I.J. Image, Graphics and Signal Processing, **2015, 4, 28-34**
Published Online March 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.04.03

A Dynamic Security Protocol for Face Recognition Systems Using Seismic Waves

Sheela Shankar
Department of Electronics & Communication Engg, KLE Dr. M. S. Sheshgiri CET, Udyambag, Belgaum-590008, Karnataka, India
E-mail: kle.ec.sheelakore@gmail.com

V.R Udupi
Department of Electronics & Communication Engg, Gogte Institute of Technology, Belgaum-590008, Karnataka, India
E-mail: vishwa_u@yahoo.com

Abstract—Face recognition system is one of the robust means of authentication. It involves comparing the faces of an individual against a set of images in the training database. Thus the security issues pertaining to the training database is very critical. This paper aims at providing security to the images in the training database by empowering the encryption algorithms using a secure Random Number Generator (RNG). To facilitate this, the seismic waves are used as seeds to drive the Pseudo-Random Number Generators (PRNGs). The efficiency of seismic waves as a True Random Number Generator (TRNG) was evaluated using two statistical suites. Also, the proposed TRNG is compared against other existing RNGs. It was found that the degree of randomness rendered by the proposed system was in good agreement like the other existing generators. The proposed system was found to be cost-effective, portable and easy to maintain.

Index Terms—Face Recognition, Pseudo-Random Number Generator, Seismic waves, True Random Number Generator.

I. Introduction

Face recognition systems are one of the powerful means of authentication when compared to the other existing authentication techniques [1, 2]. It is basically a biometric based authentication system. The main challenge encountered in this is the security of the faces stored in the training database. Though there are many well known encryption algorithms available, the generation of secure keys is the most challenging issue. This phase is very crucial and the proper generation of highly unpredictable keys is very vital. Hence the usage of RNGs is encouraged here.

The generation of keys is generally achieved using RNGs. In scientific terminology, a RNG is one, that produces infinite sequences of perfect independent and identically distributed (iid) symbols, which can be viewed as a finite probabilistic state machine where the generation of a bit is independent of its ancestor bits, nor the number of bits generated determine the current bit [3]. The applications of random numbers have augmented radically with time, especially in areas of complex financial and scientific model simulations, gambling and lotteries, security related applications [4, 5], mathematical equation solving, piracy detection in integrated circuits [6], graphics and animations, etc. RNGs fall in two categories with respect to its architecture, properties and qualities of implementation, etc. They are PRNGs and TRNGs. PRNGs are mathematical algorithms that get initiated with an externally supplied seed and bequeath long and asymmetrical random- like series. They provide excellent results in terms of distribution if its design schema is complex [7]. As per the celebrated saying of John von Neumann (1951), "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin", this is true because, their periodicity and repeatability have curtailed their applications where security is of paramount importance. The seed selected is the only factor on which the entire randomness is based. This urges the need to rely on TRNGs.

TRNGs on the other hand, are hardware to generate random numbers. TRNGs can be designed to work using atmospheric noise, radioactive decay, bio-signals, etc. Persaud [8] had concluded that humans can consciously generate random number sequences. But the same experimentation procured drastic results which violated the hypothesis rendered by Persuad [9]. Studies reveal that subjects with mental disorders have prejudicial ability to generate random numbers [10, 11, 12].This should not result in drawing conclusions which adhere that healthy humans are good sources of random numbers. Biometric signals acquired from human galvanic skin responses and an animal neurophysiologic brain response has been used exclusively in this regard [13]. Telegraph noises of a contact-resistive RAM can also be used to implement a TRNG as in [14]. TRNGs are inefficient when compared to PRNGs in terms of producing streams of uniform distribution. Also they consume lots of time in generating longer sequences and their cost of maintenance is high. They are even not portable. But they are popular because of the unpredictable nature of their output.

These issues urge a need for a RNG, which can overcome the defects of both the generators. The only source of availing true randomness is from natural signals. This does not mean that all natural signals are random. Proper selection of signals is very important in this case. Hence, seismic waves were used and were tested for randomness using standard statistical tests like the Runs test and the Correlation test. The study overcomes the drawbacks of both the types of generators by amalgamating the advantages of both the generators. Seismic waves, which are the results of energy that travels under the earth's layers [15], are used as a random seed generator and this in turn is used to drive the PRNGs. The amplitude values of seismic waveforms were taken in time domain for the experimentation.

The rest of the paper is organized as follows. Section II briefs face recognition. The implementation details are briefed in Section III. The hardware and software details are also discussed here. Section IV deals with the results and discussions of the experimentation carried out. The conclusion and future scope of the study are given in Section V and VI respectively.

II. Face recognition

Face recognition is a non-intrusive form of identifying a given image of face and comparing it against a set of faces present in the database, in order to uniquely identify a person [16]. The system is currently gaining wide acceptance in spite of the major hurdles posed by variations in facial images due to age, illumination, pose, facial hair, cosmetics, facial expressions, etc. The reason for its success can be attributed to its advantages over other biometric based authentication methodologies, which are as follows: 1) Accumulation of germs and impurities on the sensor devices is a common scenario in most of the existing biometric based techniques. However, face recognition is devoid of this shortcoming since the camera is placed at a distance and hence is not in contact of the user. 2) The devices used in face recognition systems are cheaper when compared to the sensor devices used in other biometric techniques.

The basic components involved in a typical face recognition system are as shown in Fig. 2. Firstly the face images are preprocessed for extracting features accurately and then they are stored as a particular template in the database. After this, the face images under test undergo the same sequences except for getting stored in the database. Instead, they are checked for similar images in the database. Popular algorithms like Principal Component Analysis [17], Linear Discriminant Analysis, Support Vector Machines [18, 19], etc. have helped considerably in making face recognition an attainable process.

A. Details of the face database used

Face images used for the study were taken from the AR face database. This dataset was created in the year 1988 in the Computer Vision Center (CVC) at the U.A.B. by Aleix Martinez and Robert Benavente. It was the first face database to include occlusion. The database provides provisions for variation in frontal poses, eye glasses, illumination, expressions, scarves, etc. [20]. In a 2-week interval, the subject’s face images were captured twice by subjecting them to 13 different conditions. Fig.1. shows samples taken from the AR Face Database.

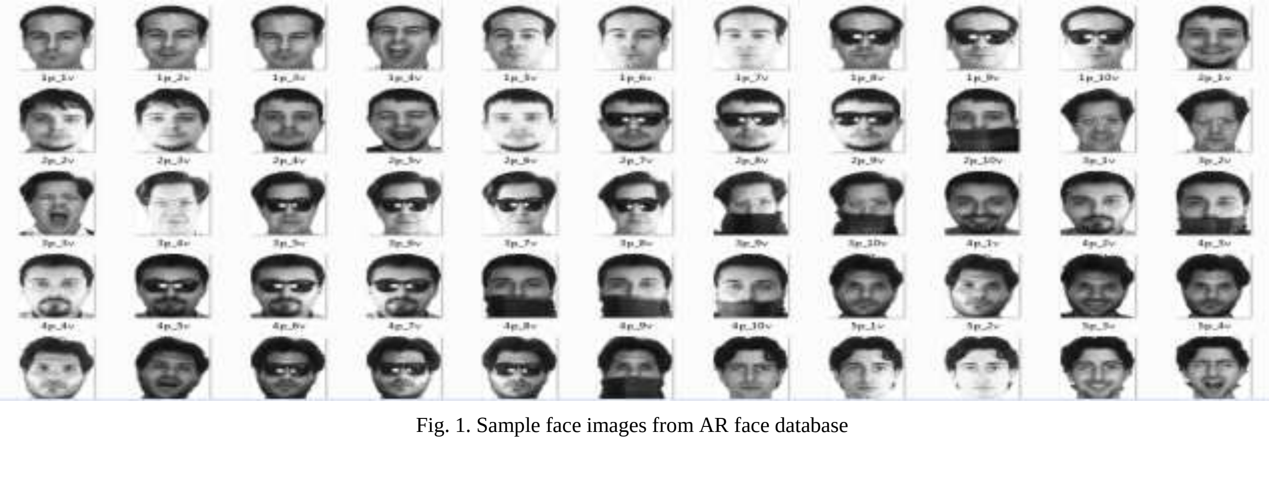

Fig. 1. Sample face images from AR face database

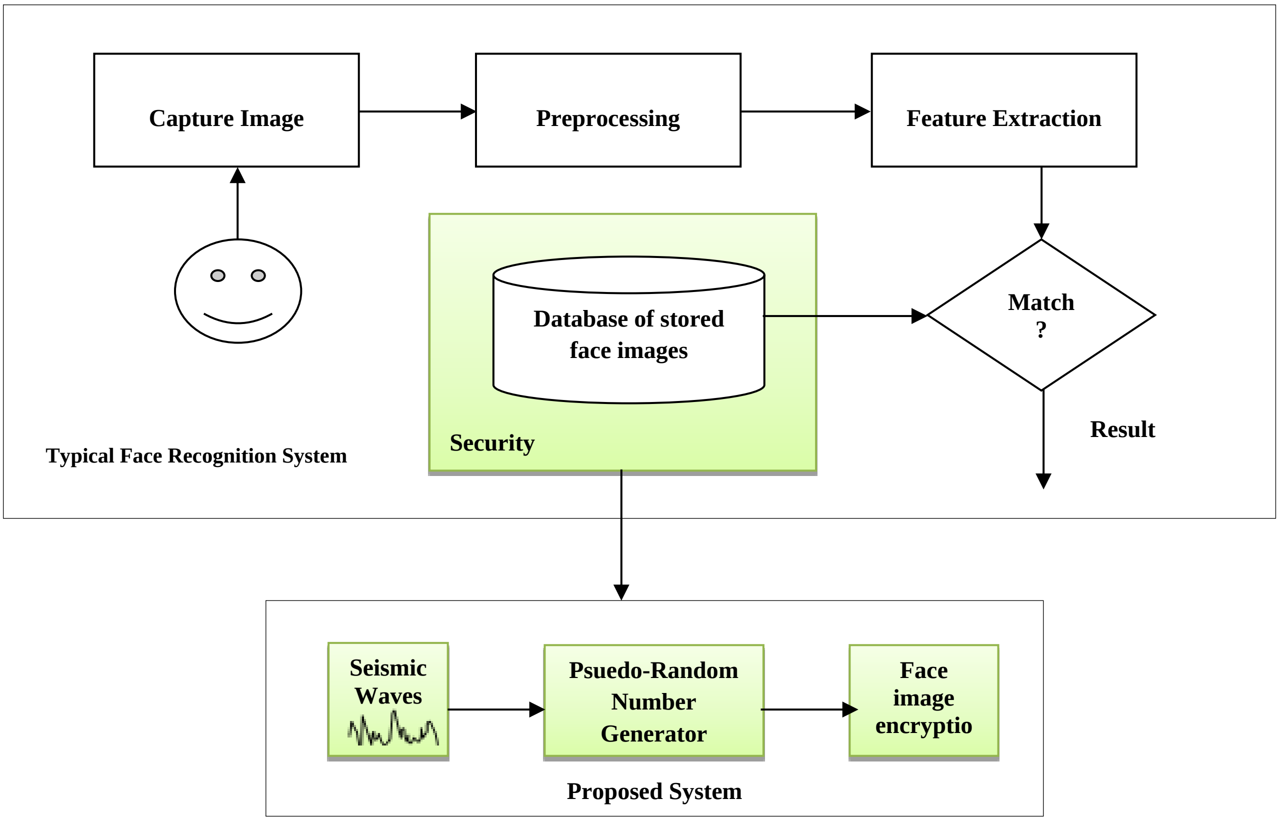

Fig. 2. Typical face recognition system along with the proposed system

III. Implementation

The proposed system is an addition to the existing face recognition systems. Fig. 2 shows the block diagram of the face recognition system along with the proposed system. The proposed system is built over the database containing the face images in the existing systems. The design of the proposed system consists of two main divisions. The first being the assessment of seismic signals and the next part dealt with the encryption methodology of the faces in the training database. Apart from this, the study initially tested the seismic waves for randomness using the Runs test and the Correlation test. The details of the results returned by these two tests are given in the results and discussion section.

A. Hardware and Software details

A.1 Hardware used

The Seismo-meter used here is Geode Ultra-Light Exploration Seismograph (Fig. 3). It consists of ultra-portable 3 to 24 channel seismic recorders that attaches to the laptop. There is provision to connect several Geodes together to build systems up to 1000 channels. The Geode is suitable for reflection, refraction, downhole, VSP and monitoring applications.

Fig. 3. Geode Ultra-Light Exploration Seismograph

A.2 Software used

Windows Visual C 2010 IDE was used for compiling the source code, parse the seismic waves acquired using seismograph and to make the executable file which can then be directly executed. MYSQL database was used to store the random numbers generated using PRNG. Matlab was used for face image encryption.

B. PRNG used

The PRNG used is the Linear Congruential Generator (LCG) due to their rapidness and least memory requirement (around 32 to 64 bits) to maintain a particular state. It was developed by Lehmer in 1951 and since then, it is the most widely used algorithm in random number generation. It produces random streams between zero and *m-1* using the following recursive relationship:

$$X_{i+1} = (a\,X_i + c\,)\ mod\ m, \quad i = 0,1,2,... \qquad (1)$$

where X_0 is the initial number called seed, *a* is the multiplier, *c* is the increment and *m* is the modulus. The period is *m* and it can get lesser for some values of *a*. To have a maximum period for all the seeds, the following criterion should be met:

1) *a-1* is divisible by all prime factors of *m*.
2) *c* and *m* are relatively prime.
3) *a-1* is a multiple of 4 if *m* is a multiple of 4.
The values for *m, a* and *c* for various compilers is as shown in Table 1:

Table 1. Values for m, a and c for various compilers.

Source	m	a	c
Microsoft Visual/Quick C/C++	2^{32}	214013	2531011
Java's java.util.Random	2^{48}	25214903917	11
Borland C/C++	2^{32}	22695477	1
Microsoft Visual Basic (6 and earlier)	2^{24}	1140671485	12820163

The proposed implementation uses the standards adopted by Microsoft Visual/Quick C/C++.

C. Design schema

The entire system design can be observed from Fig. 2. The seismograph was used to read the seismic waves. This was read in digital format and the numbers were used as seeds to drive a PRNG. The implementation of the PRNG was done using C++ program. The generated random numbers were stored in the database and a direct communication link was set up to the application program to use these numbers. These numbers were used as keys to encrypt the face images.

A simple encryption algorithm is run by using the seismic-signals as seeds to the LCG algorithm. Any other encryption algorithms can be considered by making use of the random numbers generated. The algorithm used in this regard is given in Section III.C.1.

C.1 Algorithm

Algorithm: Face image encryption using seismic-signals.
Input: Seismic signals and the data to be encrypted.
Output: Encrypted data and decrypted data.

Procedure:

```
1. Setup the seismograph device connectivity.
2. Read amplitude values of the waveform.
3. Use these amplitude values as seeds to the LCG.
4. Generate the desired number of random numbers.
5. For i=0 to sizeof(face image)
           Subtract each random number from each numerical value of the image.
       Output it as encrypted data.
6. For i=0 to sizeof(face image)
           Add each random number to each numerical value of the image.
       Output it as decrypted data.
```

IV. Results and discussions

A. Comparison of RNGs

Four RNGs were used for comparison, among which one was a PRNG and the rest were TRNGs. Quantum RNG [21, 22], RNG using Atmospheric Noise [23] and Seismic waves are the TRNGs while the Excel rand function was the PRNG used for the comparison. They were subjected to two tests, the Runs test and the Correlation test. For the testing purpose, numbers were generated from 4 different sources for 7 times. In every iteration, 100 numbers were extracted. The details of the two tests are as given below:

A.1 Runs Test

Runs test is used to determine randomness. Procedures for evaluating randomness are mainly based upon the nature and number of runs present in the data under investigation. A run is a sequence of like events, symbols or items that has been followed and preceded by an event, symbol or item of a different type, or by none at all. Randomness is doubted when there are too many or too few runs.

The underlying hypothesis in the runs test is as follows: Let,

H_0: The observations in the sample are random.
H_1: The observations in the sample are not random.
The procedure requires calculating the values for the following variables:
n=Total sample size.
n_0=Number of sample members of one type (number of samples below mean).
n_1=Number of sample members of another type (number of samples above mean).
Calculate n, where

$$n=n_0+n_1 \qquad (2)$$

Reject H_0, if R < = lower critical values (few runs) or if R > = upper critical values (many runs). If both n_0 and n_1 are < = 20, then the small sample runs test is appropriate, else large sample runs test is to be carried out. The steps for carrying out the runs test are as follows:

1) Small Sample Runs test:

```
1. Let $\alpha = 0.05$
2. Calculate R.
3. If $n_0$-1 < R < $n_1$-1
       Do not reject the null hypothesis, $H_0$.
   Else
       Reject $H_0$.
```

2) Large Sample Runs test:

1. If n_0 or n_1 is greater than 20, then calculate the

following:

$$\text{Mean} = \frac{2\times n0\times n1}{n+1} \quad (3)$$

$$\text{Variance}=\frac{2\times n0\times n1\times(2\times n0\times n1-n)}{(n-1)\times n^2} \quad (4)$$

$$\text{Standard Deviation}=\sqrt{\text{Variance}} \quad (5)$$

$$Z=\frac{R-Mean}{Standard\ deviation} \quad (6)$$

2. If -1.96<=Z<=1.96

    Do not reject H_0

  Else

    Reject H_0.

A.2 Correlation Test

This test is used to test the dependency among the datasets. It is a method for evaluating the extent of linear relationship that exists between two quantities under test. It was formulated by Karl Pearson in 1895. The term correlation coefficient signifies the measure of linear association between the two numbers. The results of this test can range between +1 to -1. A result of +1 signifies perfect positive correlation whereas -1 specifies perfect negative correlation. The test was conducted in Microsoft Excel using the *correl()* API. The closer the result is to +1 or -1, the stronger is the relationship between the two series.

This test is used exclusively in statistical analysis, pattern recognition and image processing.

Fig. 4 shows the graph of the total number of Runs obtained by running the Runs test. The numbering of the data on the X-axis corresponds to the type of RNG used. It is in the following order: 1) Quantum RNG. 2) RNG using Atmospheric Noise. 3) Excel rand function (PRNG). 4) Seismic waves. The numbering sequence for the RNGs is same for the Fig. 5 and 6. Each bar on the X axis represents the iteration of the data acquisition. Y axis on Fig.4 represents the total number of runs. As per the runs test, for a sequence to be random, the total number of runs should not be too high or too low when compared to the total number of numbers under test. This is evident from the results obtained.

Fig. 5 represents the value of Z for the data samples. The numbering of the data on the X-axis corresponds to the type of RNG used. Each bar on the X axis represents the iteration of the data acquisition. Y axis corresponds to the value of Z. For a good RNG, the value of Z is anticipated to lie in the range of -1.96 and +1.96, which is evident in most of the cases in the obtained results.

Fig. 6 represents the value of the Correlation Coefficients for the data streams. The numbering of the data on the X-axis corresponds to the type of RNG used. Each bar on the X axis represents the iteration of the data acquisition. Y axis corresponds to the value of the Correlation Coefficient. It can be observed from Fig. 6 that the data samples are independent. The data from the PRNG is in good agreement with this test when compared to the TRNGs. However, this benefit is at the cost of security. Hence the proposed system combines the TRNG with PRNG, thereby eliminating the drawbacks of both the generators.

From all these results, it can be seen that the randomness of seismic waves is similar to the randomness rendered by other existing RNGs. Hence the amplitude values of seismic waves were fed to a PRNG to get a large set of numbers in a short span of time which are uniformly distributed.

Fig. 7 shows the original face image, the encrypted face image and the decrypted face image taken from the AR Face Database. The image encryption was done using the algorithm mentioned in Section III.C.1.

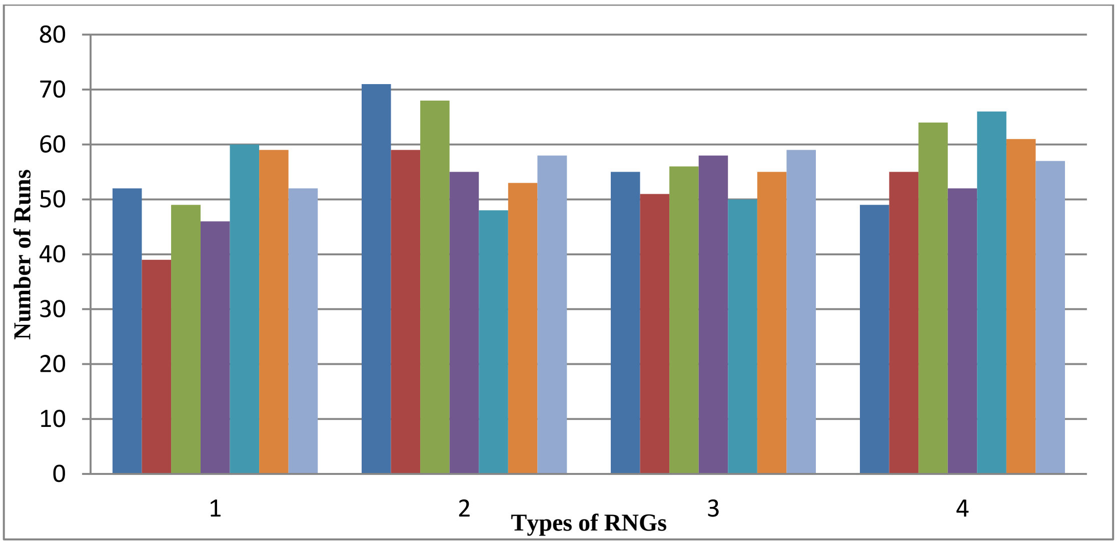

Fig. 4. Number of Runs for the datasets of 4 different RNGs.

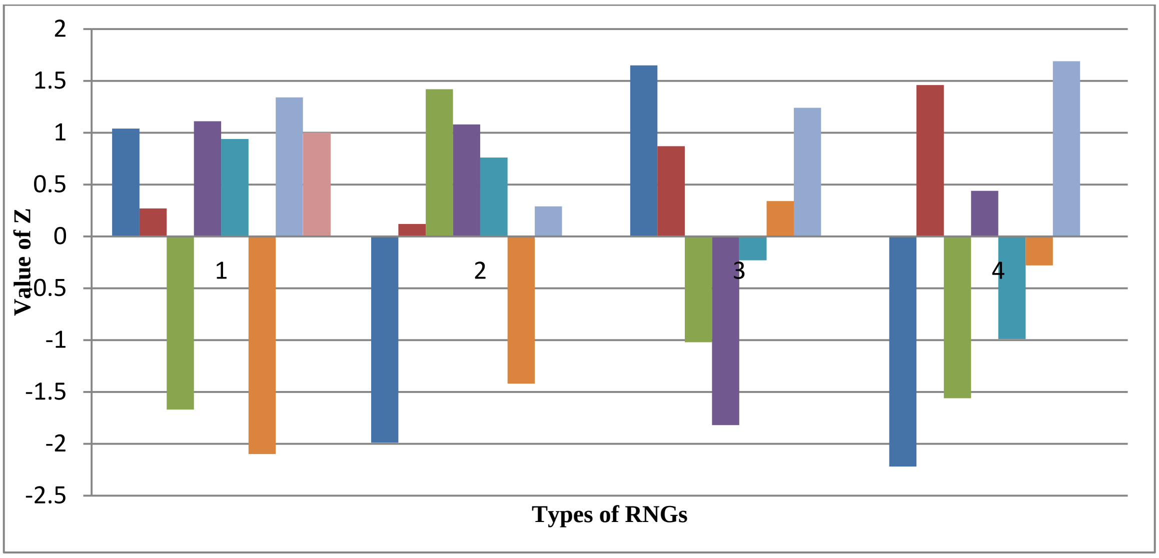

Fig. 5. Values of Z in the runs test for the datasets of 4 different types of RNGs.

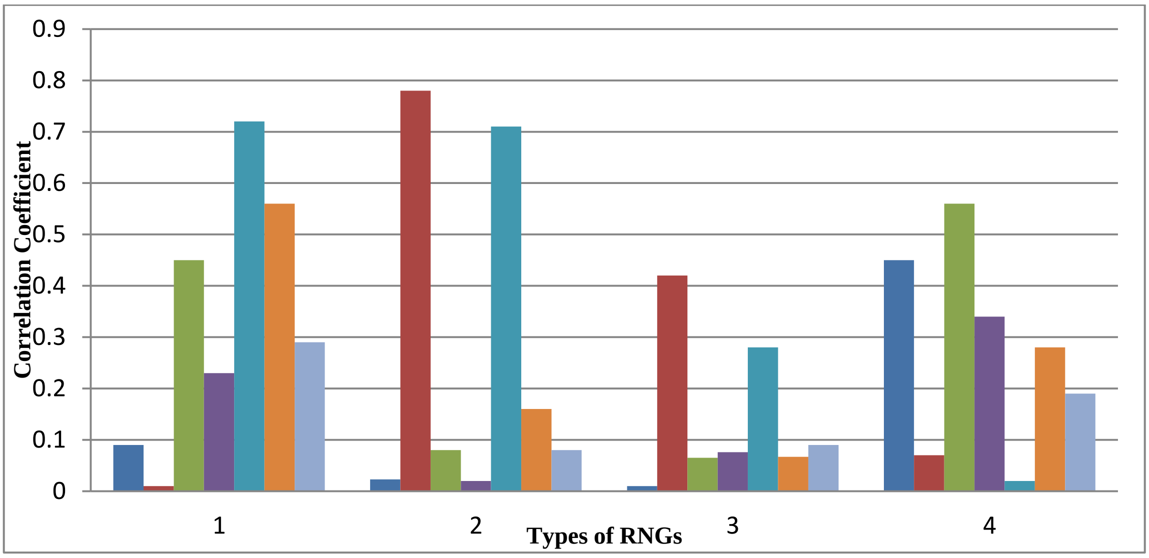

Fig. 6. Correlation Coefficient values for the datasets of 4 different RNGs.

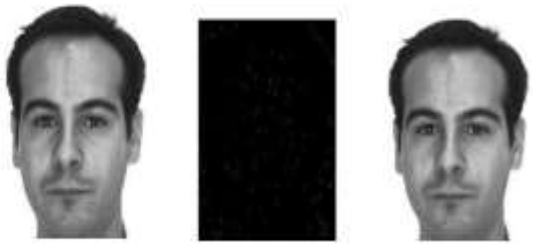

Fig. 7. Original Face image (to the left), encrypted image (to the centre) and decrypted image (to the right).

V. Conclusion

The study dealt with assessing the seismic signals to be used as seeds to drive the PRNG. This in turn was used as keys to encrypt the face images in the training database of the face recognition system. To prove the robustness of the security rendered, the seismic signals were tested for randomness using the Runs test and the Correlation test. The signals were also tested against three other existing RNGs and it was found that it is similar in functionality when compared to the rest, and hence can be used like other existing RNGs. A sample face image was encrypted using the generated random numbers as keys to an encryption algorithm. The proposed methodology of generating random streams using seismic waves is easy and feasible to use as it makes use of portable, cost-effective devices when compared to the other TRNGs.

VI. Future Scope

The underlying hypothesis of availing the random streams from seismic-signals can ensure a robust level of security to real time applications. Rigorous research can be carried out to study the complexity of the layers of the earth, which culminates in the generation of random impulses in the form of seismic waves. This could then be used to deploy efficient systems which run using random numbers.

ACKNOWLEDGEMENTS

The authors are immensely grateful to the valuable suggestions and help provided by the Department of Electronics and Communication Engineering, KLE Dr. M. S. Sheshgiri College of Engineering and Technology, Udyambag, Belgaum, Karnataka, India.

REFERENCES

[1] Eleyan, Alaa. "Enhanced Face Recognition using Data Fusion." International Journal of Intelligent Systems and Applications (IJISA) 5.1 (2012): 98. DOI: 10.5815/ijisa.2013.01.10.

[2] Gurumurthy, Sasikumar, and B. K. Tripathy. "Design and Implementation of Face Recognition System in Matlab Using the Features of Lips." International Journal of Intelligent Systems and Applications (IJISA) 4.8 (2012): 30. DOI: 10.5815/ijisa.2012.08.04.

[3] Fabio Pareschi, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 57, NO. 12, DECEMBER 2010. DOI: 10.1109/TCSI.2010.2052515.

[4] J. Daemen and V. Rijmen, "The Design of Rijndael: AES—The Advanced Encryption Standard", New York: Springer-Verlag, 2002.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone," Handbook of Applied Cryptography", Boca Raton, FL: CRC, 1996.

[6] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending piracy of integrated circuits", in Proc. IEEE Des. Autom. Test Eur. (DATE), 2008, pp. 1069–1074.

[7] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM J. Comput., vol. 15, pp. 364–383, May 1986.

[8] Persaud N., "Humans can consciously generate random number sequences: a possible test for artificial intelligence", Med Hypotheses 2005;65:211–4.

[9] Małgorzata Figurska, Maciej Stan´czyk , Kamil Kulesza, "Humans cannot consciously generate random numbers sequences: Polemic study", Medical Hypotheses (2008) 70, 182–185, Elsevier. DOI: 10.1016/j.mehy.2007.06.038.

[10] Brown RG, Soliveri P, Jahanshahi M., "Executive processes in Parkinson's disease – random number generation and response suppression", Neuropsychologia 1998; 36(12):1355–62.

[11] Brugger P, Monsch AU, Salmon DP, Butters N., "Random number generation in dementia of the Alzheimer type: a test of frontal executive functions",Neuropsychologia 1995; 34(2):97–103.

[12] Pollux PMJ, Wester A, Haan EHF., "Random generation deficit in alcoholic Korsakoff patients", Neuropsychologia 1995;33:125–9.

[13] J. Szczepanski), E. Wajnryb, J.M. Amigo, Maria V. Sanchez-Vives, M. Slater, "Biometric random number generators", Computers & Security (2004) 23, 77e84, Elsevier. DOI: 10.1016/S0167-4048(04)00064-1.

[14] Chien-Yuan Huang, et.al, "A Contact-Resistive Random-Access-Memory-Based True Random Number Generator", IEEE ELECTRON DEVICE LETTERS, VOL. 33, NO. 8, AUGUST 2012.

[15] Ben-Menahem, Ari, and SarvaJit Singh. Seismic waves and sources. Courier Dover Publications, 2012.

[16] RabiaJafri, Hamid R. Arabnia, "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol.5, No.2, June 2009. DOI : 10.3745/JIPS.2009.5.2.041.

[17] Ali Javed, "Face Recognition Based on Principal Component Analysis, I.J. Image, Graphics and Signal Processing (IJIGSP), 2013, 2, 38-44. DOI: 10.5815/ijigsp.2013.02.06.

[18] Alireza Tofighi, Nima Khairdoost, S. Amirhassan Monadjemi, Kamal Jamshidi, "A Robust Face Recognition System in Image and Video", I.J. Image, Graphics and Signal Processing (IJIGSP), Vol. 6, No.8, July 2014, pp.1-11. DOI: 10.5815/ijigsp.2014.08.01

[19] P.S. Hiremath, Manjunatha Hiremath, "3D Face Recognition based on Radon Transform, PCA, LDA using KNN and SVM", I.J. Image, Graphics and Signal Processing (IJIGSP), Vol. 6, No. 7, June 2014, pp. 36-43. DOI: 10.5815/ijigsp.2014.07.05.

[20] Available at: http://www2.ece.ohio-state.edu/~aleix/ARdatabase.html.

[21] Stipcevic, Mario. "Quantum random number generators and their use in cryptography." MIPRO, 2011 Proceedings of the 34th International Convention.IEEE, 2011.

[22] Jennewein, Thomas, et al. "A fast and compact quantum random number generator." Review of Scientific Instruments 71.4 (2000): 1675-1680.

[23] Available at: http://www.random.org.

Author's Profile

Prof. Sheela Shankar has completed her Bachelor of Engineering in Electronics and Communication from BIET, Davangere, Karnataka, India. She has pursued her Masters in Electronics and Control Engineering from Birla Institute of Technology and Science, Pilani. Currently she is working as an associate professor in the department of Electronics and Communication Engineering, KLE Dr.M.S.Sheshgiri College of Engineering and Technology, Belgaum, Karnataka, India. She is a life member of ISTE. Her areas of research includes image processing, communication engineering and control engineering.

Dr. V. R. Udupi did his bachelor's degree in Electronics and communication Engg. from Mysore University in 1984 and pursued his master's degree in Electronics Engineering with computer applications as specialization from Shivaji University, Kolhapur, Maharashtra, India in 1989. He has completed his doctoral degree in Electrical Engineering from Shivaji University, Kolhapur, Maharashtra state, in 2003. His field of interests includes signal processing, Image processing, cryptography, and knowledge based systems. Currently he is working as a professor in Electronic and communication department of Gogte Institute of Technology, Belgaum, Karnataka state. He has 30 years of total teaching experience and currently he is guiding 05 research scholars and has guided 04 candidates for Ph.D. He has published more than 42 technical papers in national and international conferences and 08 articles in journals. He is a life member of ISOI, SSI, CSI, BMESI, and ISTE.