ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

A SURVEY ON SWARM INTELIGENCE BASED BIOMETRIC INFORMATION SYSYTEM

[1] **K. Juliana GnanaSelvi,**
[1] Head of the Department,
[1] Department of Information Technology,
[1] Rathinam College of Arts and Science, Coimbatore, Tamil Nadu – 641 021.

Abstract:-

Swarm intelligence (SI) is the collective behavior of decentralized, self-organized systems, natural or artificial. Systems consist typically of a population of simple agents or boids interacting locally with one another and with their environment. The inspiration often comes from nature, especially biological systems. The agents follow very simple rules, and although there is no centralized control structure dictating how individual agents should behave, local, and to a certain degree random, interactions between such agents lead to the emergence of "intelligent" global behavior, unknown to the individual agents. Examples in natural systems of SI include ant colonies, bird flocking, animal herding, bacterial growth, fish schooling and microbial intelligence.

Keywords: - [Swarm intelligence, Biometrics, Intelligence, behavior metrics]

1. INTRODUCTION

Swarm intelligence is a modern artificial intelligence discipline that is concerned with the design of multi agent systems with applications, e.g., in optimization and in robotics. The concept is employed in work on artificial intelligence. The expression was introduced by Gerardo Beni and Jing Wang in 1989, in the context of cellular robotic systems. SI The design paradigm for these systems is fundamentally different from more traditional approaches. Instead of a sophisticated controller that governs the global behavior of the system, the swarm intelligence principle is based on many unsophisticated entities that cooperate in order to exhibit a desired behavior. Inspiration for the design of these systems is taken from the collective behavior of social insects such as ants, termites, bees, and wasps, as well as from the behavior of other animal societies such as flocks of birds or schools of fish.

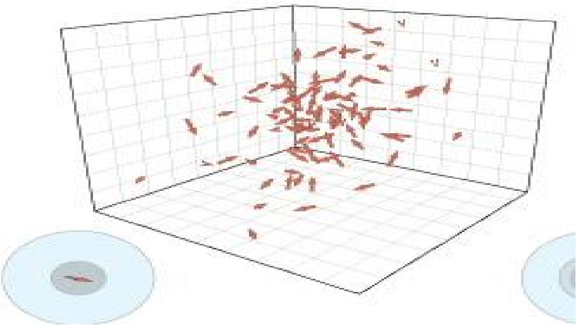

Figure 1: Swarm sample Simulation for any Specimen

Even though the single members of these societies are unsophisticated individuals, they are able to achieve complex tasks in cooperation. Coordinated behavior emerges from relatively simple actions or interactions between the individuals. Moreover, engineers are increasingly interested in this kind of swarm behavior since the resulting “swarm intelligence” can be applied in optimization for ex. in telecommunicate systems, robotics, traffic patterns in transportation systems and military applications. Swarm intelligence is the emergent collective intelligence of groups of simple autonomous agents. Here, an autonomous agent is a subsystem that interacts with its environment, which probably consists of other agents, but acts relatively independently from all other agents. The autonomous agent does not follow commands from a leader.

2. THE BIO METRIC INTRODUCTION

Biometrics refers to the identification of persons by their individuality or behavior. Biometrics is mainly used in various fields as an outline of recognition and access control. Also it is used to identify each person in groups that are under observation. Biometric identifiers are exclusive, significant characteristics used to tag and illustrate individuals. Biometric identifiers are frequently sort as physiological against behavioral characteristics. Physiological biometric would recognize by one's voice, DNA, hand print or behavior and the behavioral biometrics are typing rhythm, walk, voice etc. Researchers have introduced the word called behaviometrics to explain the other class of biometrics. Further conventional approaches of access control comprise of token-based identification systems, such as a driver's license, passport, voter id and knowledge-based identification system such as a password or personal identification number etc. Even though biometric identifiers are distinctive to each person, they are consistent in verifying identity than the other methods. Hence, the collection of biometric identifiers raises privacy concerns about the vital use of this information.

3. RECENT RESEARCH PROBLEM

Conventional security and authentication systems have been developed largely by various researchers. The Conventional authentication system simply needs the user to give the authorized account and password to log into the system once they start to use a computer or a terminal. Though, under this authentication support, the machine can only be familiar with the user’s identity from the login information. It does not have the data to identify who is using it. Disadvantage of the one-time authentication system is that if a person use the system in daily life, when the user leaves the place for a break like to get some documents or have a drink, that time anybody can steal up to the computer and pretend to be the authorized user to access their data, or do anything under a fake identity. Afterward if the system is on, no one will know who used the computer. This type of security fault is not tolerable in some applications with the sensitive data, for instance, the banking financial record, the military industry and the business confidentiality.

3.1 Research literature in Swarm Intelligence

The continuous authentication is not a class idea it is an interrelated research has been taking place for more than a past few years. Nevertheless, the interest in this field is increases with time due to the need of the security issue existing in the conventional one-time authentication system. The recent authentication method is extensively used in our day to day life and it can be classified as the one-time authentication system. This system requests the user to entry the account and the related password to login the system. Once the login is done, the account will be kept in the login status up to the user logoffs the system. Still, while the user using the system, the machine is blind, it does not know who is using the system. To prevail over this problem, many continuous authentication approaches, models, and systems have been introduced. Even though, at least one of the factors like knowledge factors, ownership factors, and inherence factors are present in authentication system which is used to be the recognition core. Here the term Knowledge factors means that unique things that are authorized in terms of user's knowledge, for example the user account and the password. Ownership factor means certain things that are accessed only by the authorized user, for example the smart card, the radio frequency identification (RFID) card. Inherence factor includes the distinctive feature owned by the authorized user, for example, the biometric information.

4. APPLICATION OF SWARM INTELLIGENCE IN BIOMETRICS

The protection and the intelligence communities need high level security systems. Border management, interface for criminal and civil applications, and first responder verification are the major areas which use the Multimodal Biometrics. Personal information and Business transactions need fraud prevent solutions that increase security and are cost effective and user friendly. Multi modal biometrics can provide finest solutions to all the areas where high level security systems are needed. Swarm intelligence is personalized for verification process. Signature is highly preferable by means of Collectability and Acceptability. So the studies on signature verification have a great importance. A great deal progress has been performed in SI modern days. Swarm Intelligence (SI) is an inventive intelligent paradigm for solving optimization problems that originally took its motivation from the biological examples of insects or animals that collectively exhibit complex behaviors, for example, bees, ants or birds. Contemporary environmental remote sensing satellite imagery, owing to their large volume of high-resolution data, offer greater challenges for automated image analysis. Ant Colony Optimization (ACO) algorithm takes motivation from the synchronized behavior of ant swarms. Using the ACO algorithm for pattern recognition in remote sensing imagery does not suppose an underlying statistical distribution for the pixel data, the contextual information can be taken into account, and it has strong robustness. We are capable of modeling the problem by representing biometric templates as ants, grouped in colonies representing the clients of a biometrics authentication system. The biometric template classification process is modeled as the collection of ants to colonies. The swarm look for optima in the solution space and shrinks the search area step by step. If an active change occurs in the system affecting the search area, the PSO will automatically find new optimum without any modification. The system design, however, is problem specific and has many implied and unequivocal factors which affect its performance. Using the ACO algorithm for pattern recognition in remote sensing imagery does not assume an underlying statistical distribution for the pixel data, the contextual information can be taken into account, and it has strong robustness. When test input data is confined, there is a new ant in our representation and it will be inclined by the deposited pheromones related to the inhabitants of the colonies. Hence we can safely assume that swarm intelligence is moving towards a very capable track for further investigations for biometrics verification and identification.

CONCLUSIONS

'Swarm intelligence' refers to the more general set of algorithms. 'Swarm prediction' has been used in the context of forecasting problems. Biometric technology appends a new layer of security by ensuring secure identification and authentication. However biometric authentication systems like any other technology are also vulnerable to attacks such as transmission, replay and spoofing. There are many proposed methodologies that are used to defeat them. Multimodal biometric system is a major approach to defeat spoofing attacks. Various scenarios of swarm biometrics systems are discussed. We conclude that swarm intelligence is moving towards a very capable track for further investigations for biometrics verification and identification.

REFERENCES

[1] Hong L, Jain A .& Pankanti S., Can Multibiometrics Improve performance, Proceedings of AutoID 99, pp. 59-64, 1999.

[2] Ross A.& Jain A.K , Information Fusion in Biometrics, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

[3] Ross.A. A, Nandakumar.K, Jain.A.K. Handbook of Multibiometrics. Springer-Verlag, 2006.

[4]J. Fierrez-Aguilar, Ortega-Garcia J.,Garcia-Romero D., and Gonzalez Rodri guez J, ―A comparati ve eval uati on of fusi on strategi es for multimodal biometric verification,‖i n Proc. 4th Int , Conf, Audio-video-based Biometric PersonAuthentication , J. Kittler and M. Nixon, Eds., 2003 vol. LNCS 2688, pp. 830–837

[5] Hong L. and Jain A. K , ―Integrati ng faces and fingerprint s for personal i denti fi cati on,‖ IEEE Trans. Pattern Anal. Mach. Intell. , vol. 20, no. 12, pp. 1295– 1307, Dec. 1998

[6] Kumar A. , Wong, Shen1 H. C. , and Jai n A. K, ― Personal verifi cati on usi ng pal mpri nt and hand geometry biometric, ‖i n Proc. 4th Int. Conf. Audio- Video-Based Biometric Person Authentication , J. Kittler and M Nixon, Eds., 2003 vol. LNCS 2688, pp 668–678

[7]Frischhol z R. and Di eckmann U., ―Biol D: A multimodal bi ometri c i denti fi cati on system,‖ Comput er, vol. 33,no. 2, pp.64-68,Feb,2000

[8] Chandran GC, Rajesh RS (2009). Performance Analysis of Multimodal Biometric System Authentication, Int. J. Comput. Sci. Network Security, 9: 3.

[9]Toh K. A , Jiang X.D, and Yau W. Y, ―Expl oit ing global and local decisions f or mult i-modal biometrics verification,‖ IEEE Trans. Signal Process. , vol. 52, no. 10, pp. 3059–3072, Oct. 2004

[10] Poinsot A, Yang F, Paindavoine M (2009). Small Sample Biometric Recognition Based on Palmprint and Face Fusion, Fourth International Multi-Conference on Computing in the Global Information Technology.

[11] Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype Design for High Security Biometrics, CIBEC'08.

[10] A. Zramdini, "Study of optical font recognition based on global typographical features", PhD thesis, University of Fribourg, 1995.

[11] H. Nezam, S. Nezam Abadipour, and V. Saryazdi and Ebrahimi, "Font recognition based on Gabor filters" (in Farsi), in 9th Iranian Computer Conference , pp. 371-378, 2003.

[12] E. Rashedi, H. Nezamabadi-pour, and S. Saryzadi, "Farsi font recognition using correlation coefficients" (in Farsi), in 4th Conf. on Machine Vision and Image Processing , (2007): Iran.

[13] A. Borji and M. Hamidi, "Support vector machine for Persian font recognition", International Journal of Computer Systems Science and Engineering , Vol.2 (3), 2007.

[14] H. Khosravi and E. Kabir, "Farsi font recognition based on Sobel-Roberts features",
Pattern Recognition Letters, Vol.31, p. 75-82, 2010

[15] J. Yang and V. Honavar, "Feature subset selection using a enetic algorithm", IEEE Intelligent Systems and their Applications, Vol.13, p. 44-49, 1998.

[16] X. Wang, et al., "Feature selection based on rough sets and particle swarm optimization",
Pattern Recognition Letters, Vol.28, pp. 459-471, 2007.

[17] M. Dorigo, "Optimization, learning and natural algorithms", in Dipartimento di Elettronica, Ph.D. dissertation, Politecnico di Milano: Italy, 1992

[18] M. Dorigo and T. Sttzle, "Ant colony optimization", MIT press, 2004.