International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 8 196 - 200

Security provision for biometric authentication systems using Enhanced Nelder Mead Algorithm

Miss Poonam Janardan Talele
Department of Computer Engineering
Yadavrao Tasgaonkar College of Engineering and Mngt.
Bhivpuri, Mumbai, India
poonamjtalele@gmail.com

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

***Abstract*—** Since, their are numerous advantages of biometrics-based authentication systems over traditional security systems based on knowledge, they are susceptible to attacks that can decrease their security significantly. We analyze these attacks in the multibiometric system. We propose an attack system that uses a hill climbing procedure to synthesize the targeted templates and evaluate its achievability with experimental results conducted on large 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 actions can be utilized to decrease the probability of such attacks and their result are also presented. Some of the measures are uniform quantization techniques, non-uniform quantization techniques and many more. We are using uniform quantization, as quantization is the process of mapping a set of continuous pixel values into a finite numbers of possible values. The template division can be 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 interval.

Keywords- *Hill climbig attack, Nelder-Mead method, Uniform quantization, Multibiometrics, Authentication*

*****

I. INTRODUCTION

A. *Biometrics*

Biometrics is nothing but metrics related to human personality. Biometrics authentication (or realistic authentication) is used in computer technology for the purpose of identification and access control. It is also used to identify individuals in groups that are under inspection. There are two main types of biometrics identifiers:

1. Physiological characteristic: The shape or composition of body.
2. Behavioral characteristic: The behavior of person.

The example of physiological characteristic used for biometric authentication include fingerprint, face, hand, ear and behavioral characteristic include pattern of behavior of person such as monitoring keystroke, typing rhythm, gesture, voice.

B. *Hill climbing attack*

Security attacks based on generating synthetic data 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. In biometrics, this attack can be used to generate a fake sample, by examining the matching score returned by the system. A hill-climbing attack may be carried out by an application that sends random templates to the system, which are disturbed iteratively. The application reads the output match score and continues with the disturbed template only when the matching score increases until the decision threshold is exceeded [1].

The need of this research is the identification and verification of person, is to ensure the weather person is a legitimate user or not.

Basically, this biometric system used in the forensics such as, identification of criminals, surveillance, in government for voter-id, employee authentication, in travel and immigration such as air travel, border crossing and so on [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 work of the system, chapter 6 describes the performance evaluation system and chapter 7 is the conclusion of the system.

II. LITERATURE REVIEW

A. *Literature survey*

The SPSA optimization procedure has been defined in order to provide the means to compute approximations for the gradient of unknown functions, being successfully accepted in many different applicative scenarios. Only two measurements, 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 or simplex search algorithm, is one of the best known algorithms for multidimensional unconstrained optimization without derivatives. Apart from some minor computational 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 minimum 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 $\mathcal{L}$ 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].

B. *Challenges*

1. SPSA algorithm has the disadvantage in obtaining a good reduction in the function value using a relatively small number of function evaluations.
2. This usually results in premature termination of iterations. A heuristic approach to solve such cases is to restart the algorithm several times, with reasonably small number of allowed iterations per each run.
3. NM algorithm also has the problem of termination of iteration.
4. Non-uniform quantization has the problem of high success rate.

III. PROBLEM DEFINITION

Biometrics is the most secure than the traditional authentication system but besides of some weaknesses it may affect the security which may be directly affect the user's privacy. Because of that attacker may attack on biometric templates and leak the confidential data of user. By the observation of above survey, there are some issues related to existing system which need to be solved.

1. SPSA algorithm has the disadvantage in obtaining a reduction in the function value using a small number of function evaluations.
2. This usually results in premature termination of iterations. The approach to solve such cases is to restart the algorithm several times, with reasonably small number of allowed iterations per each run. Because of this two demerits, it's better use nelder-mead algorithm to detect the attack.
3. NM algorithm also has the problem of termination of iteration. Since to solve this problem we are using the enhanced nelder mead algorithm with score value.
4. Non-uniform quantization has the problem of high success rate, so that we are using the uniform quantization to countermeasure the attack.

IV. EXISTING SYSTEM

The existing system considers the hill climbing attack on multibiometric with providing the proper countermeasure for system. It uses simultaneous perturbation stochastic approximation (SPSA) method to perform hill climbing attack on multibiometric system with serial fusion architecture also provide countermeasure for the biometric system using non-uniform quantization as a security.

The hill-climbing attacks can be applied to any generic biometric recognition system, given that the templates are expressed through a finite set of N parametric features $\mathbf{x}[i]$, $i = 1. . . N$. The purpose of these methods consists in finding a local optimum point for an objective function $F(\cdot)$, whose arguments are calculated by the determinations $\mathbf{x}$ of an N-dimensional random variable $\mathbf{X}$.

The methods described can be easily applied to a unimodal biometric recognition system as a attack strategies, being the produced similarity scores broken as evaluations of the unknown objective function, upon which the creation of synthetic biometric representations $\mathbf{x}$ can be driven. However, their application to a multibiometric system is not necessarily straightforward. This system uses serial fusion for implementing multibiometrics hill climbing attack.

A serial fusion scheme for a bimodal biometric system is depicted in Fig.1. A system where the considered biometrics is acquired sequentially may provide some benefits in terms of processing time.

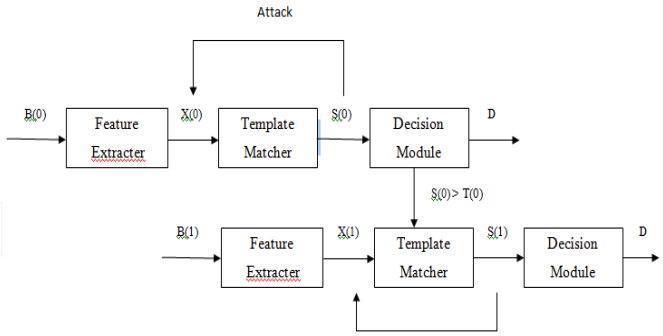

Fig.1. Serial fusion with hill climbing attack [11]

The application of a nonuniform quantization to the matching scores can actually limit the effectiveness of hill-climbing attacks. Nonuniform quantization can be performed using a Lloyd-Max quantizer having set the number L of desired quantized score levels, the nonuniform quantization intervals can be determined by minimizing the mean-square error (MSE) between a given similarity score and its quantized version. The employed score is obtained collecting data during a training phase and performing comparisons among real biometric data [11].

V. PROPOSED SYSTEM

In this project, we are diagnosing 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 eventually be incremented 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 amplitudes is infinite).

With the obtained score at each level, we will make further movement and if find sample size is mismatching 2/n size of total samples then will say 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 will be the case for fingerprint and iris template which will provide better authentication terminology with respect to synthetic template generation which can be definitely prevented.

Fig.2. shows flow of execution of attack and their countermeasure. In this project, we are considering the image which will be registered by the user at first time. After this when user comes for authentication, the image meant for authentication will be evaluated for Enhanced Nelder-Mead Algorithm.

With this image will be the Nelder-Mead algorithm is normally initialized by arbitrarily picking samples from the estimated distribution of the N considered features, assumed to be independent and with Gaussian behaviors. To prevent hill climbing attack, we will be implementing uniform score quantization. It is used for increasing the system security against the hill-climbing attack, although not achieving proper robustness against the studied attack.

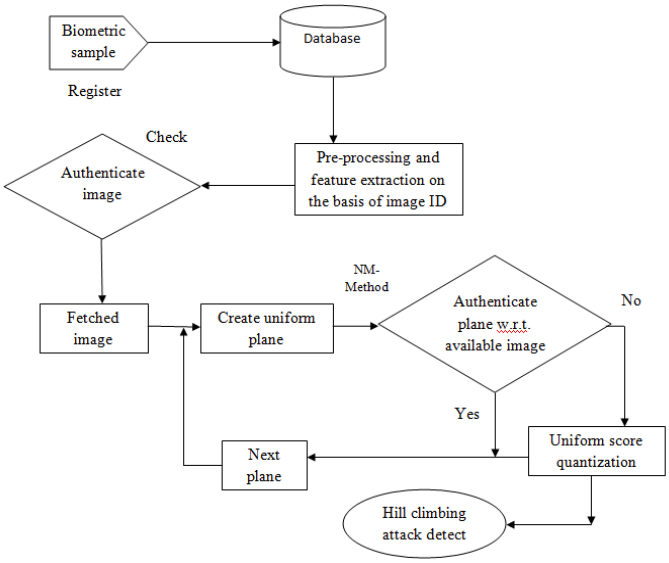

Fig.2. Architectural diagram of proposed system

A. *Nelder-Mead method*

The Nelder-Mead algorithm is one of the most excellent well-known algorithms for multidimensional unconstrained optimization without derivatives. This method solves a linearly constrained linear problem. The basic algorithm is very easy to use and simple to use. Because of this, it is accepted in many fields of science and technology, especially in chemistry and medicine.

This method doesn't require any derivative information, which is suitable for problems with non-smooth functions. It is generally used to solve parameter estimation and similar statistical problems, where the function values are tentative or subject to noise. It can also be used for problems with discontinuous functions, which occur frequently in statistics and experimental mathematics.

B. *Uniform quantization*

When a solution is introduced in a biometric system to minimize the risk of attack, it should be evaluated while considering two main parameters:

- Effect of the countermeasure in the system performance. The inclusion of a particular protection scheme might change the false acceptance rate (FAR) and false rejection rate (FRR) of a system, and these changes should be evaluated and reported
- Performance of the countermeasure, i.e. impact of the countermeasure in the Security rate (SR) and Eff (efficiency) of the attack.

Among the biometric-based approaches to reduce the effects of hill-climbing attack, score quantization technique has been proposed as an effective countermeasure. 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.

```
x= image blocks of image to be authenticated
Consider the image x with r * c
Divide the complete image in similar size of blocks n
From j= 1 to n
  If counter = 3
   If j = x then
     Consider next block
   Else
     Counter ++
End if
  Next j
```

C. *Biometric sample*

The data obtained from biometric system's capture device-such as a facial image, voice recording or a fingerprint.

D. *Database*

A term is used to refer to any computer data that is created during a biometric process. This includes samples, models, fingerprints, similarity score, and all verification or identification data excluding individuals name and demographics.

E. *Hill climbing attack*

A hill-climbing attack may be performed by function that sends random templates to the system, which are disturbed iteratively. The function reads the output match score and continues with the disturbed template only when the matching score increases until the decision threshold is exceeded.

F. *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.

G. *Feature extraction*

Feature extraction is the process in which input features of the sample are selected. Typically, the process of feature extraction based on a set of algorithms; the method changes depending on the type of biometric identification used.

Since, some examples of biometric feature extraction:

- A fingerprint feature extraction program will situate measure and encode ridge edgings and bifurcations in the print.
- A voice recording may sort out particular frequencies and patterns.
- A digital picture may consider particular measurements, like the relative positions of the ears, forehead, cheekbones and nose.
- Iris prints will select the mapping of furrows and striations in the iris.

VI. PERFORMANCE EVALUATION

The goal of the experiments is to analyze in an objective and replicable manner the attacking skills of the hill-climbing attack. With this purpose, the performance of the attack will be evaluated in terms of the following parameters.

- **Success Rate (SR)**: It is the probability that the attack breaks a given account. It is calculated as the ratio of the number of broken accounts (A_B) and the total number of accounts attacked (A_T)

$$SR=A_B / A_T \quad (1)$$

This parameter indicates how dangerous the attack is: the higher the SR, the bigger the threat.

- **Efficiency (Eff):** It indicate average number of matching needed by the attack to break the account. It is defined as,

$$Eff = \sum_{i=1}^{A_B} n_i / A_B \quad (2)$$

Where n_i is the number of matching computed to bypass each of the broken accounts. This parameter gives an evaluation of how easy for the attack to break into system in terms of speed: the lower the Eff, the faster the attack.

- **False match rate (FAR = False Accept Rate)**: The possibility that the system incorrectly matches the input pattern to a non-matching template in the database. It calculated the percentage of invalid inputs that are incorrectly accepted. In case of similarity range, if the person is an imposter in reality, but the matching score is higher than the threshold, then person is treated as genuine.

FAR= Number of false acceptance/ Number client accesses (3)

- **False non-match rate (FRR = False Reject Rate)**: This is the probability that the system fails to identify a match between the input sample and a matching template in the database.

FRR=Number of false rejection/Number client accesses (4)

- **Total Error Rate (TER):** It is also remarkable that any of the two values FRR and FAR can be reduced to an random small number, with the drawback of increasing the other value is the TER.

TER= (No. of FA + No. of FR)/ total number of access (5)

VII. CONCLUSION

Biometric system provide major task for different areas basically used to secure user's confidential data. Since there are several biometric devices are available such as iris, fingerprint, 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 uses 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, apart from using this algorithm we need to provide countermeasure for the system. 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.

REFERENCES

[1] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez,J. Ortega-Garcia, and J. A. Siguenza, "Hill-climbing and brute-forceattacks on biometric systems: A case study in match-on-card fingerprintverification," 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 applicationto 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] 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.

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

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

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

[10] 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.

[11] Emanuele Maiorana, Gabriel Emile Hine and Patrizio Campisi, "Hill-Climbing Attacks on Multibiometrics Recognition Systems," IEEE Trans. Inf. Theory, VOL. 10, NO. 5, MAY 2015.