b)

Fig. 10. Histogram plot. (a) Encrypted audio and (b) Decrypted audio

## V. CONCLUSION AND FUTURE WORK

This research work has successfully implemented the process of encryption and decryption by using the pseudo-random key generation technique. It s also successful in achieving a novel procedure for pseudo-random key generation by using the features extracted from the facial image through SURF algorithm. Experimental results of the Chi-Square test and runs up-down test that confirms the strength of the key generated through LFSR in terms of the randomness factor. Graphical representation in Fig. 9 proves that the generated pseudo-random key has a higher value of non-repeating subsequence in most of the cases, which are several times larger than the fetched seed value into LFSR. From this, it is proved to generate a very long pseudo-random key sequence.

In future, the work can be enhanced to increase the strength of the random key by considering only the selected facial features to achieve more randomness. The current research has applied a single feature extraction technique that can be extended by using multiple feature extractors, which possibly strengthens the length and randomness of the generated key. The proposed system can also be carried forward to encrypt various other types of information, including stenographic applications.

## REFERENCES

[1] Saste, P., & Martis, J. (2016). Converged OAM. In *Proceedings of the second international conference on computer and communication technologies* (pp. 437-444). Springer, New Delhi.

[2] Upadhyaya, A., Shokeen, V., & Srivastava, G. (2015, September). Image encryption: using aes, feature extraction and random no. generation. In 2015 4th International Conference on Reliability,

Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-4). IEEE.

[3] Blum, L., Blum, M., & Shub, M. (1986). A simple unpredictable pseudo-random number generator. *SIAM Journal on computing*, *15*(2), 364-383.

[4] KB, S., & Aithal, G. (2020). Generation of pseudo random number sequence from discrete oscillating samples of equally spread objects and application for stream cipher system. *Concurrency and Computation: Practice and Experience*, *32*(1), e5181.

[5] Sannidhan, M. S., Prabhu, G. A., Robbins, D. E., & Shasky, C. (2019). Evaluating the performance of face sketch generation using generative adversarial networks. *Pattern Recognition Letters*, *128*, 452-458.

[6] Lawrence Fernandes, S., & Josemin Bala, G. (2014). Development and analysis of various state of the art techniques for face recognition under varying poses. *Recent Patents on Engineering*, *8*(2), 143-146.

[7] Fernandes, S. L., & Bala, G. J. (2016). Self-Similarity Descriptor and Local Descriptor-Based Composite Sketch Matching. In *Proceedings of Fifth International Conference on Soft Computing for Problem Solving* (pp. 643-649). Springer, Singapore.

[8] Sudeepa, K. B., Raju, K., Ranjan, K., & Ghanesh, A. (2016). A new approach for video steganography based on randomization and parallelization. *Procedia Computer Science*, *78*, 483-490.

[9] Sudeepa, K. B., & Aithal, G. (2017). Generation of maximum length non-binary key sequence and its application for stream cipher based on residue number system. *Journal of computational science*, *21*, 379-386.

[10] Sudeepa, K. B., Raju, K., Sannidhan, M. S., & Bhandary, A. (2016, October). Maximum period word oriented non-binary key sequence generation and its application in image encryption/decryption. In *2016 International Conference on Emerging Technological Trends (ICETT)* (pp. 1-6). IEEE.

[11] Kokila, R., Sannidhan, M. S., & Bhandary, A. (2017, March). A Study and Analysis of various Techniques to match Sketches to Mugshot Photos. In *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 41-44). IEEE.

[12] Kokila, R., Sannidhan, M. S., & Bhandary, A. (2017, September). A novel approach for matching composite sketches to mugshot photos using the fusion of SIFT and SURF feature descriptor. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1458-1464). IEEE.

[13] Sannidhan, M. S., & Chaitra, K. M. (2019, August). Assessment of Image Enhancement Procedures for Matching Sketches to Photos. In *2019 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)* (pp. 1-5). IEEE.

[14] Bay, H., Tuytelaars, T., & Van Gool, L. (2006, May). Surf: Speeded up robust features. In *European conference on computer vision* (pp. 404-417). Springer, Berlin, Heidelberg.

[15] Juan, L., & Gwon, L. (2007). A comparison of sift, pca-sift and surf. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *8*(3), 169-176.

[16] Pallavi, S., Sannidhan, M. S., Sudeepa, K. B., & Bhandary, A. (2018, September). A Novel Approach for Generating Composite Sketches from Mugshot Photographs. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 460-465). IEEE.

[17] Sudeepa, K. B., Aithal, G., Rajinikanth, V., & Satapathy, S. C. (2020). Genetic Algorithm Based Key Sequence Generation for Cipher System. *Pattern Recognition Letters*.

[18] Murali, P., & Senthilkumar, G. (2009, April). Modified version of playfair cipher using linear feedback shift register. In *2009 International Conference on Information Management and Engineering* (pp. 488-490). IEEE.

[19] Win, T. L., & Kyaw, N. C. (2008). Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR). *World Academy of Science, Engineering and Technology*, *48*, 463-467.

[20] Ryabko, B. Y., Stognienko, V. S., & Shokin, Y. I. (2004). A new test for randomness and its application to some cryptographic problems. *Journal of statistical planning and inference*, *123*(2), 365-376.

[21] Tootill, J. P. R., Robinson, W. D., & Adams, A. G. (1971). The runs up-and-down performance of Tausworthe pseudo-random number generators. *Journal of the ACM (JACM)*, *18*(3), 381-399.

[22] Wichmann, B. A., & Hill, I. D. (1982). Algorithm AS 183: An efficient and portable pseudo-random number generator. *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, *31*(2), 188-190.