ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Applications of Swarm Intelligence in Biometrics systems

Sumit Chabbra, Nirmaljit Singh

Assistant Professor, PG Dept. of Computer Science, Khalsa College for Women, Amritsar, Punjab, India

Assistant Professor, PG Dept. of Computer Science, Khalsa College for Women, Amritsar, Punjab, India

ABSTRACT – Biometrics are applied to analyze human uniqueness for security purposes. The universal physical biometrics patterns analyzed for security purposes are the fingerprint, hand, eye, face and voice. 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. In this paper we explore a swarm intelligence classification approach for biometrics verification and identification problems. With the fusion of biometrics and swarm intelligence we can reduce the system error rates.

KEYWORDS*:* Biometric Systems, Swarm Intelligence, Ant Colonies Optimization

I. INTRODUCTION

Biometric is defined as an automatic system that uses measurable physiological characteristics or behavior traits to recognize the identity or verify/authenticate the claimed identity of an individual. The advantage to a biometric is that it doesn't change or lose. Several body parts, personal characteristics and imaging methods have been used for biometric systems such as fingers, hands, feet, eyes, ears teeth, veins voices, signatures, typing styles and gaits. Each biometric has its own strength and limitations and accordingly each biometric is used in identification (authentication) applications. It is not hard to steal a biometric, create a copy and use the fake trait to attack biometric systems. This a serious issue as the people these days are using biometric as a means to enhance network security. Different technologies have been developed to defeat the spoofing attack. Since biometrics is not secret they cannot be protected like passwords. People flee their biometrics everywhere without being aware that their biometric information can easily be captured, copied or forged. An additional challenge to a biometric system is the speed i.e. the system must make an accurate decision in real time.

II. RELATED WORK

The research on multi modal biometrics started in late 90˝s. Face is most common biometric which is used alone or in combination with other biometrics. In 1998, a bimodal approach was proposed by Hong and Jain [5] for a PCA based face and a minutiae-based fingerprint identification system with a fusion method at the decision level. In 2000, Frischholz and Dieckmann [7] developed a commercial multimodal approach, BioID. Lip motion and face images were extracted from a video sequence and the voice from an audio signal for verifying the person. Fierrez-Aguilar and Ortega-Garcia (2003) [4] proposed a multimodal approach using face and minutiae-based fingerprint verification system, and an online signature verification system. Ross and Jain (2003) [2] combined face, fingerprint and hand geometry at the matching score level. Kumar et al. (2003) presented multimodal personal verification system using hand images by combining hand geometry and palm image at the feature level and match score level. Fusion at the match score level had good performance as compared to unimodal biometric. In 2004, Toh et al. [9] developed a multimodal biometric system using hand geometry, fingerprint, and voice at match-score-level fusion. Shahin et al. (2008) [11] used hand veins, hand geometry and fingerprint to provide high security. Chandran et al. (2009) [8] combined iris and fingerprint to improve the performance. Chin et al. (2009) [13] integrated palm print and fingerprint at feature level. Kang and Park (2009) [14] presented multimodal finger veins recognition using score level fusing for finger geometry and finger veins. Poinsot et al. (2009) [10] presented palm and face multimodal biometrics for small sample size problems. They used Gabor filter to extract features of palm and face images. Tayal et al. (2009) [12] presented multimodal iris and speech authentication system using decision theory.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

III. ATTACKS ON BIOMETRIC SYSTEMS

Biometric systems offer several advantages over traditional token (e.g. key) or knowledge (e.g. password) based authentication schemes. Still, they are vulnerable to attacks. These attacks can be grouped into eight classes.

Class I: Spoof attack: In this type of attack a fake biometric e.g. (finger made from silicon, face mask, lens including iris texture) can be presented to a sensor.

Class II: The second class of attack is called *replay attack*. In it an interspected biometric data is submitted to the feature extractor by passing the sensor. To detect the replay attack, the authenticator as to ensure that the data is captured through the sensor and has not been injected. But sensor noise and input variations make hurdle in this detection so the best method is either to build a time stamp or using challenge and response mechanism to address the replay attack.

Class III: Substitution attack: In the third type of attack the feature exactor module is replaced by a Trojan horse program that functions according to its designer specifications. Then the attacker gets an access to storage either locally or globally. He can overwrite the legitimate users template with his /her own -in essence stealing their identity

Class IV: In the fourth type of attack a genuine feature values are replaced with values (synthetic or real) selected by the attacker or an imposter

Class V: In this type of attack the matcher is replaced with a Trojan horse program. This class of attack is called *Trojan horse Attack*.

*Class VI***:** This type of attack occurs on the *template database*. The template database can be added, modified or removed. The templates can also be stolen which can be most dangerous.

Class VII: Transmission attack: A man in the middle attack is possible while the data is transmitted from one component to another. The attacker can manipulate the input data stream, send a fake template as an enrolled user, inject an artificial matching score or even generate a forged response.

Class VIII: Lastly the matured result (accept or reject) can be overridden by the attacker.

IV. MULTIMODAL BIOMETRIC SYSTEMS

Biometric systems used in real world applications are unimodal. They rely on the evidence of a single source of information for authentication. These systems have to deal with variety of problems such as:

Noise in the sensed data. (e.g., due to repeated use of fingerprint sensor)

Intra-class variation: User who is incorrectly acting with the sensor typically causes these variations.

Inter-class similarities: In a Biometric System where there are large no of users, there may be inter–class overlap in the feature space of multiple users.

Non-Universality: The Biometric System might not be able to acquire a meaningful Biometric data from a subset of users.

Spoof Attack: This attack occurs when signature or voice are used in Biometric System.

Not all but some of the limitations of the unimodal can be overcome by including multiple source of information for identification**.** These types of system are called as *Multimodal Biometric Systems***.** These systems are more reliable due to the presence of multiple, independent biometrics. They also have better performance, as it would be difficult for an imposter to spoof multiple biometric traits of a genuine user simultaneously. Moreover, they provide a challenge – response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a „live" user is indeed present at the point of data acquisition. Some common multimodal biometrics are: face and finger print, face and iris, iris and finger print etc.

V. SWARM INTELLIGENCE

Swarm intelligence is a modern artificial intelligence discipline that is concerned with the design of multiagent systems with applications, e.g., in optimization and in robotics. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

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.

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. For example, for a bird to participate in a flock, it only adjusts its movements to coordinate with the movements of its flock mates, mainly its neighbours that are close to it in the flock. A bird in a flock simply tries to stay close to its neighbours, but avoid collisions with them. Each bird does not take commands from a leader bird since there is no leader bird. Any bird can fly in the front, centre and back in the swarm. Swarm behaviour helps birds take advantage of several things including protection from predators and searching for food. The main principles of the collective behaviour as presented in Figure[1] are:

• Homogeneity: Every bird in flock has the same behaviour model. The flock moves without a leader, even though temporary leaders seem to appear.
• Locality: The motion of each bird is only influenced by its nearest flock mates. Vision is considered to be the most important senses for flock organization.
• Collision Avoidance: Avoid with nearby flock mates.
• Velocity Matching : Attempt to match velocity with nearby flock mates.
• Flock Centering: Attempt to stay close to nearby flock mates.

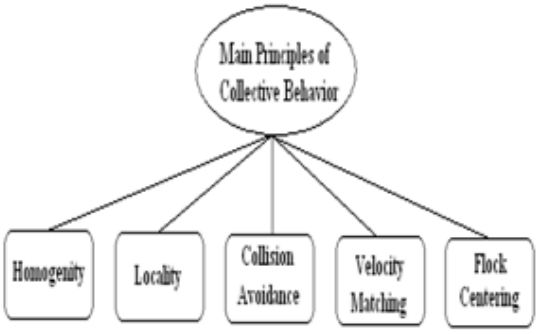

Fig.1. principles of collective behavior

This collective intelligence seems to emerge from what are often large groups of relatively simple agents. The agents use simple local rules to govern their actions and via the interactions of the entire group, the swarm achieves its objectives. A type of self-organization emerges from the collection of actions of the group. 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, or some global plan. For example, for a bird to participate in a flock, it only adjusts its movements to coordinate with the movements of its flock mates, typically its neighbors that are close to it in the flock. A bird in a flock simply tries to stay close to its neighbors, but avoid collisions with them. Each bird does not take commands from any leader bird since there is no lead bird. Any bird can in the front, center and back of the swarm. Swarm behavior helps birds take advantage of several things including protection from predators (especially for birds in the middle of the flock), and searching for food (essentially each bird is exploiting the eyes of every other bird).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Ant Colonies Optimization

Ant Colonies Optimization (ACO) algorithms were introduced around 1990. These algorithms were inspired by the behavior of ant colonies. Ants are social insects, being interested mainly in the colony survival rather than individual survival. Of interests is ants 'ability to find the shortest path from their nest to food. This idea was the source of the proposed algorithms inspired from ants' behavior. When searching for food, ants initially explore the area surrounding their nest in a random manner.

Instead of leaders or managers, the colony relies on "countless interactions between individual ants, each of which is following simple rules of thumb." Communication between ants is by touch and smell, and the frequency of contacts is an indicator of how much – food, or danger is there, for example – waits outside the nest. Information-sharing is key, and each ant is guided by what it encounters: you tell me what you know, and I use that information to decide what I do next. For example, when a foraging ant finds food, it lays a chemical trail all along the path it takes from the food source back to the nest. Every ant that encounters this chemical trail follows it to the food source – and on the return journey, leaves its own trail until there's no more food, and the trail is not renewed. The indirect communication between the ants via pheromone trails enables them to find shortest paths between their nest and food sources.

The main steps of the ACO algorithm are given below:

1. *pheromone trail initialization*
2. *solution construction using pheromone trail*
   Each ant constructs a complete solution to the problem according to a probabilistic
3. *state transition rule.* The state transition rule depends mainly on the state of the pheromone.
4. *pheromone trail update.*

Data Clustering

Data Mining (DM) or Knowledge Discovery in Databases (KDD) is the nontrivial extraction of implicit, previously unknown, and potentially useful information from data. This encompasses a number of different technical approaches, such as clustering, data summarization, learning classification rules, finding dependency networks, analyzing changes, and detecting anomalies.

Clustering is the task of identifying groups in a data set based upon some criteria of similarity. Clustering aims to discover sensible organization of objects in a given dataset by identifying and quantifying similarities or dissimilarities between the objects.

Clustering is applied in various fields, including data mining, statistical data analysis, compression and vector quantization. In data mining, clustering is used especially as preprocess to another data mining application. A variety of clustering formulation exists. We implement a clustering method using ant colony optimization for clustering a data set into a pre-determined number of clusters.

Real ants have the ability to find the shortest path from their nests to the food source without any visual trace. Ant colony [FIGURE 2]optimization is developed by modeling this behavior of real ants. Applications of ant colony optimization applied on firstly traveling salesman problem, which is defined as finding the shortest or nearly shortest path connecting a number of locations, such as cities visited by a traveling salesman on traveler's sales route. Furthermore, ant colony optimization technique is used to solve many problems like graph coloring, vehicle routing problems, scheduling problems, communication network design. But, recently there exist new ant colony optimization algorithms developed for clustering and classification problems used also in data mining.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

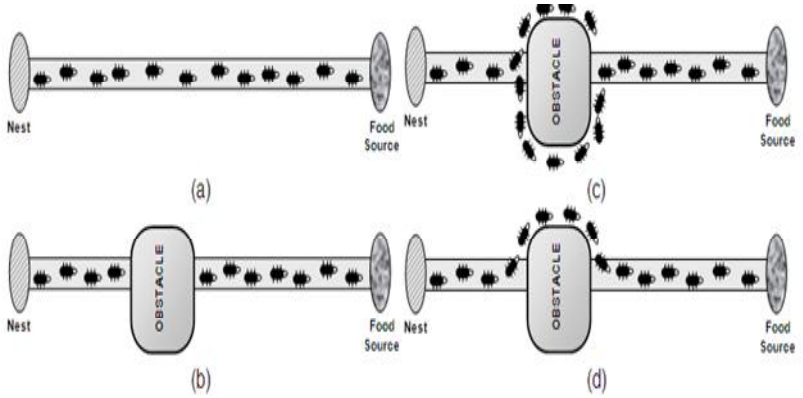

Fig.2. Ant Colony

The aim of this study is solving data-clustering problem with a new approach named ant colony optimization. The algorithm developed aiming to solve this problem is applied on a dataset and to increase working performance of the algorithm.

VI. 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 phermonones 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.

VII. CONCLUSIONS

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

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 Rodriguez J, ―A comparative evaluation of fusion strategies for multimodal biometric verification,‖in 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 , ―Integrating faces and fingerprints for personal identification,‖ IEEE Trans. Pattern Anal. Mach. Intell. , vol. 20, no. 12, pp. 1295– 1307, Dec. 1998
[6] Kumar A., Wong, Shen1 H.C., and Jain A.K, ― Personal verification using palmprint and hand geometry biometric,‖in Proc. 4th Int. Conf. Audio- Video-Based Biometric Person Authentication , J. Kittler and M Nixon, Eds., 2003 vol. LNCS 2688, pp 668–678
[7]Frischholz R. and Dieckmann U., ―BiolD: A multimodal biometric identification system,‖ Computer,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, ―Exploiting global and local decisions for multi-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.
[12]Tayal A, Balasubramaniam R, Kumar A, Bhattacharjee A, Saggi M (2009). A Multimodal Biometric Authentication System Using Decision Theory, Iris and Speach Recognition, 2nd International Workshop on Nonlinear Dynamics and Synchronization.
[13] Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security.
[14] Kang BJ, Park K (2009). Multimodal Biometric Authentication Based on the Fusion of Finger Veins and Finger Geometry, Optical Eng., 48.
[15] Daughman J., ―Combining multiple biometric,‖ Avaliable online at www.cl.ca.ac.uk/users/igd1000/combine.html, 2002.
[16] Anil K. Jain , Ruud Bolle and Sharath Pankanti "Biometric Personal Identification in Networked Society".
[17]" Global Security. Emerging Technologies
URL: http://www.globalsecurity.org/security/systems/emerging.htm
[18] Kassabalidis, E. M. A. Sharkawi, R. J. Marks, P. Arabshahi, and A. A. Gray, "Swarm intelligence for routing in communication networks," in Proc. of the IEEE Global Tel. Conf. (GLOBECOM). IEEE Press, 2001.
[19] Kennedy J.and Eberhart R., Swarm Intelligence. Morgan Kaufmann, 2001.
[20] Dorigo M. "Optimization, learning and natural algorithms," Ph.D. dissertation, Politecnico di Milano, Italy, 1992.
[21] Bonabeau E. and Théraulaz G., Swarm Smarts, Scientific American 2000.
[22] Sarfati, J., Ants find their way by advanced mathematics, 2001.
[23] Foster, I., and Kesselman, C. (eds.). The Grid: BluePrint for a new Computing Infrastructure. Morgan Kaufmann, 1999.
[24] Pulina L,. A Swarm Intelligence Approach for Biometrics Verification and Identification
Veeramachaneni K, Ann Osadciw Land Varshney P.K, Adaptive Multimodal Biometric Fusion Algorithm Using Particle Swarm