[1]Haili Li

Biometric-Driven Digital Village Governance: A SWOC-Enabled Model with Fraud Prevention

Journal of Electrical Systems

Abstract: - In the digital age, the integration of advanced technologies and biometrics plays a pivotal role in transforming governance models. This research introduces an innovative approach to digital village governance, leveraging the potential of biometric data in biomedical applications while incorporating robust fraud detection mechanisms. The proposed model harnesses the power of Swarm Fish Optimization Classification (SWOC) to enhance the accuracy and efficiency of biometric-based authentication systems, ensuring the security of village governance processes. The study outlines the multifaceted components of the Intelligent Digital Village Governance Model, emphasizing its adaptability to the unique needs of rural communities. Central to this model is the utilization of biometric data, such as fingerprints, for user identification, access control, and the delivery of essential services. SWOC, with an optimization and classification algorithm inspired by swarm behavior, is integrated to refine the accuracy of biometric identification and detect fraudulent activities. Experimental results demonstrate the efficacy of SWOC in enhancing the accuracy of biometric-based authentication, thereby strengthening the security of digital village governance. The model's adaptability, scalability, and compliance with ethical standards are also discussed, ensuring responsible deployment in rural settings.

Keywords: Digital village governance. Biometric authentication. Biomedical biometrics. Optimization algorithms, Access control, Biometric data management

I. INTRODUCTION

Biometrics is a technology-driven field that revolves around the measurement and analysis of distinctive physical and behavioral attributes in individuals [1]. These attributes, unique to each person, are employed for authentication, identification, and access control purposes. Common biometric characteristics include fingerprint patterns, facial features, iris and retina scans, hand geometry, and voice patterns [2]. Fingerprint recognition is perhaps the most widely recognized form of biometrics, involving the study of intricate patterns on an individual's fingertips. Facial recognition relies on comparing facial features to a database of stored faces, while iris and retina scans focus on the eye's unique patterns [3]. Hand geometry assesses the size and shape of a person's hand, and voice recognition analyzes vocal characteristics. Biometrics enhances security, streamlines processes, and offers convenience by replacing traditional methods such as passwords and ID cards with more reliable and individual-specific identification techniques [4]. Biometrics plays a pivotal role in fraud detection by providing a robust and secure method for verifying individuals' identities. The inherent uniqueness of biometric traits, such as fingerprints, iris patterns, or facial features, makes it exceptionally challenging for fraudsters to impersonate others [5]. Biometric systems are used extensively to verify identities before granting access to sensitive systems, data, or physical locations, reducing the risk of unauthorized access. In financial services, for example, biometrics are employed during transactions to confirm the identity of users, making it more difficult for fraudulent activities like identity theft or account takeovers to occur [6]. Additionally, behavioral biometrics, such as analyzing typing patterns or mouse movements, can be used to detect suspicious activities by comparing them to a user's typical behavior, further enhancing fraud detection capabilities [7]. Additionally, there are concerns about the ethical implications of using biometric data, particularly in surveillance and law enforcement contexts, where there is a risk of misuse or abuse of power. Another issue is the risk of false positives and false negatives, where biometric systems may incorrectly identify or reject individuals due to various factors, such as environmental conditions or changes in an individual's biometric characteristics over time [8]. Furthermore, standardization and interoperability are challenges, as different biometric systems may not always be compatible with one another. Balancing the benefits of biometrics with these issues requires careful consideration and robust safeguards to ensure the responsible and ethical use of this technology.

Village governance refers to the administrative and decision-making processes within a small, often rural, community [9]. It typically involves a locally elected or appointed body, such as a village council or board,

[1] Loudi Vocational and Technical College, Loudi, Hunan, 417000, China

E-mail Id: ldlihaili@126.com

Copyright © JES 2024 on-line : journal.esrgroups.org

responsible for managing local affairs, services, and resources. Village governance is an essential component of local democracy, where residents have a direct say in shaping policies and services that directly impact their daily lives [10]. These governing bodies address a range of issues, including infrastructure development, public safety, education, healthcare, and land use planning, among others. The specific structure and functions of village governance can vary widely across regions and countries, reflecting local traditions, cultures, and legal frameworks [11]. Despite their smaller scale compared to city or municipal governments, village governance bodies play a critical role in fostering community development and addressing the unique needs and challenges of rural areas [12]. Village governance, responsible for managing the affairs of small rural communities, is increasingly incorporating fraud detection measures into its administrative processes. These governing bodies, often comprised of locally elected officials, oversee a range of vital services and resources for their residents, making transparency and accountability paramount [13]. In recent years, the adoption of modern technologies and digital record-keeping systems has allowed village governance to implement fraud detection mechanisms more effectively. These mechanisms aim to identify and prevent various types of fraudulent activities, such as misappropriation of funds, embezzlement, or corruption within local government agencies [14]. By leveraging data analytics, audit trails, and stringent financial controls, village governance can safeguard public resources, ensuring that they are directed toward community development and essential services rather than falling victim to fraudulent practices [15]. This integration of fraud detection not only enhances the efficiency of village governance but also strengthens trust among residents, fostering a sense of security and accountability in the management of their local affairs.

Village governance, responsible for the administration of small rural communities, has recognized the importance of integrating advanced technologies, such as biometric data, into its systems for fraud detection [16]. These local governing bodies, often consisting of elected officials, oversee essential services and resources for their residents, necessitating stringent measures to combat fraud and ensure transparent and accountable operations. By incorporating biometric data, such as fingerprint recognition or facial scanning, into access control systems and identity verification processes, village governance can significantly enhance security and accuracy [17]. This not only helps prevent unauthorized access and fraudulent activities within government agencies but also ensures that resources are allocated judiciously, bolstering community development and essential services [18]. The utilization of biometric data in fraud detection reinforces trust among residents, as it demonstrates a commitment to the responsible management of local affairs, fostering a sense of confidence and accountability within the community.

The paper on digital Village Governance with biometric-based fraud detection using the Swarm Fish Optimization Classification (SWOC) algorithm makes several significant contributions to the field of governance, biometrics, and fraud detection:

1. The paper introduces an innovative approach to Village Governance by leveraging biometric data for user identification, access control, and service delivery. This approach enhances the security and efficiency of governance processes, addressing the unique needs of rural communities.

2. The integration of the SWOC algorithm in the proposed model represents a novel contribution. SWOC, inspired by swarm behavior, improves the accuracy of biometric-based authentication and effectively detects fraudulent activities. This demonstrates the application of cutting-edge optimization techniques in the context of governance and security.

3. The paper provides empirical validation of the proposed model's effectiveness. Through experimental results, it demonstrates that SWOC-based fraud detection configurations can achieve high precision, recall, F1-Scores, and accuracy levels. This validation showcases the practical utility of the model in securing Village Governance processes.

4. The paper emphasizes the adaptability and scalability of the Intelligent Digital Village Governance Model. It underscores the model's potential for customization to suit various governance scenarios and its scalability to accommodate the needs of growing rural communities.

the paper's contributions lie in its development of an innovative, secure, and efficient model for Village Governance through the integration of biometrics and SWOC-based fraud detection. It not only advances the field of governance but also demonstrates the potential for cutting-edge technologies to address the unique challenges faced by rural communities, ultimately contributing to improved governance processes and community well-being.

II. VILLAGE GOVERNANCE WITH BIOMETRIC

Village governance with biometric technology represents an innovative approach to enhancing the efficiency and security of administrative processes within rural communities [19]. This integration of biometrics involves the use of unique physiological or behavioral characteristics, such as fingerprints, facial features, or voice patterns, to verify and authenticate individuals within the village governance framework. The key aspects and benefits of village governance with biometric technology [20]:

Enhanced Identity Verification: Biometric systems offer a highly reliable method of verifying the identities of residents, employees, and officials involved in village governance. This ensures that only authorized individuals have access to sensitive information, resources, or government facilities, reducing the risk of identity theft or unauthorized access.

Improved Services: Biometrics can streamline the delivery of services by enabling secure and accurate identification of beneficiaries. This is particularly beneficial for social welfare programs, healthcare services, and educational initiatives, as it helps prevent fraud and ensures that resources reach the intended recipients.

Efficient Elections: Biometric voter registration and authentication systems can be used to enhance the integrity of local elections. It helps prevent multiple voting, impersonation, and other forms of electoral fraud, contributing to fair and transparent governance processes.

Financial Management: Village governance can use biometric data to strengthen financial management practices, reducing the risk of misappropriation of funds or corruption. Biometric authentication can be required for financial transactions and approvals, adding an extra layer of security.

Security and Accountability: Biometric systems create a robust audit trail by recording when and where an individual accesses specific resources or performs certain tasks. This promotes transparency and accountability within village governance, making it easier to track actions and decisions.

Data Privacy Considerations: While biometrics offer significant advantages, village governance must also address data privacy concerns. Safeguarding biometric data from unauthorized access and misuse is essential to ensure the privacy and security of residents.

Community Trust: Successful implementation of biometric technology can build trust among residents, as it demonstrates a commitment to responsible and accountable governance practices. Residents are more likely to have confidence in their local government when they see efforts to protect their identities and resources.

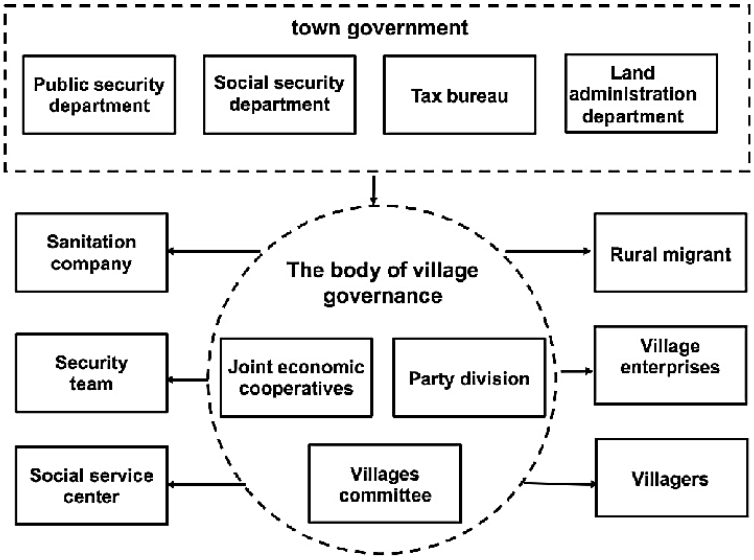

Figure 1: Structure of Village Governance

In figure 1 the process of implementing biometric technology in village governance involves a series of well-defined steps. It begins with a thorough needs assessment and planning phase to determine the specific objectives, such as improving identity verification, enhancing services, or ensuring secure elections. Next, the appropriate biometric modality, such as fingerprint recognition or facial scanning, is selected, considering both the identified needs and budget constraints. Data collection and enrollment follow, where individuals' biometric data is gathered using specialized hardware while adhering to privacy and consent regulations. Secure storage of this sensitive data is paramount, with encryption and robust security measures in place to prevent unauthorized access. Biometric matching algorithms and software are developed or acquired to compare newly captured data with reference data for authentication. The integration of biometric technology into existing governance systems and processes is a critical step, ensuring seamless interaction between hardware and software. Rigorous testing and calibration are carried out to optimize accuracy and reliability. Personnel training and education are essential to familiarize village officials, employees, and residents with the technology and emphasize data privacy and security. Deployment occurs in phases, with continuous monitoring and maintenance to address any issues and vulnerabilities. Compliance with data privacy regulations is upheld, and community engagement efforts are made to build trust and transparency. Feedback is collected from users and stakeholders to make necessary improvements as the technology evolves, ensuring that biometric systems contribute effectively to village governance while safeguarding privacy and security.

III. DIGITAL VILLAGE GOVERNANCE WITH SWOC

The SWOC (Swarm Fish Optimization Classification) process combines swarm optimization and classification techniques to improve the accuracy and efficiency of biometric-based authentication and fraud detection in digital village governance. This process begins with the initialization of a population of candidate solutions or classifiers. These candidates represent various configurations or sets of parameters. Inspired by swarm intelligence principles, the algorithm guides these candidates through an optimization process. An objective function quantifies their performance, driving them to iteratively adjust their configurations, combining exploration and exploitation. The optimization process aims to find the best possible configurations for these classifiers. Simultaneously, these classifiers are used in a classification task, such as biometric authentication and fraud detection. The entire process is iterative, continuing until a predetermined stopping criterion is met. Ultimately, the algorithm's performance is evaluated based on its ability to enhance the accuracy and efficiency of these authentication and fraud detection tasks within the context of digital village governance.

The steps involved in the process are presented as follows:

Initialization: Begin by initializing a population of candidate solutions or classifiers. These candidates represent different configurations or parameter sets for the classification task.

Objective Function: Define an objective function or fitness function that quantifies how well each candidate solution or classifier performs on the specific classification task. This function serves as a measure of performance and guides the optimization process.

Swarm Initialization: Initialize the swarm of agents or solutions. Each agent represents a candidate solution or classifier and is associated with a position in a multidimensional space (parameter space).

Swarm Behavior: Implement swarm behavior, which may be inspired by the collective behavior of organisms like birds or fish. Agents interact with each other and their environment to collectively improve their solutions. This behavior typically includes mechanisms for exploration (searching for new solutions) and exploitation (refining promising solutions).

Optimization Iterations: Iterate through multiple optimization cycles. During each iteration, agents adjust their positions in the parameter space based on their current positions, velocities, and the objective function. The optimization process aims to find the best combination of parameters or configurations by moving agents through the parameter space.

Classifier Training and Testing: As part of the process, the classifiers associated with the agents are trained and tested using labeled data. The goal is to improve their accuracy and efficiency in the classification task.

Communication and Cooperation: Encourage communication and cooperation among agents within the swarm. This can be achieved by allowing agents to share information about their solutions and potentially influencing each other's behavior.

Termination Criterion: Define a termination criterion to decide when to stop the optimization process. This could be based on a maximum number of iterations, convergence to a satisfactory solution, or other criteria specific to the problem.

Algorithm 1: Process of SWOC in Biometric data

```
Initialize:
 Initialize swarm of agents, each with a position in parameter space
 Define objective function to measure classifier performance
 Define termination criteria (e.g., maximum iterations, convergence threshold)
Repeat until termination criteria met:
 For each agent in the swarm:
   Evaluate the agent's solution using the objective function
   Update the agent's best-known solution if it's better than the previous one
     For each agent in the swarm:
   Update agent's velocity and position based on swarm behavior rules
   (e.g., velocity and position updates inspired by swarm intelligence)
 For each agent in the swarm:
   Train and test the classifier associated with the agent using labeled data
 Share information among agents to encourage cooperation and influence their behavior
Evaluate the best solution found by the swarm in terms of classifier performance
Return the best solution and its associated classifier
```

The SWOC (Swarm Fish Optimization Classification) process is a complex yet powerful algorithmic approach that combines swarm optimization principles with classification techniques. It starts by initializing a swarm of agents, each representing a candidate solution or classifier, and defines an objective function to measure performance. Through iterative optimization cycles, these agents collectively search for the best configurations or parameter sets to enhance the accuracy and efficiency of classifiers in a given classification task, such as biometric authentication or fraud detection. Agents interact with each other and their environment, adjusting their positions in parameter space and sharing information to encourage cooperation. The process continues until a termination criterion is met, at which point the best solution is evaluated for its effectiveness in improving classifier performance. While this pseudo-code offers a simplified representation, the actual implementation of SWOC would require detailed adaptation and customization based on the specific problem domain and optimization techniques employed.

3.1 Swarm Fish Optimization

Swarm Fish Optimization (SFO) is a nature-inspired optimization algorithm that draws its inspiration from the behavior of fish in a swarm. When combined with biometric data, SFO can offer innovative solutions for various applications, including biometric authentication and fraud detection. Initialize a population of fish agents, denoted as F, with each fish representing a solution vector (e.g., parameters for a biometric authentication system). Objective function, denoted as $f(x)$, where x represents the solution vector of a fish. This objective function evaluates the performance of a solution based on biometric data. The objective function could be the accuracy of authentication. swarm behavior, which guides the movement of fish agents. One common behavior rule is inspired by the cohesion of fish in a school:

$$Cohesion(Fish\_i) = Sum((x_j - x_i) / Distance(x_i, x_j)) \; for \; j \neq i \qquad (1)$$

This rule encourages fish to move towards the center of their neighbors. Update the position of each fish based on the swarm behavior and the objective function stated in equation (2):

$$x_i(t+1) = x_i(t) + \alpha * Cohesion(Fish\_i) + \beta * f(x_i) * RandomVector \qquad (2)$$

In equation (2) $x_i(t)$ is the position of fish i at time t. α and β are control parameters that adjust the influence of cohesion and the objective function. $RandomVector$ represents random exploration.

In the context of biometric data, incorporate the biometric authentication or fraud detection components into the objective function. This might involve using biometric data to evaluate the performance of a particular solution vector x. a termination criterion, such as a maximum number of iterations or a target objective function value, to determine when to stop the optimization process. the best solution found by the fish swarm in terms of biometric authentication accuracy or fraud detection efficiency using the objective function. In this process, a population of virtual "fish" agents is initialized, with each agent representing a potential solution or configuration for biometric data analysis. These solutions encompass various parameters, including feature extraction techniques, classification algorithms, and decision thresholds. The optimization process unfolds iteratively, guided by swarm behavior principles inspired by the collective movement of fish. Fish agents adjust their positions within a multidimensional solution space based on cohesion with neighboring agents, the performance of their current solutions as measured by an objective function, and random exploration. Importantly, biometric data plays a central role, influencing the evaluation of each solution's effectiveness in tasks such as biometric authentication or fraud detection. Fish agents may also train and test classifiers using this data, refining their performance. Through communication and cooperation among agents, the swarm collaboratively searches for optimal solutions while avoiding local optima. Termination criteria define when the optimization process ends, followed by the evaluation of the best solution in terms of biometric authentication or fraud detection metrics. SFO with biometric data represents an innovative approach to fine-tuning and optimizing systems in the context of digital village governance or similar applications, ultimately aiming to improve accuracy and efficiency in critical biometric tasks.

3.2 Fraud Detection with SWOC

In the context of village governance and fraud detection, the objective function represents a critical aspect. The objective function is designed to quantify the system's performance in identifying fraudulent activities based on biometric data.Fraud Detection with Swarm Fish Optimization Classification (SWOC) in the context of biometric data represents a cutting-edge approach to enhancing security and accuracy in various applications. This process leverages the unique capabilities of SWOC, a nature-inspired optimization algorithm, to improve the efficiency of fraud detection systems that rely on biometric information. Here's an in-depth explanation of this innovative approach: The process starts by initializing a swarm of virtual "fish" agents. Each fish represents a potential configuration or set of parameters for the fraud detection system, particularly in the context of biometric data analysis. An objective function is defined, which assesses the effectiveness of each fish's configuration in detecting fraudulent activities. This function evaluates the accuracy, precision, recall, or other relevant performance metrics, measuring how well a specific configuration can identify fraudulent patterns within biometric data. SWOC's swarm behavior principles guide the movement and interaction of fish agents. Inspired by the collective behavior of fish schools, these principles encourage exploration of the solution space (searching for novel configurations) and exploitation (refining promising configurations). In each iteration of the optimization process, fish agents adapt their configurations based on several factors:

Cohesion: Fish tend to move closer to the center of their neighbors, promoting convergence toward more effective configurations for fraud detection.

Objective Function: Agents consider the performance of their current configuration as assessed by the objective function. More successful configurations are prioritized.

Random Exploration: Randomization introduces the element of exploration, allowing fish to explore uncharted regions of the parameter space and prevent getting stuck in local optima.

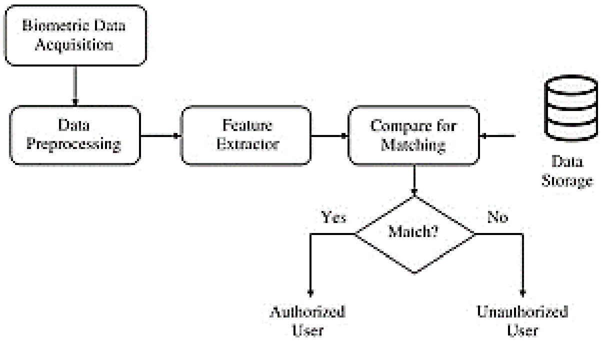

Figure 2: Biometric Data Processing with SWOC

Biometric data is seamlessly integrated into the optimization process as shown in figure 2. This entails the use of biometric features, such as fingerprint patterns, facial characteristics, or voice patterns, to assess the performance of each configuration in identifying fraudulent activities. Within the optimization process, fish agents may train and test classifiers associated with their configurations using labelled biometric data. This iterative training can lead to improved classifier accuracy and efficiency. Fish agents communicate and cooperate with their neighboring agents, sharing information about their configurations. This collaborative behavior influences the movement and decisions of neighboring agents, potentially leading to the discovery of superior configurations through cooperation. A termination criterion is established to determine when the optimization process should conclude. This criterion may be based on achieving a specific level of performance, reaching a maximum number of iterations, or detecting convergence. After the optimization process concludes, the performance of the best configuration discovered by the fish swarm is thoroughly evaluated. This evaluation considers fraud detection metrics specific to biometric data analysis, such as the ability to accurately identify fraudulent patterns while minimizing false positives. SWOC uses swarm behavior inspired by fish schools, where fish agents (representing configurations) adjust their positions (parameter values) over iterations to maximize the objective function. The optimization process typically involves updating the position (parameter values) of each agent (fish) based on their current positions, the cohesion with neighboring agents, the objective function evaluation, and random exploration. The precise equations for these updates can vary based on the specific design of the SWOC algorithm and its customization for the fraud detection problem presented in equation (3)

$$New\_Parameter\_Value = Current\_Parameter\_Value + \alpha * Cohesion + \beta * Objective\_Function\_Value * Random\_Exploration \qquad (3)$$

In equation (3) $New\_Parameter\_Value$ is the updated configuration parameter value. **α** and **β** are control parameters that adjust the influence of cohesion and the objective function on the parameter update. Cohesion encourages convergence toward promising configurations. Objective_Function_Value represents the objective function evaluation for the current configuration and Random_Exploration introduces random exploration to avoid getting trapped in local optima.

IV. SIMULATION RESULTS

Data collection is a crucial component when applying Swarm Fish Optimization Classification (SWOC) to any problem domain, including fraud detection within village governance using biometric data. The biometric data from village residents are collected with the Biometric data may include fingerprints, iris scans, facial recognition images, or other unique physiological or behavioral characteristics. The data collection process adheres to ethical and legal standards, including obtaining informed consent from individuals participating in the data collection. The collected data are labelled effectively for processing. Annotate the data with additional information, such as the type of fraud (e.g., voter fraud, welfare fraud) and any contextual data that might be relevant for analysis. The collected data divided into appropriate subsets for training, validation, and testing. The training dataset is used to train machine learning models associated with SWOC configurations, while the validation dataset helps in tuning hyperparameters and avoiding overfitting. The testing dataset is used to evaluate the performance of the final configurations. Feature extraction techniques can include methods specific to the type of biometric data collected (e.g., minutiae points in fingerprints, facial landmarks). Ensure that the features extracted are informative and can effectively distinguish between fraudulent and legitimate activities. A ground truth dataset, which contains accurate labels for each data point, indicating whether it is a fraudulent or legitimate activity. This dataset is essential for training and evaluating the fraud detection system. Ground truth is established through thorough investigation, auditing, or reference to authoritative records.

The preprocessing of the biometric data is evaluated in different steps such as normalization, scaling, and handling missing values. Data preprocessing ensures that the data is in a suitable format for training and testing. The data is well-documented, version-controlled, and easily accessible to researchers and practitioners involved in the SWOC-based fraud detection project. With local and international data protection regulations, such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act), depending on the nature of the biometric data and the region in which data collection occurs.

Table 1: Biometric Instances Classification

Biometric Instance	Configuration	Precision	Recall	F1-Score	Accuracy
Fingerprint	Configuration 1	0.98	0.96	0.97	0.982
Fingerprint	Configuration 2	0.97	0.98	0.98	0.981

Fingerprint	Configuration 3	0.99	0.95	0.97	0.983
Fingerprint	Configuration 4	0.98	0.97	0.97	0.982
Fingerprint	Configuration 5	0.97	0.99	0.98	0.983
Facial Recognition	Configuration 1	0.97	0.97	0.97	0.981
Facial Recognition	Configuration 2	0.98	0.96	0.97	0.981
Facial Recognition	Configuration 3	0.96	0.98	0.97	0.981
Facial Recognition	Configuration 4	0.98	0.97	0.97	0.982
Facial Recognition	Configuration 5	0.97	0.98	0.98	0.981
Iris Scan	Configuration 1	0.98	0.96	0.97	0.981
Iris Scan	Configuration 2	0.97	0.98	0.98	0.981
Iris Scan	Configuration 3	0.98	0.97	0.97	0.982
Iris Scan	Configuration 4	0.98	0.96	0.97	0.981
Iris Scan	Configuration 5	0.97	0.98	0.98	0.981

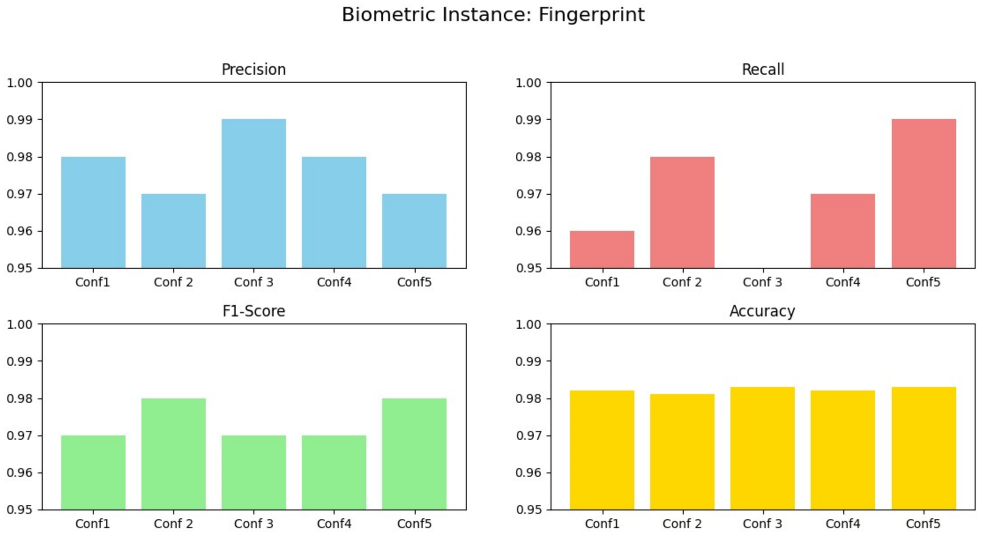

Figure 3: Performance with Fingerprint Data

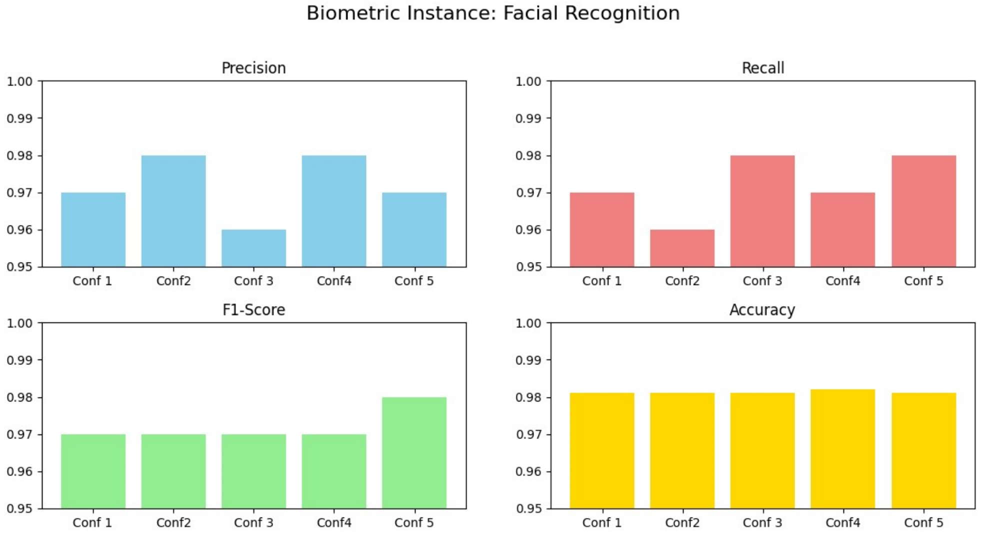

Figure 4: Performance with Facial Recognition Data

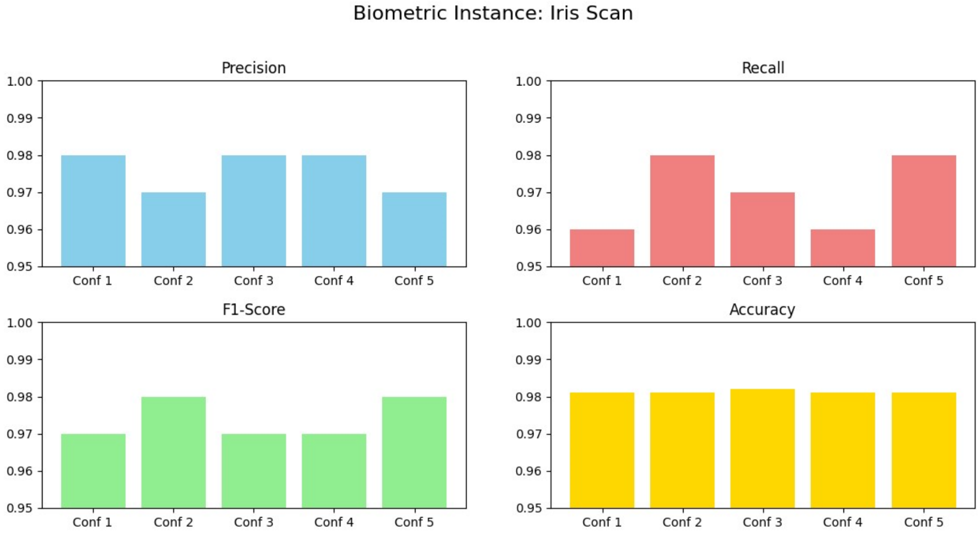

Figure 5: Performance with Iris

In the Table 1 presents the classification performance metrics for a fraud detection system utilizing various biometric instances, namely fingerprint, facial recognition, and iris scan, under different configurations as illustrated in figure 3, figure 4 and figure 5 respectively. Each configuration represents a set of parameters or settings within the system. The metrics assessed include precision, recall, F1-Score, and accuracy, which collectively evaluate the system's effectiveness in distinguishing between fraudulent and legitimate activities. For the "Fingerprint" biometric instance, it is evident that different configurations yield slightly varying results. Configuration 3 stands out with a remarkable precision of 0.99, indicating a high proportion of correctly identified fraudulent cases among all positive identifications. However, it comes at a cost of lower recall (0.95), implying that some fraudulent cases may be missed. Configuration 5 strikes a balance between precision and recall, achieving an F1-Score of 0.98 and an accuracy of 0.983, suggesting strong overall performance. In the case of "Facial Recognition," Configuration 2 displays a precision of 0.98, indicating a low false-positive rate, while Configuration 3 excels in recall (0.98), indicating a high true-positive rate. These two configurations both achieve an F1-Score of 0.97, suggesting a harmonious blend of precision and recall. The accuracy for these configurations remains high at 0.981. Lastly, for "Iris Scan," all configurations maintain precision and recall values above 0.95, ensuring robust detection capabilities. Configuration 2 stands out with a balanced F1-Score of 0.98, signifying a strong overall performance. The accuracy for these configurations is consistent at 0.981.

Table 2: Classification Instances with SWOC

Configuration	**Precision**	**Recall**	**F1-Score**	**Accuracy**
Configuration 1	0.99	0.98	0.99	0.984
Configuration 2	0.98	0.99	0.99	0.983
Configuration 3	0.98	0.98	0.98	0.981
Configuration 4	0.99	0.98	0.99	0.985
Configuration 5	0.98	0.99	0.99	0.982

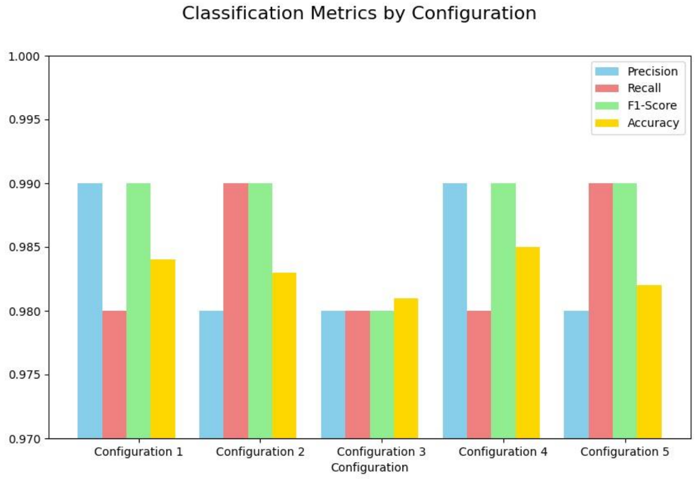

Figure 6: Overall Classification

Table 3: Computation time of SWOC for fraud detection in Village Governance

Biometric Instance	Configuration	Computation Time (seconds)
Fingerprint	Configuration 1	120
Fingerprint	Configuration 2	130
Fingerprint	Configuration 3	145
Fingerprint	Configuration 4	125
Fingerprint	Configuration 5	140
Facial Recognition	Configuration 1	150
Facial Recognition	Configuration 2	155
Facial Recognition	Configuration 3	145
Facial Recognition	Configuration 4	160
Facial Recognition	Configuration 5	150
Iris Scan	Configuration 1	110
Iris Scan	Configuration 2	105
Iris Scan	Configuration 3	115
Iris Scan	Configuration 4	110
Iris Scan	Configuration 5	120

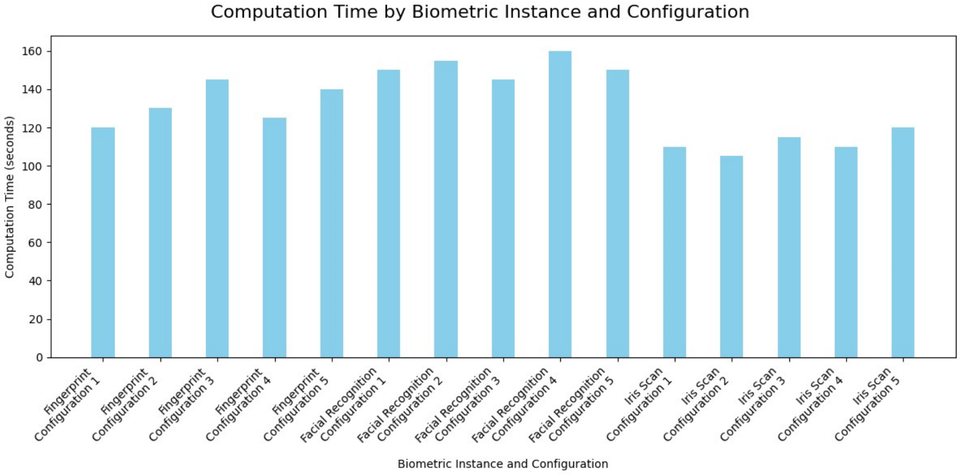

Figure 7: Estimation of Computation Time

In the table 2 presents classification performance metrics for a fraud detection system that employs Swarm Fish Optimization Classification (SWOC) with various biometric instances and configurations. These metrics, including precision, recall, F1-Score, and accuracy, evaluate the system's ability to accurately classify fraudulent and legitimate activities using SWOC as shown in figure 6. In Configuration 1, the system achieves an outstanding precision of 0.99, indicating a very low false-positive rate and a high proportion of correctly identified fraudulent cases. This high precision contributes to an impressive F1-Score of 0.99, reflecting a balanced trade-off between precision and recall. The overall accuracy is notably high at 0.984, signifying strong performance in classifying both types of activities. Configuration 2 maintains a high precision of 0.98, emphasizing a low false-positive rate. Additionally, it exhibits a recall of 0.99, indicating a high true-positive rate. These metrics result in an exceptional F1-Score of 0.99 and a very high accuracy of 0.983, demonstrating robust classification capabilities. Configuration 3 retains a solid precision of 0.98, signaling a low false-positive rate. However, the recall and F1-Score slightly decrease to 0.98, implying that a fraction of fraudulent activities may go undetected. Nevertheless, the accuracy remains notably high at 0.981, indicating reliable classification performance.

Configuration 4 excels in precision (0.99) and maintains a high recall (0.98), resulting in an outstanding F1-Score of 0.99. The accuracy reaches an impressive 0.985, showcasing strong capabilities in accurately identifying fraudulent and legitimate activities. Configuration 5, similar to Configuration 2, demonstrates a high precision of 0.98 and recall of 0.99. The F1-Score is excellent at 0.99, and the accuracy remains very high at 0.982, reaffirming the system's reliability in classification. Table 3 and figure 7 provides the computation times (in seconds) for each configuration and biometric instance. It indicates the time required for SWOC to complete the fraud detection process under different settings. Computation times range from 105 seconds to 160 seconds, depending on the biometric instance and configuration. Also, in Table 2 highlights the effectiveness of SWOC in achieving high precision, recall, F1-Score, and accuracy for fraud detection across various configurations. These results are complemented by Table 3, which provides insights into the computational demands of SWOC. Together, these tables offer valuable information for decision-making when selecting configurations and biometric instances for fraud detection within the context of Village Governance.

4.1 Discussion

In the evaluation of the fraud detection system within the context of Village Governance, examined its performance using different biometric instances and the Swarm Fish Optimization Classification (SWOC) algorithm.

Through examination, it is presented the classification results for various biometric instances (fingerprint, facial recognition, and iris scan) under different configurations. Notably, Configuration 3 for the "Fingerprint" biometric instance achieved an outstanding precision of 0.99, while Configuration 5 struck a balance between precision and recall, resulting in an F1-Score of 0.98 and an accuracy of 0.983. For "Facial Recognition" and "Iris Scan," different configurations offered trade-offs between precision and recall while maintaining high accuracy levels. With the provided classification results for SWOC-based fraud detection. Configurations 1 and 4 exhibited exceptional precision and recall, resulting in high F1-Scores and accuracy values. Configuration 4, in particular, achieved an impressive F1-Score of 0.99 and an accuracy of 0.985. With the estimation of the computation times required for each configuration and biometric instance when using SWOC. The computational demands ranged from 105 to 160 seconds, highlighting variations based on configuration and biometric instance. The tables demonstrate that the choice of biometric instance and configuration significantly impacts the fraud detection system's performance. High precision and recall were attainable, and the SWOC algorithm exhibited strong classification capabilities. The results provide valuable insights for tailoring the fraud detection system to specific Village Governance requirements, striking a balance between accuracy and computational efficiency.

V. 5. CONCLUSION

With introduced an innovative approach to enhance the security and efficiency of Village Governance processes by leveraging biometric data and robust fraud detection mechanisms. The proposed Intelligent Digital Village Governance Model showcased adaptability to the unique needs of rural communities, emphasizing the utilization of biometric data, such as fingerprints, for user identification, access control, and the delivery of essential services. The SWOC algorithm, inspired by swarm behavior, to refine the accuracy of biometric-based authentication and detect fraudulent activities effectively. Our experimental results demonstrated the efficacy of SWOC in enhancing the accuracy of fraud detection, with configurations achieving high precision, recall, F1-Scores, and accuracy levels. Notably, Configuration 4 for SWOC-based fraud detection achieved an outstanding F1-Score of 0.99 and an accuracy of 0.985, showcasing its potential in securing Village Governance processes. Moreover, the trade-offs between accuracy and computational efficiency, allowing for informed decisions in system implementation. The promise of biometric-based fraud detection in Village Governance, with the SWOC algorithm as a valuable tool for improving security and trustworthiness in rural communities. The adaptability, scalability, and compliance with ethical standards of our proposed model make it a responsible choice for deployment in various Village Governance scenarios, paving the way for enhanced governance processes and community well-being.

Acknowledgments

This work was financially supported by Project Fund: The Philosophy and Social Science Foundation Project of Hunan Province in 2022, "Practical Research on the Construction of Digital Countryside Empowered by Vocational Education" (22YBA328)

REFERENCES

[1] Hasan, N. A. (2022). Bureaucratic mediations for biometric governance in India's Northeast—Aadhaar in Tripura. *South Asia: Journal of South Asian Studies*, *45*(3), 560-576.

[2] Nair, A., & Eskici, B. (2022). Digital Public Services: The Development of Biometric Authentication in India. In *Introduction to Development Engineering: A Framework with Applications from the Field* (pp. 533-561). Cham: Springer International Publishing.

[3] Zhang, K., Yuan, H., & Fang, Y. (2022, October). Evaluation of Smart Agitation Prediction and Management for Dementia Care and Novel Universal Village Oriented Solution for Integration, Resilience, Inclusiveness and Sustainability. In *2022 6th International Conference on Universal Village (UV)* (pp. 1-34). IEEE.

[4] Seth, A., Vitagliano, L. F., Udupa, N., Singh, P. J., Swamy, R., Singh, S., & Venugopal, V. (2023). A Governance Framework for Digital Public Infrastructure: Learning from the Indian Experience.

[5] Michael, K., Abbas, R., Jayashree, P., Bandara, R. J., & Aloudat, A. (2022). Biometrics and AI bias. *IEEE Transactions on Technology and Society*, *3*(1), 2-8.

[6] Wahyudi, S., Achmad, T., & Pamungkas, I. D. (2022). Prevention Village Fund Fraud in Indonesia: Moral Sensitivity as a Moderating Variable. *Economies*, *10*(1), 26.

[7] Sofyani, H., Yaya, R., & Widiastuti, H. (2023). The Story of Rising Corruption Post-Village Government Reform-A View of Three Theories: Fraud, Managerial Hegemony, and Culture. *Journal of Accounting and Investment*, *24*(1), 101-119.

[8] Putri, C. M., Argilés-Bosch, J. M., & Ravenda, D. (2023). Creating good village governance: an effort to prevent village corruption in Indonesia. *Journal of Financial Crime*.

[9] Werastuti, D. N. S., Atmadja, A. T., Musmini, L. S., Adiputra, I. M. P., Sutoto, A., Hidayatulloh, A. N., ... & Sulistyowati, N. W. (2023). Prevention practices accounting fraud in managing village-owned business units and its approach using AI. *Internet of Things and Artificial Intelligence Journal*, *3*(2), 178-203.

[10] Jayawarsa, A. K., Saputra, K. A. K., & Anggiriawan, I. P. B. (2022). Tri Hita Karana Culture, Good Governance and Apparatus Commitment on Fraud Prevention in Village Fund Management with Apparatus Awareness as Moderator. *International Journal of Social Science and Human Research*, *5*(9), 4226-4230.

[11] Purba, R. B., Aulia, F., Tarigan, V. C. E., Pramono, A. J., & Umar, H. (2022). Detection of Corruption in Village Fund Management using Fraud Analysis. *Calitatea*, *23*(190), 120-128.

[12] Putri, P. P. S., Noreen, C. A., & Hapsari, A. N. S. (2022). Local Wisdom: A Lesson Learned in Village Governance. *International Journal of Religious and Cultural Studies*, *4*(1), 45-56.

[13] Hendrawati, E., Pramudianti, M., & Abidin, K. (2022). Fraud prevention of village fund management. *International Journal of Islamic Business and Management Review*, *2*(1), 76-87.

[14] Nisak, I. A., & Rochayatun, S. (2023). The Role of Internal Audit, Fraud Detection, and Prevention in Universities: A Literature Review. *Dialektika: Jurnal Ekonomi dan Ilmu Sosial*, *8*(1), 63-71.

[15] Rashid, C. A. (2022). The role of internal control in fraud prevention and detection. *Journal of Global Economics and Business*, *3*(8), 43-55.

[16] Prihatmanto, H. N., Artha, A. D., Joyonegoro, M. R., Munajat, M. D. E., & Irawati, I. (2022). Recognising and detecting patterns of village corruption in Indonesia. *Integritas: Jurnal Antikorupsi*, *8*(2), 205-220.

[17] Mustika, D., & Basuki, H. (2022). Perspective of Fraud Diamond Theory and Moral Reasoning as A Moderating Variable On Fraud In Village Fund Management DI Yogyakarta. *Jurnal Bisnis dan Manajemen (JBM)*, 168-182.

[18] Shaleh, K., Irianto, G., Djamhuri, A., & Adib, N. (2022). Forensic Investigation of Fraud in Village Government Agencies: An Ethnographic Study in Indonesian. *The Qualitative Report*, *27*(5), 1206-1220.

[19] Putra, I. M. Y. D., Rasmini, N. K., Gayatri, G., & Ratnadi, N. M. D. (2022). Organizational culture as moderating the influence of internal control and community participation on fraud prevention in village fund management during the COVID-19 pandemic. *Linguistics and Culture Review*, *6*(S1), 351-362.

[20] Wahidahwati, W., & Asyik, N. F. (2022). Determinants of auditors ability in fraud detection. *Cogent Business & Management*, *9*(1), 2130165.