Security for Biometric Samples Using Nelder-Mead

Mrs. Poonam Talele
Department of Computer Engineering
Yadavrao tasgaokar college of engineering (YTCEM)
Bhivpuri, Karjat, India
poonamjtalele@gmail.com

Prof. Vanita Mane
Department of Computer Engineering
Ramrao Adhik Institute of Engineering (RAIT)
Nerul, Navi Mumbai, India
vanitamane1@gmail.com

Abstract— **Rather than of plentiful advantages of biometrics-based authentication systems over traditional security systems based on token or knowledge, they are susceptible to attacks that can decrease their security considerably. We have examined these attacks on the dataset of the multi-biometric system. We have implemented a system that uses a hill climbing procedure to synthesize the target minutia templates and estimate its possibilities with experimental results conducted on databases. Hill climbing attack is nothing but security attack based on generating artificial data, after analyzing the output; updating such data, so as to improve the output. This is done repeatedly till output is desire output. So that, several methods that can be used to decrease the probability of such attacks are implemented in this system. Some of the methods are uniform quantization techniques, non-uniform quantization techniques and many more. We have implemented uniform quantization technique, as quantization is the process of mapping a set of continuous pixel values into a finite numbers of possible values. The template distribution have been done on the basis of uniform quantized method which replicates the principle of uniform or linear quantizer has all the quantization levels uniformly distributed in the intervals.**

Keywords—Hill climbing, Nelder-mead, Uniform quantization, Biometrics, Authentication.

I. INTRODUCTION

Biometrics is nothing but measures related to human personality. Biometrics authentication is used in computer technology for the reason of identification and access control. Basically, it is used to identify individuals in group that are under examination. Hill climbing attack is nothing but security attacks used to generate synthetic data and introduce it in the system and after examining the output, update such data, as to improve the output. This is done repeatedly till the output is the preferred result [1]. Need of the system is the identification of human being and verification of legitimate user. Basically, this system used in the forensics such as identification of criminals, surveillance etc, in government such as national identification card, voter ID etc, travel and immigration and health care [2].

The remainder of this report is organized as, in chapter 2, we introduce the literature survey of different methods, chapter 3 describes the problem definition, chapter 4 describes existing system, chapter 5 describes proposed system of the system, chapter 6 describes the biometric security using Nelder-Mead, chapter 7 is the describe performance and result analysis of the system, chapter 8 describes limitation and future scope of system and chapter 9 is the conclusion of system.

II. LITERATURE REVIEW

The SPSA optimization procedure has been defined in order to provide the means to calculate approximations for the slope of unknown functions, being successfully accepted in many different applications. Only two dimensions, regardless the dimensionality N of the considered representation **x**, are evaluated at each iteration [3]. The demerits are premature termination of iteration [4], some a priori knowledge about the statistics of **X**, such as X is the multi-dimensional variable [5].

The Nelder-Mead algorithm is one of the best known algorithms for multidimensional unconstrained optimization without derivatives. Apart from some minor calculational details in the basic algorithm, the main difference between different implementations lies in the construction of the initial simplex, and in the selection of termination tests used to end the iteration process [6]. The demerit is the criterion for stopping process has been encounter in which unknown parameters enters non linearly [7].

This method finds a smallest of multivariable, unconstrained and non-linear function. The procedure is based on direct search method. No derivatives are required. The procedure accepts a unimodal function; therefore, if more than one minimum exist, several sets of starting values are recommended [8]. It was observed that the pattern move, an intrinsic part of the HJ algorithm, hardly contributed to the quality of the outcome [9]

Implicit filtering builds upon coordinate search and then interpolates to get an approximation of the gradient. Similarly to the SPSA algorithm, it is based on a gradient estimate, computed by evaluating the objective function above two simplexes, each with N points [6]. There may be problem with the termination [10].

We resort to a Lloyd-Max quantizer which, having fixed the number *L* of desired quantized distance levels, determines the non-uniform quantization intervals minimizing the mean-square-error (MSE) between an original distribution and its quantized version. In more detail, the distribution employed for estimating the desired intervals is derived from the analysis of the genuine scores obtained when performing recognition over a training data set [3].

Uniform score quantization is used for increasing the system security against the hill-climbing attack. Quantization is the process of mapping a set of continuous pixel values into a finite number of possible values. The template division can be done on the basis of uniform quantized Method which replicates the principle of a uniform or linear quantizer has all the quantization levels uniformly distributed in the interval [3].

III. PROBLRM DEFINITION

Compared to traditional authentication system, biometric system is more secure but it has some weaknesses such as it may affect the security which may be directly affect the user's privacy. Because of this, attacker may attack on biometric templates and leak the confidential data of user. As reference with the above survey, there are some issues related to existing system which we have solved such as, SPSA algorithm has the drawback of obtaining a drop in the function value using a relatively small number of function evaluations. This usually results in premature termination of iterations. To deal with such cases is to restart the algorithm several times, with reasonably small number of allowed iterations per each run. Because of these two demerits, we have implemented elder- mead algorithm to detect the attack. NM algorithm also has the problem of termination of iteration. Since to solve this problem we have implemented the enhanced Nelder-mead algorithm with score value. Non-uniform quantization has the problem of high success rate, so that we have implemented the uniform quantization to countermeasure the attack.

IV. SYSTEM IMPLEMENTATION

In this project, we have identify the detection of attacker on the basis NM-method which conveys that complete template has to be divided and then the score of size has to be considered which will ultimately be increases to time of authenticating a user. Quantization is the process of mapping a set of continuous pixel values into a finite number of possible values. The template division can be done on the basis of uniform quantized Method which replicates the principle of a uniform or linear quantizer has all the quantization levels uniformly distributed in the interval (except possibly the two intervals at the boundaries when the range of possible amplitude is infinite

With the obtained score at each level, we have made further movement and if find sample size is mismatching 2/n size of total samples then we can say that error bound in finding matching template else the process will continue till last samples and if all samples are obtained as requisite then authentication will be provided. This is the case for signature and face template which provide better authentication terminology with respect to synthetic template generation which can be definitely prevented.

A. System architecture

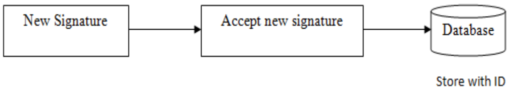


Fig. 1. Signature registration

With reference to Fig 1, first select signature of new authorized user and store it in database with some new id. That id related to the number of entries in the database.

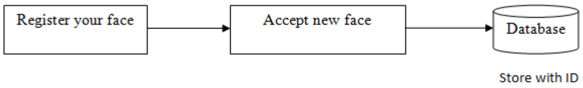


Fig. 2. Face registration

With reference to Fig 2, First capture new face then store it in database with id. That id related to number of entries in database.

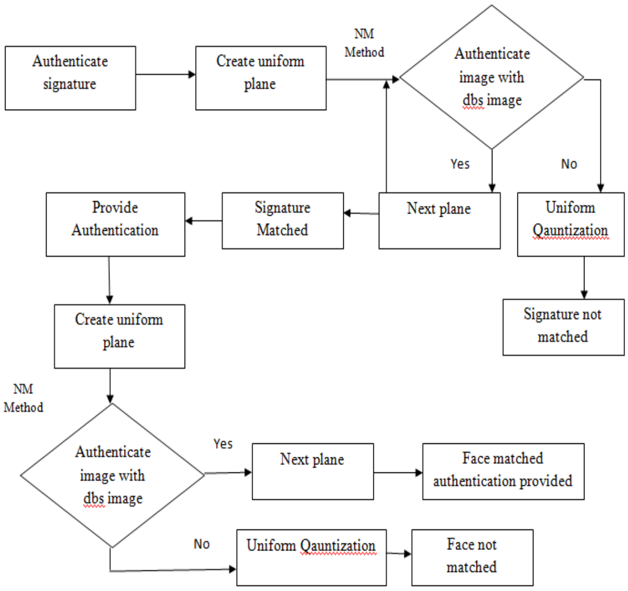


Fig. 3. Authorization

With reference to Fig 3, first authenticate signature then authenticate face. If signature is authenticated, then only algorithm work for face authentication. If signature doesn't match then algorithm stops their only.

1. *Database*

   A general term used to refer to any computer data that is created during a biometric process. This includes sample id, signature, faces and all verification or identification data excluding individuals name and demographics. Basically in this project we are using the signature database [11].

2. *Uniform plane*

   Here, uniform plane is created while dividing the biometric samples in to 'n' number of parts, compare extracted score of each part with image in the database if match found score counter is increased and continues if it doesn't matches then continues to match next plane if up to last plane, counter is below the threshold value, then hill climbing attack is detected.

B. Algorithms

1. Nelder-mead algorithm

Although the method is quite simple, it is implemented in many different ways. Apart from some minor computational details in the basic algorithm, the main difference between various implementations lies in the construction of the initial simplex, and in the selection of convergence or termination tests used to end the iteration process. The algorithm is,

Step 1: Construct the initial simplex S.

Step 2: Repeat the following steps until the termination test is satisfied:

i) calculate the termination test information;

ii) if the termination test is not satisfied then transform the working simplex.

Step 3: Return the best vertex of the current simplex *S* and the associated function value.

1. Initial simplex

The initial simplex S is constructed by generating n+1 vertices x0,…,xn with the given input $x_{in}\in R^n$. In general, the most common choice is $x_0=x_{in}$ to allow proper restarts of the algorithm. The remaining n vertices are then generated to obtain one of two standard shapes of S:

- S is right-angled at x0, based on coordinate axes, or

$$xj:=x0+hjej \quad j=1,\dots,n \tag{1}$$

Where hj is a step size in the direction of unit vector ej in R*n* .

- S is a normal simplex, where all edges have the same precise length.

2. Simplex Transformation Algorithm

The iteration of the Nelder-Mead method consists of the following three steps.

1. Ordering: Verify the indices h,s,l of the worst, second worst and the best vertex, respectively, in the current running simplex S

$$f_h=max_jfj,\ fs=max_j\neq hf_j,\ f_l=min_j\neq hf_j \tag{2}$$

In some implementations, the vertices of S are prearranged with respect to the function values, to satisfy
f0≤f1≤⋯≤fn−1≤fn. Then l=0, s=n−1 , and h=n.

2. Centroid: Compute the centroid c of the best side—this is the opposite of the worst vertex x_h

$$c=1n\sum j\neq hx_j \tag{3}$$

3. Transformation: Calculate the new running simplex from the current one. First, try to change only the worst vertex x_h with a better one by using reflection, expansion or contraction with respect to the best one. All test points recline on the line defined by xh and c , and at most two of them are calculated in one iteration. If this succeeds, the accepted point becomes the new vertex of the running simplex. If this fails, shrink the simplex towards the best vertex x_l. In this case, n new vertices are calculated.

Simplex transformations in the Nelder-Mead method are controlled by four parameters; α for reflection, β for contraction, γ for expansion and δ for shrink. They should satisfy the following condition,

$$\alpha>0,0<\beta<1,\gamma>1,\gamma>\alpha,0<\delta<1 \tag{4}$$

The standard values, used in most implementations,

$$\alpha=1,\beta=12,\gamma=2,\delta=12 \tag{5}$$

3. Termination tests

Basically, implementation of the Nelder-Mead method must include a test that ensures termination in a finite amount of time. The termination test is often consisting of three different cases: term-x, term-y and fail.

- term-x is the domain convergence or termination test. It becomes true when the running simplex S is satisfactorily small in some sense (some or all vertices xj are close enough).
- term-y is the function-value convergence test. It becomes true when (some or all) function values fj are close enough in some sense.
- fail is the no-convergence test. It becomes true if the number of iterations or function evaluations exceeds some prescribed maximum suitable value.

The algorithm terminates as soon as at least one of these tests becomes true.

2. Uniform quantization algorithm

Quantization is the process of mapping a set of continuous pixel values into a finite number of possible values. The template division can be done on the basis of uniform quantized method which replicates the principle of a uniform or linear quantizer has all the quantization levels uniformly distributed in the interval.

Step 1: Consider the image x with r * c

Step 2: Divide the complete image in similar size of blocks n

Step 3: From j= 1 to n

Step 4: Check If counter = 3

Step 5: If j = x then

Step 6: Consider next block

Step 7: if within the tolerance limit then also we can say images are matching. Then in this condition check for feature extraction parameter.

Step 8: If the features of database images such as area, perimeter, solidity, boundaries, and circularity are matches with feature of user images then provide authentication.

Step 9: else user is not authorized person

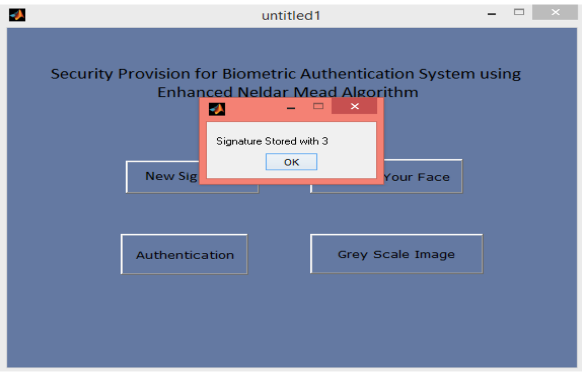
Step 10: else counter++

Step 11: End If

Step 12: Next j

V. OUTCOMES

A. *Results*

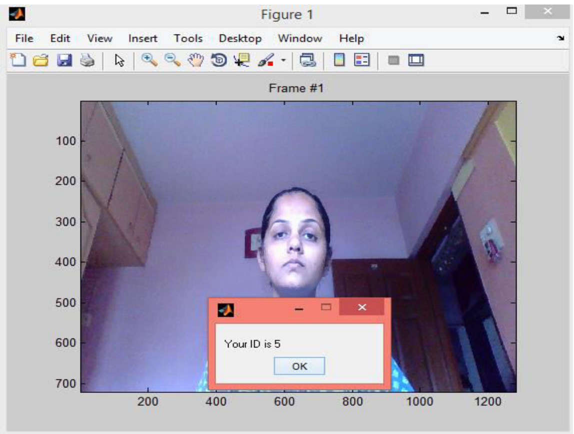


Security Provision for Biometric Authentication System using Enhanced Neldar Mead Algorithm

Signature Stored with 3

Fig. 4. Sign registration

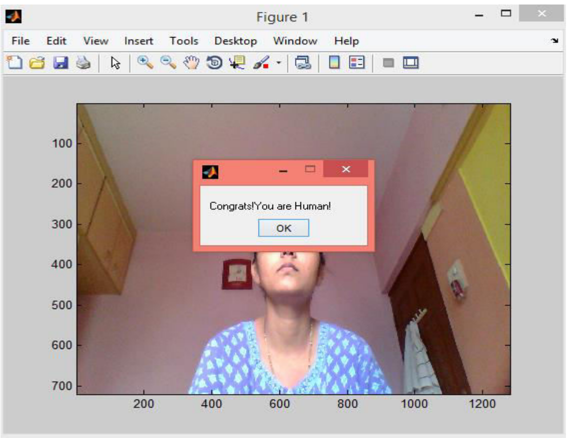
To registered new signature and face in the database we need to click on the new signature and select new signature and store it. This will generate a message called signature stored with some number depend on number of entries in database. Similarly, for face just to click on the register your face and system will capture your face and generate ID. As shown in Fig 4 and Fig 5.



Your ID is 5

Fig. 5. Face registration

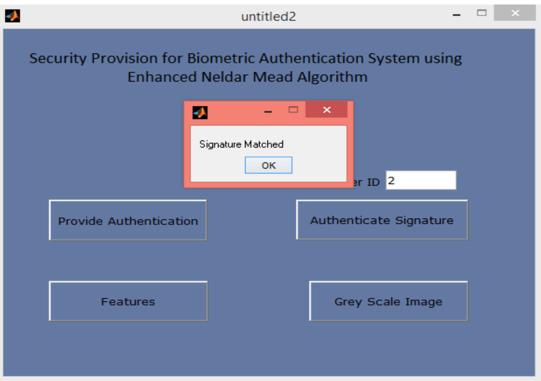
To provide authentication, it will create temporary image to compare with the database image. As shown in Fig 6



Congrats!You are Human!

Fig. 6. Provide authentication

Authentication signature will check for face and signature and depend on result, allow for authentication done or not. As shown in Fig 7 and Fig 8.

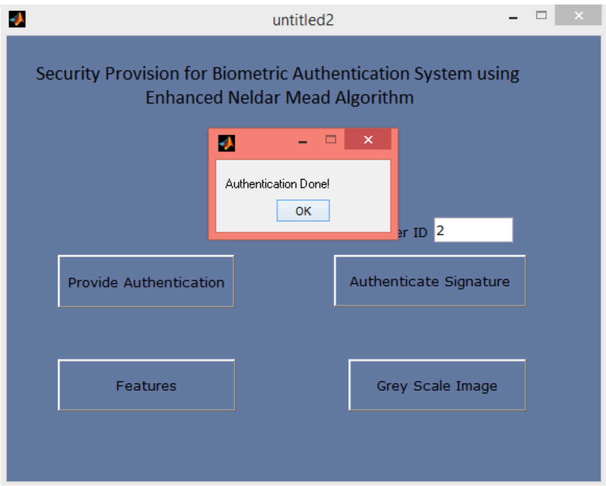


Security Provision for Biometric Authentication System using Enhanced Neldar Mead Algorithm

Signature Matched

r ID 2

Fig. 7. Signature matched



untitled2

Security Provision for Biometric Authentication System using Enhanced Neldar Mead Algorithm

Authentication Done!

Fig. 8. Authentication done

B. *Result Analysis*

TABLE 1

Comparative study

Parameters	**Existing system (%)**	**Proposed system (%)**
Success rate (SR)	0.25	0.125
False acceptance rate (FAR)	0.3	0.2
False rejection rate (FRR)	0.7	0.8
Total error rate (TER)	1.0	0.8

With reference to table 1, we have compare the existing system with proposed system. As research said as higher the SR, bigger the threat. As FAR is smaller in proposed system because of this SR is also smaller. As there is a reduction in FAR because of this FRR increases indirectly reduced TER. So, we can conclude from this the proposed system is better than existing system.

VI. CONCLUSION

Thus it can be concluding that biometric system play major role for different areas basically used to secure user's confidential data. Since there are several biometric devices are available such as iris, fingerprint, and face recognition machine and so on. Attacker try to attack on these biometric templates to stolen the user data, which uses hill climbing attack to perform this and for the detection of this attack we implemented NM- method. Since there are several algorithms available for this kind of attack such as SPSA, Hook- Jeeves algorithm but the NM- method is the best method to achieve this. If the biometric template is attacked by attacker then it cannot be detect by human vision, algorithm is required to detect such attack. Basically security is the main issue of biometric system, for this we implemented uniform score quantization technique. Since, score quantization is used to countermeasure the attack; there are two types of quantization, uniform and non-uniform. From the above analysis, uniform score quantization is the best method to countermeasure the attack.

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Prof. Vanita Mane for their exemplary guidance, monitoring and constant encouragement throughout the completion of this report. I am truly grateful to her efforts to improve my technical writing skills. The blessings, help and guidance given by her time to time shall carry me a long way in a journey of life on which I am about to embark. I take this privilege to express my sincere thanks to Prof. Dr. A. K. Sen, Principal, and Y.T.C.E.M. for providing the much necessary facilities. I am also thankful Prof. Vijay Shelake, Head of Department of Computer Engineering and PG coordinator Prof. Suchita Walke, Department of computer engineering, Y.T.C.E.M., Bhivpuri, Karjat for their generous support. Last but not the least I would also like to thanks all those who have directly or indirectly help me in completion of this report.

REFERENCES

[1] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega Garcia, and J. A. Siguenza, "Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification," in Proc. 40th IEEE ICCST, Oct. 2006, pp. 151–159.

[2] https://www.studymafia.org

[3] E. Maiorana, G. E. Hine, and P. Campisi, "Hill-climbing attack: Parametric optimization and possible countermeasures. An application to on-line signature recognition," in *Proc. IEEE ICB*, Jun. 2013, pp. 1–6.

[4] J. C. Spall, "Implementation of the simultaneous perturbation algorithm for stochastic optimization," IEEE Trans. Aerosp. Electron. Syst., vol. 34, no. 3, pp. 817–823, Jul. 1998.

[5] E. Maiorana, G. E. Hine, D. La Rocca, and P. Campisi, "On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures," in *Proc. IEEE BTAS*, Sep./Oct. 2013, pp. 1–6.

[6] J. A. Nelder and R. Mead, "A simplex method for function minimization," Comput. J., vol. 7, no. 4, pp. 308–313, 1965.

[7] Hooke R & Jeeves T A. "Direct search" solution of numerical and statistical problems J. Ass. Comput. Mach. **8**:212-29, 1961.

[8] Hooke R & Jeeves T A., "Hooke-Jeeves Revisited," I Moser, Member, IEEE, 2009

[9] P. Gilmore and C. T. Kelley, "An implicit filtering algorithm for optimization of functions with many local minima," *SIAM J. Optim.*, vol. 5, no. 2, pp. 269–285, 1995.

[10] S. Lloyd, "Least squares quantization in PCM," IEEE Trans. Inf. Theory, vol. 28, no. 2, pp. 129–137, Mar. 1982.

[11] https://www.aut.bme.hu/Pages/Research/Signature/Resources