Authentic Patient Data and Optimization Process Through Cryptographic Image or sound as Key Using Genetic Algorithm and Particle Swarm Optimization (PSO) in Body Area Network

Pradeep Kumar
Ph.D. Student, Enrollment Number: 120481
Mody University of Science and Technology, Lakshmangarh, Sikar-332311, Rajasthan, India

Abstract: ***Wireless Body area network can be secured by both genetic algorithm and particle swarm optimization algorithm both. Although, IoT-based patient health status monitoring has become very popular, monitoring patients remotely outside of hospital settings requires augmenting the capabilities of IoT with other resources for health data storage and processing. In this paper, we propose an IoT-based authentication and optimization process through image key management using a genetic algorithm in body area network. Recent advances in wireless communications technologies for medical/fitness applications***

Keywords: Body area network, genetic algorithm, particle swarm optimization

---

II. **Image Processing: [1]** Mathematically, an image can be considered as a function of 2 variables, *f(x, y)*, where *x* and *y* are spatial coordinates and the value of the function at given pair of coordinates *(x, y)* is called the *intensity value*. The programming counterpart of such a function could be a one or two-dimensional array. Code Snippet 1 and Code Snippet 2 show how to traverse and use 1-D and 2-D arrays programmatically. Both of them essentially can represent an image as shown in
Figure 1.

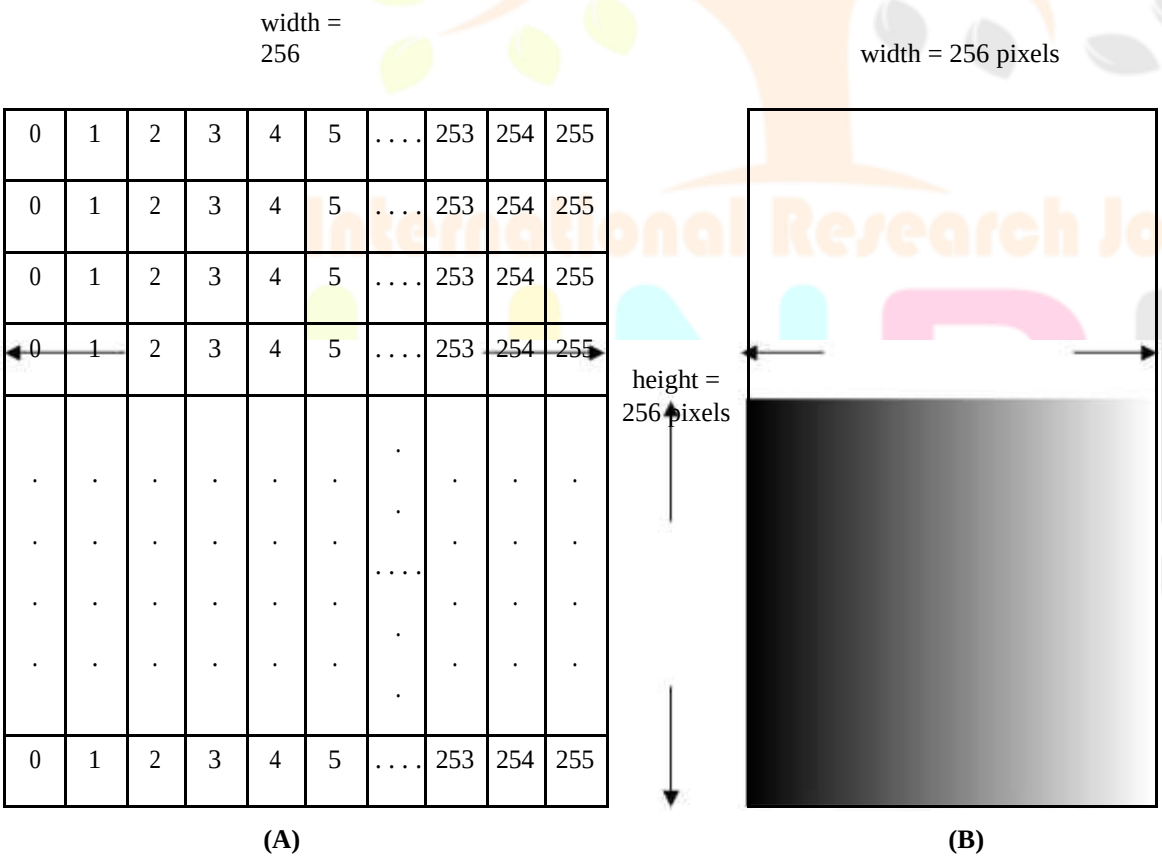

Figure: Values in the grid represent the grayscale intensities of the image on the right.

(A) Intensity values are shown in a grid of the same dimension as image **(B)** Image as seen on a monitor

A. Following code declares a 1-D array of type 'unsigned byte' having

B. size 256*256. It then puts values from 0 through 255 in each row.

```
int width, height;                          // width        and height of image
int offset;                                 // num of elements traversed in array
int value;                                  // image intensity value
width = height = 256;
value = offset = 0;

unsigned byte array_1D[height * width];

for(int j=0; j<height; j++)                 // traverse height (or rows)
{
        offset = width * j;                 // modify offset traveled
        for(int i=0; i<width; i++)          // traverse width (or columns)
        {
                array_1D[offset + i] = value++;          // update value at
                                                         // current index  i.e.
                                                         // (offset+i)
        }
        value = 0;
}
```

// Following code declares a 2-D array of type 'unsigned byte' having

// size 256*256. It then puts values from 0 through 255 in each row.

```
int width, height;                          // width and height of image
int value;                                  // image intensity value
width = height = 256;
value = 0;

unsigned byte array_2D[height][width];

for(int j=0; j<height; j++)                 // traverse height (or rows)
{
        for(int i=0; i<width; i++)                  // traverse width (or columns)
        {
                array_2D[j][i] = value++;           // update value at
                                                    // current  (i, j)
        }
        value = 0;

}
```

Code Snippet 2

The 'for' loop in Code Snippet 1 and 2 can be visualized as shown in Figure 2.

Y = 0	0	1	2	3	4	5	. . . .	253	254	255
Y = 1	0	1	2	3	4	5	. . . .	253	254	255
Y = 2	0	1	2	3	4	5	. . . .	253	254	255
Y = 3	0	1	2	3	4		. . . .			
	.	.	.	.	.	.	.	.	.	.

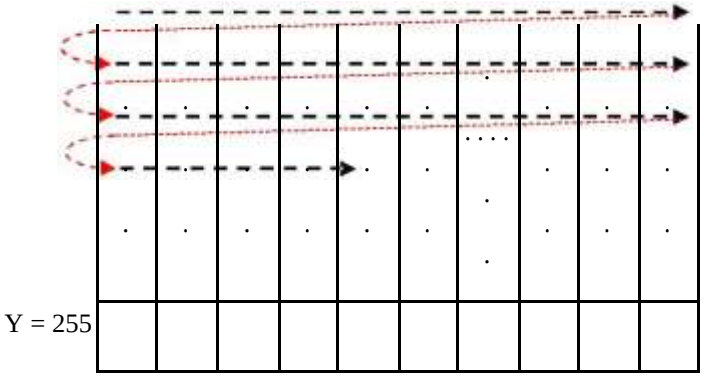

Figure: Array traversal in a 'for' loop. Note that rows are being accessed one after the other. This is known as '*Row Major Traversal*'. The graphic suggests that in the current iteration, x = 4 and y = 3 both starting from 0.

Security optimization through key management using a PSO in body area network: Particle Swarm Optimization (PSO) is a stochastic, population based, relatively recent heuristic search method. It is based on swarm intelligence. PSO optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. Before performing the actual classification, an aggregation process is needed to reduce the amount of extra data which got generated while trying security keys from various images. Aggregated data is stored to a DataMart, and the data in the DataMart is divided into a raw data set and test data set. The raw data set is use for making rules and the test data set is used for evaluating the accuracy of the rules.

- Particle Swarm Optimization Classification Algorithm pseudo code:

Input: raw data
repetition number (generate initial particles (=threshold rule) randomly)
for repetition number do {for each particle do {
Calculate the fitness value using raw data for finding the pbest; end for;
find the gbest;
for each particle do {compute velocity and update particle; end for}
end for}
output: rule same as gbest

IV. **Security optimization through key management using a genetic algorithm in body area network:**

A genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic [2] algorithms contain selection, crossover, and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

C. Selection It is quantitative criterion based on fitness value to choose the chromosomes from *a* population which is going to reproduce.

D. Crossover

In crossover operation, two chromosomes are taken and a new is generated by taking some attributes of the first chromosome and the rest from the second chromosome. [2]

For example, the strings 11001111 to 01101110 could be crossed over after the third locus in each to produce the two offspring 11001110 to 01101111.

Mutation

Mutation is used to maintain genetic diversity from one generation of the population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome. For example, the string 01000100 might be mutated in its second position to yield 00000100.

IV. PROPOSED METHODOLOGY

In the proposed method GA will be used in the key generation process. The crossover and mutation operation is used along with Pseudo-random number generators to make the key very complex. A number of rows in the array can be a population for crossover and mutation purposes. For encryption, we have proposed AES. The symmetric key algorithm is proposed due to its computation speed and less overhead in key management. The process of generating the key from the Genetic Population has the following steps:

STEP 1: From various images of various intensities and from various sound signal we can classify images and sound signals which are suitable for key size in body area network which require low powered arrangements. Images with low intensities can be separated through classification and be given for next step for cryptographic purpose.

STEP 2: A pseudo-random binary sequence is generated with the help of a small image like part of the image of ECG sensor image. Means any image can be used as a cryptographic security key. Another key like sound frequency of patient can be used for a cryptographic key for algorithm

or material of a mixture of various metal touches to the sensor can be used for cryptographic security key just like biometric way. As Mathematically, an image can be considered as a function of 2 variables, f(x, y), where x and y are spatial coordinates and the value of the function at given pair of coordinates (x, y) is called the intensity value. The programming counterpart of such a function could be a one or two-dimensional array. The first row of this two-dimensional array can be used as key generated from the same image used for the cryptographic purpose. For more criticality, a random number can be generated to choose the row from the array because the first-row idea can be hacked. But in GA for population limits can be decided for population and for a number of digits through fitness function from rows of the array from image processing. Two images can be used for intermixing of arrays to increase the population at sending and receiving end for heterogenous environment.

STEP 3: Fitness function like converting first row bit into a decimal number and the new decimal number generated by this process can be divided by hundred or more as per optimality factor after experimentation to reduce the bit size to convert this number back into binary and can be used as the population of cryptographic keys. For other fitness function, further new expression can be used as per requirement of key size.

STEP 4: The generated string or population is divided into two halves.

STEP 5: On the selected string crossover operation is performed to achieve good randomness among the key.

STEP 6: After crossover operation, the bits of the string are swapped again to permute the bit values.

STEP 7: The same process is iterated two times.

Here the crossover and mutation are done two times to create more complexity and randomness in the key. This key will be then used for the encryption process. Here AES will be used for encryption as it is one of the most efficient symmetric key algorithms and its whole security lies in the key used.

V. CONCLUSION

The BAN is an emerging technology that will alter people's everyday experiences revolutionarily. Privacy and data security in BANs is a significant area, and still, there is a number of challenges which need to be overcome. Image processing can create an image as a data for cryptographic purposes. So, there is no limit to a number of images and so as to the number of keys. Mathematical function on keys can help us to more growth in this field. Particle swarm optimization can be used for classification among images, which can be used for security key in body area networks.

VI. Reference:

[1] Copyright © 2005-2007, Advanced Digital Imaging Solutions Laboratory (ADISL). http://www.adislindia.com

[2] Aarti Soni, Suyash Agrawal," Using Genetic Algorithm for Symmetric key Generation in Image Encryption", ISSN: 2278 – 1323, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 10, December 2012

[3] Pradeep Kumar," Right Patient Data and Optimization Process Through CryptographicImage as Key Using Genetic Algorithm in Body Area Network", ISSN (Online): 2347 – 4718, International Journal for Technological Research In Engineering Volume 5, Issue 9, May- 2018