IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 23, 2021, accepted January 12, 2022, date of publication January 18, 2022, date of current version January 24, 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3144145*

# Template Aging in Multi-Modal Social Behavioral Biometrics

**SANJIDA NASREEN TUMPA AND MARINA L. GAVRILOVA, (Senior Member, IEEE)**
Department of Computer Science, University of Calgary, Calgary, AB T2N 1N4, Canada

Corresponding author: Sanjida Nasreen Tumpa (sanjidanasreen.tumpa@ucalgary.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada by the Discovery Grant (DG) on Machine Intelligence for Biometric Security under Grant 10007544, in part by the Strategic Partnership Grant on Biometric-Enabled Identity Management and Risk Assessment for Smart Cities under Grant 10022972, and in part by IDEaS Collaborative Project 10027075.

**ABSTRACT** The uniqueness of social interactions on online social networks draws attention to cybersecurity research. Social Behavioral Biometric (SBB) systems extract unique patterns from online communication traits trails and generate digital fingerprints for user identification. However, with time those behavioral patterns change. These affect the authentication ability of a SBB system. In this paper, we have combined for the first time textual, contextual and interpersonal communicative information of users in online social networks to develop a biometric system. The SBB traits are combined using the weighted sum rule score level fusion algorithm with the genetic algorithm employed to choose the feature weights. The effects of template aging on the individual SBB traits and overall system have been analyzed for the first time. The proposed system achieves the recognition accuracy of 99.25% and outperforms all prior research on SBB. The experimental results on permanence evaluation demonstrate that the developed system can perform remarkably well despite the template aging effect.

**INDEX TERMS** Feature fusion, feature permanence, genetic algorithm, online social network, natural language processing, social behavioral biometrics, template aging, user identification.

## I. INTRODUCTION

Over the past decade, exploring human behavior as biometric traits has gained popularity [1]. The ways a person walks, talks, interacts with others, writes, authenticates documents are unique and inherently difficult to imitate [2]. In addition to traditional forms of biometrics such as face, gait and iris, emerging research has focused on technologies that measure signals generated directly or indirectly by human thought processes. Examples of those biometrics include Electroencephalography (EEG) brain signal [3], linguistic style [4], keystroke dynamics [5], mouse movement [6], eye tracking [7], etc. The next-generation behavioral biometrics has broadened its scope from real-world activities to virtual user recognition in the cyberworld. The purpose of augmenting the area of behavioral biometrics is to utilize human behavior from all available sources, including in-person and remote interactions.

Online and offline social interactions are integral parts of human behavior in a society. The amount of information generated by social network users has lead to information explosion in the virtual world. Ensuring security and privacy of online users has become an absolute necessity for a digital society. People are highly engaged in online social networking activities. They meet, interact with others, share their interests, make friends and followers irrespective of physical distances. Every day, social network users contribute new information to their digital footprints. These footprints are unique enough to be used for user identification and verification. This concept has been introduced into the biometric domains by Sultana *et al.* [8] as Social Behavioral Biometrics (SBB). User's communication patterns, daily routine, spatial information, emotions, linguistic style and even psychological profiles, play a vital role in creating a distinct user's behavioral profile. The research on SBB focuses on user identification and verification [9], user profiling and fraud investigation [10], psychological traits detection [11], sexual-predator detection [12], authorship identification [13] and cyberworld risk management [14]. Continuous authentication using SBB increases cybersecurity, identifies fake users and detects forgery activities. Thus, SBB ensures a safe environment for diverse cyberworld users.

The associate editor coordinating the review of this manuscript and approving it for publication was Vincenzo Conti.

Changes in the biometric features over time are known as template aging, which gradually lead to a decrease in the system accuracy [15]. One of the key challenges of behavioral biometric-based decision-making systems is behavioral change with time. For example, the keystroke dynamics of a novice user and an experienced user are different [16]. As users learn to type more efficiently, their enrolled keyboard dynamic template may become outdated. Social Behavioral Biometrics (SBB) also faces difficulty while matching the old templates with recently acquired sample for user identification. Over a certain period, there can be changes in the user networks, interaction pattern, preferences, hobbies, routine, style of communication, etc. As permanence is one of the vital biometric characteristics [17], [18], we intend to evaluate the permanence of our proposed SBB system as well as individual SBB traits in this paper. The following research questions will be answered:

1) How is the performance of an individual Social Behavioral Biometric trait affected over time and which trait is more stable?
2) How much does the overall performance of the Social Behavioral Biometric system change over different year gaps?
3) Can the integration of the stylistic features negate the template aging effect of the Social Behavioral Biometric system?
4) Is it viable to improve the performance of the Social Behavioral Biometric system by incorporating a genetic algorithm with the score level fusion algorithm?

Contributions of this article are:

1) The temporal permanence of individual Social Behavioral Biometrics (SBB) traits over four years has been evaluated and the most stable and least deteriorating SBB trait has been identified.
2) The performance analysis of the stylistic features as social behavioral biometric traits has been conducted.
3) An architecture of a new social behavioral biometric system and the method to mitigate the degradation of performance based on genetic algorithm and score-level fusion have been proposed.
4) The proposed system achieves the recognition accuracy of 99.25% and outperforms all prior research on SBB.

This research is the first study of template aging in a social behavioral biometric system. The rest of the paper is organized as follows: Section II discusses related research on social behavioral biometrics. The proposed methodology of a social behavioral biometric system is presented in Section III and the experimental results on the dataset of 5 years time span are discussed in Section IV. Finally, Section V concludes the paper and presents directions for future research.

## II. RELATED WORKS

The majority of research on Social Behavioral Biometrics (SBB) is very recent, with the attempt of extracting behavioral features from user's online social network activities, which are strong enough to be used as biometric identifiers [8]. Sultana *et al.* introduced the concept of SBB and designed a unimodal SBB system to identify users based on their profile information, network information, and communicative information [8]. Authors extracted knowledge-based features, style-based features and statistical features from this information. The identification rate, however, was not high enough to be used as a standalone system. Therefore, authors proposed a multimodal biometric system incorporating social behavioral biometrics with another physiological biometric.

A self-sufficient unimodal SBB system has been presented by Sultana *et al.* in [9] with a view to identifying users using their interpersonal communications, spatio-temporal behavior and interests on Twitter. Authors used an average score level fusion algorithm for combining five different weighted networks, namely, reply network, retweet network, URL network, hashtag network and temporal profile. However, these systems did not consider the textual information available in the tweets. Therefore, Tumpa and Gavrilova proposed a SBB trait based on the linguistic characteristic of the tweets [19]. Later, Tumpa and Gavrilova integrated the user's writing profile with other SBB traits to develop a new SBB system. In addition, a comparative analysis of the rank level and score level fusion algorithms was conducted [17].

Researchers used stylistic features as a cognitive biometric trait. Pokhriyal *et al.* designed a biometric system to distinguish between genuine user and imposter by extracting stylistic features, semantic features, and syntactic features from the written contents of blogs on the internet [20]. Neal *et al.* developed a continuous verification system using the character and lexical-level features extracted from the blogs written by the individuals and used these linguistic features as cognitive biometric trait [4]. Authors of [20] and [4] did not, however, consider the user's vocabulary set as linguistic features and did not experiment with their systems on any social networking data. Most recently, Alonso-Fernandez *et al.* proposed a system for social media forensics using the frequency of lexical, structural and syntactic properties obtained from tweets [21]. This research focused on writer identification of Twitter considering the stylometric features of the tweets and usage number of Twitter-specific features such as hashtags, URLs, replies, mentions, etc. and achieved 79.80% of accuracy at rank-1. Kaur *et al.* proposed a system to continuously authenticate the textual contents to detect compromised accounts on Twitter based on textual and stylometric behavior of the users [22]. Authors used content-specific and content-free features to develop the system and achieved 94.38% of accuracy for compromised account detection. Authors of [21] and [22] did not consider the friendship profiles, interactions, interests and preferences of the users in social media forensics.

Novel practical applications of this research emerged recently. A continuous authentication system using their social interaction was brought forward by Anjomshoa *et al.* [23]. The system extracted features from

the smartphone sensors and online social networks on user's location, data usage, number of sessions and session duration for multiple social networking platforms. Saleema and Thampi combined the concept of cognitive psychology with social behavioral biometric to generate feasible biometric templates, which were distinctive and stable [24].

The aforementioned studies examined various SBB traits for user identification. However, only a few researchers focused on evaluating the permanence and uniqueness of biometric traits. Gómez-Adorno *et al.* studied the changes in the writing style of novels over the years for seven authors using stylometric features [25]. Authors concluded that the change in writing style was noticeable even though there were three years of gap between the consecutively written contents. Can and Patton conducted a study on how writing style changes over a long period [26]. Authors used the frequencies of word lengths in text, vocabulary and the usage rate of most repeated words. They deduced that the stylometric pattern of the writers changes significantly with time.

In the discussion above, we have established that the effect of template aging on the biometric systems can be profound. Permanence is an important characteristic of the biometric traits, that ensures that legitimate users will be authenticated even if some time is elapsed from the time of their enrollment [18]. Therefore, evaluating the performance of social networks based biometric system over time has significant importance.

However, despite this significance, there has been no prior research that analyzed the effects of template aging on the permanence of a social behavioral biometric system. Moreover, as can be seen from the above survey, prior works in this domain used only selected textual or contextual user data for online authentication. In this work, it is for the very first time that the SBB recognition system fused textual, contextual and interpersonal communication information to generate a complete and accurate digital template for the users. The effect of template aging on individual SBB traits is also studied.

## III. METHODOLOGY

### A. OVERVIEW

Every interaction of the users over social networks collectively creates a virtual footprint that can be used for authentication. In this research, we have investigated users' social interactions on the Twitter platform to establish a biometric system. Twitter enables users to share their thoughts virtually with other acquaintances by posting tweets, which contain textual information, shared web links, hashtags, images, etc. The digital footprints of these users are a great source of unique features. We first describe the social behavior-based person identification system that utilizes a genetic algorithm for feature weight selection.

### B. SOCIAL BEHAVIORAL BIOMETRIC TRAITS

In the proposed system, several established social behavioral biometric traits are generated from the textual data, contextual data and interpersonal communication. Usually, tweets contain lexical information about the users from their vocabularies, abbreviations, misspelled words, frequency of punctuation, proclivity to capitalize words, sentence structures, etc. Shared weblinks, hashtags and emoticons reveal contextual information about the users. Interpersonal communicative information is obtained from the social interactions among acquaintances through mention, reply and retweet.

We have created writing profiles, stylometric profiles, reply networks, retweet networks, shared weblink networks and trendy topic networks from the mentioned data to identify users.

#### 1) USER'S WRITING PROFILE

A writing profile represents the user's vocabulary set that contains the most frequently used and distinctive words. As Twitter is an informal thought-sharing platform, users have the privilege to use words from their comfort zone, which varies from person to person. The writing profiles for every user present in the dataset are generated from the aggregated tweets and replies shared in their timelines.

At first, the raw tweets and replies of a user are given as input to the writing profile generator. A text pre-processing step is required to remove the noise from the tweets because punctuation, special characters, emoji and non-ASCII characters are helpful to increase the human readability of tweets. However, these characters are ineffectual for the machine learning algorithms. Therefore, after the noise removal step, these characters have been filtered from the tweets. Additionally, the shared hashtags, URLs and mentions are removed as the writing profile does not consider this information. Then, the clean data is converted into lowercase to normalize and tokenized into tokens. To keep only the significant tokens, the stop words, such as articles, prepositions and other frequently occurring words that do not bear much importance are eliminated from the matrix. This matrix of tokens is now considered as the vocabulary set for the user. All users in the dataset have their separate vocabulary sets. The vocabulary set generation from a raw tweet is illustrated in Fig. 1.

Twitter provides a unique alphanumeric handle to every user. The handles are encoded with numeric values, as machine learning algorithms are unable to understand the alphanumeric labels. After that, the feature extraction module of the writing profile generator extracts the features from the matrix of tokens using a popular feature engineering technique, Term Frequency-Inverse Document Frequency (TF-IDF) [27]. The textual vocabulary sets are converted into numerical representation through vectorization. TF-IDF was chosen as it assigns higher values to those words in the vocabulary sets, which are unique, uncommon and of significant importance for user identification. Finally, a predictive model is designed using the Multinomial Naïve Bayes (MNB) algorithm to identify users based on the feature vectors. MNB is one of the most popular and suitable machine learning algorithms for text-based multi-class problems [28].

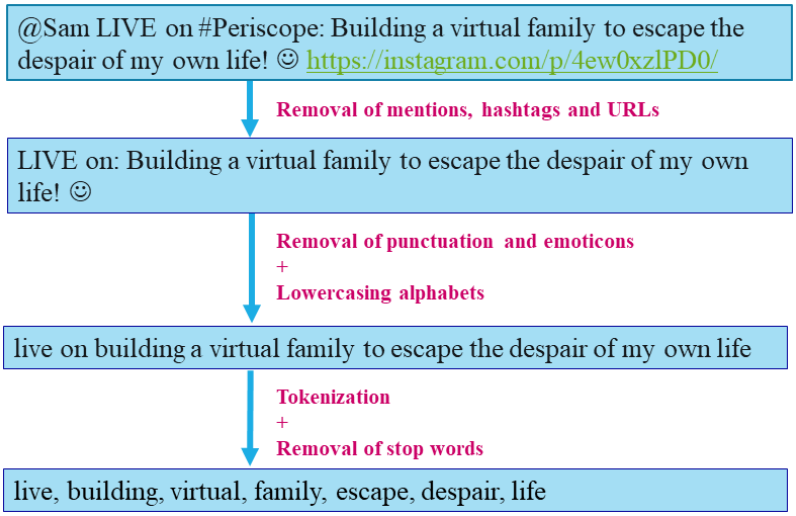



**FIGURE 1.** The steps of a vocabulary set generation from a single tweet.

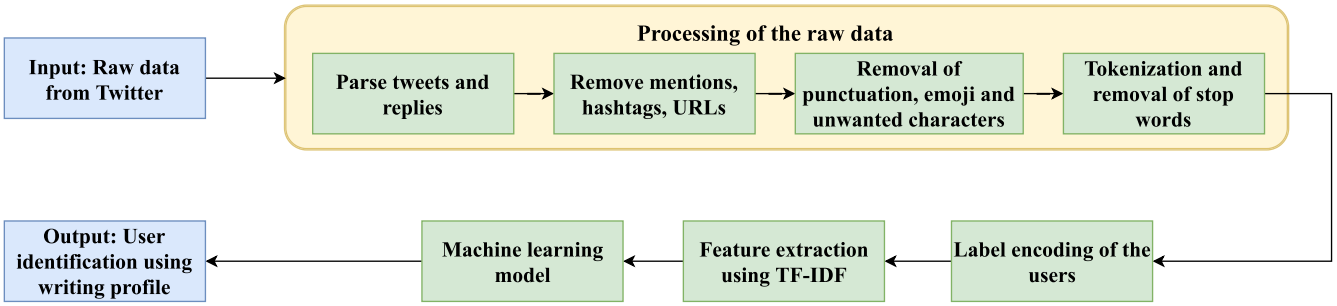



**FIGURE 2.** The workflow of user identification based on the writing profile.

The predictive model provides a matrix of predicted probabilities, where the model contains probabilities for all potential classes for all users of the dataset. Considering these probabilities, the user identification decision is performed. The workflow of user's writing profile generation is demonstrated in Fig. 2.

### 2) STYLOMETRIC PROFILE

The stylometric profile is generated from the writing pattern of a user, which deals with the stylistic features rather than the content of the tweets. Stylometry investigates the recurring patterns of a user's word distribution, sentence structure, punctuation usage, etc. The features of stylometry can be divided into six categories, namely, lexical, structural, syntactic, semantic, idiosyncratic and domain-specific features [29]. The lexical features are extracted at the character and word level of the texts, disregarding the grammar and context. Structural features capture the organization of sentences and paragraphs in a document. Syntactic features are language-dependent and concerned about parsing the formal grammatical rules of the text documents, such as punctuation and function words. Semantic features deal with the meaning of words, idioms, phrases and sentences. Idiosyncratic features concern the unusual person-specific features, such as misspelled words, abbreviations and slang. Domain-specific features or content-specific features vary according to the application and content of the documents.

**TABLE 1.** List of lexical features used to generate the lexical profile.

| | |
|---|---|
| Average number of words per tweet | Average sentence length in characters |
| Average length of words | Average number of unique words per tweet |
| Average number of characters per tweet | Percentage (%) of long words |
| Average number of words per sentence | Percentage (%) of short words |

We have incorporated two types of stylometric profiles in our SBB system. One is based on lexical features, and another is generated from the structural features, as it has been established that they perform the best for analyzing the stylometry of tweets of Twitter dataset [30].

The lexical features at the character and word level are extracted to generate the lexical profile for the users. At first, the raw tweets are fed into the system as input. The hashtags, URLs, user tags and emoticons are removed to prepare the data as they do not contain any lexical information. The lexical features listed in Table 1 are used to generate the lexical profiles [30].

Fig. 3 demonstrates the algorithm of the lexical profile generator. The numerical feature values are stored in a $1 \times 8$ matrix for a single user.

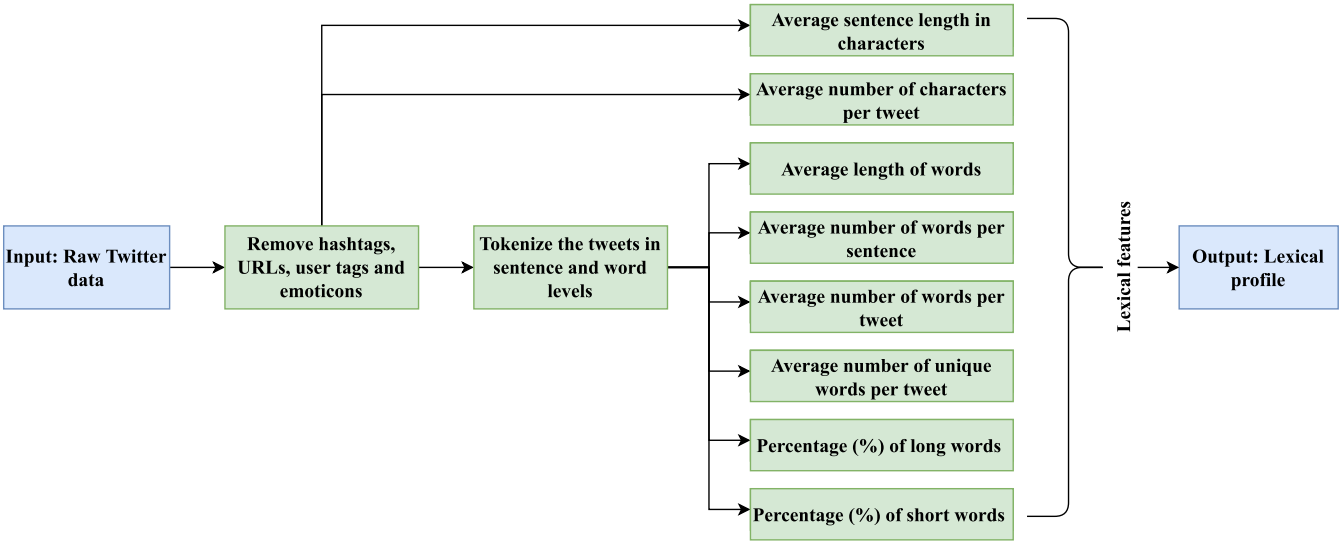



**FIGURE 3.** The process of generating user's lexical profile.

**TABLE 2.** List of structural features used to generate the structural profile.

| | |
|---|---|
| Average trend per tweet | Number of sentences starting with lowercase per tweet |
| Average URL per tweet | Average number of sentences starting with uppercase |
| Average tagged users per tweet | Average number of sentences starting with lowercase |
| Number of sentences starting with uppercase per tweet | Average number of sentences per tweet |

The structural profiles of the users are created from the structural features obtained from the tweets. As the structural features reveal how an author organizes the written piece, the URLs, hashtags and mentions are preserved. We remove the emoticons and punctuation from the data. The structural features listed in Table 2 are extracted to generate the profile. Fig. 4 illustrates the algorithm for profile generation.

### 3) REPLY NETWORK

The reply network is generated from the interpersonal communicative data of Twitter users [8]. The replies and mentions are separated from the data of a user. A list of acquaintances is parsed from the replies and mentions. A weighted reply network for a single user contains a set of nodes and edges. The replied and mentioned contacts, who pass a threshold value, are eligible to create nodes in the network. An edge between two nodes is formed based on the reply and mention relationship. The weight of an edge is calculated from the logarithm of relationship frequency produced by the connecting nodes. If both users communicate with each other frequently, the edge between them gets higher weight. The algorithm of generating reply network is illustrated in Fig. 5.

### 4) RETWEET NETWORK

On Twitter, users share their self-written tweets or other user's tweets with their followers to share knowledge and thoughts. Reposting others' tweets is known as ''Retweeting'' on Twitter. The retweet network is built using this retweeting behavior of a user [8]. This weighted network contains a set of nodes and edges similar to the reply network. The contacts whose tweets user retweets frequently are considered in the list of retweet acquaintances. From this list, upon qualifying a threshold value, the set of nodes is generated. The retweeting relationship of these two nodes is the basis of developing an edge between them, and the weight is calculated from the logarithm of frequency of their retweeting occurrence. The algorithm for generating the retweet network is identical to the reply network generation, depicted in Fig. 5.

### 5) URL NETWORK

Contextual information shared on Twitter helps to generate the URL network [8]. People usually browse websites according to their interests and thrust for knowledge. The browsing pattern of the users can be considered as a behavioral fingerprint of the users [31]. Often, users share web links with their tweets to present their ideas to their followers. These shared URLs also possess unique patterns that can identify users. The frequently shared web links represent a user's interests and personal choices, which vary from person to person. The URLs are parsed from the data to create the nodes in the network. The edges are formed between the user and their shared web links according to their sharing relationship. Typically, the domains shared by many users get less importance while assigning the weights on the edges. The algorithm of the URL network is demonstrated in Fig. 6.

### 6) TRENDY TOPIC NETWORK

Sharing hashtag with the tweets is a common phenomenon on Twitter. In any current trend, people add popular hashtags to their posts connecting them with the trends. These hashtags

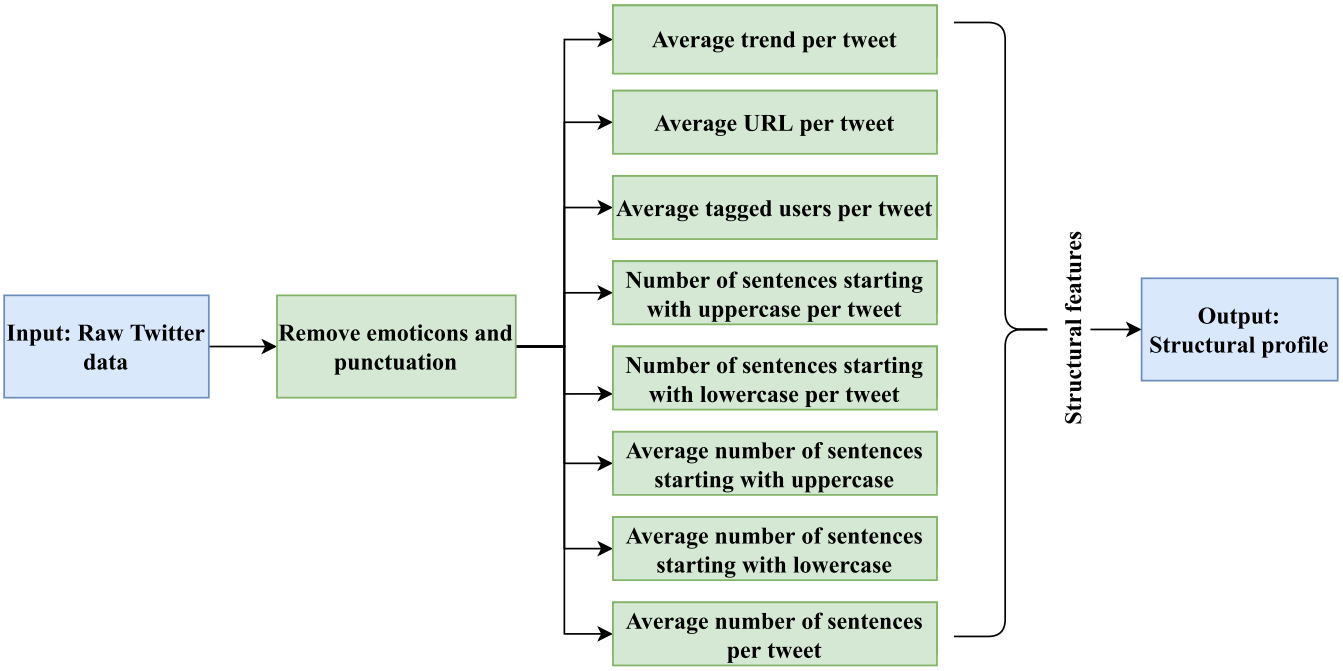



**FIGURE 4.** The flowchart of the structural profile generation.

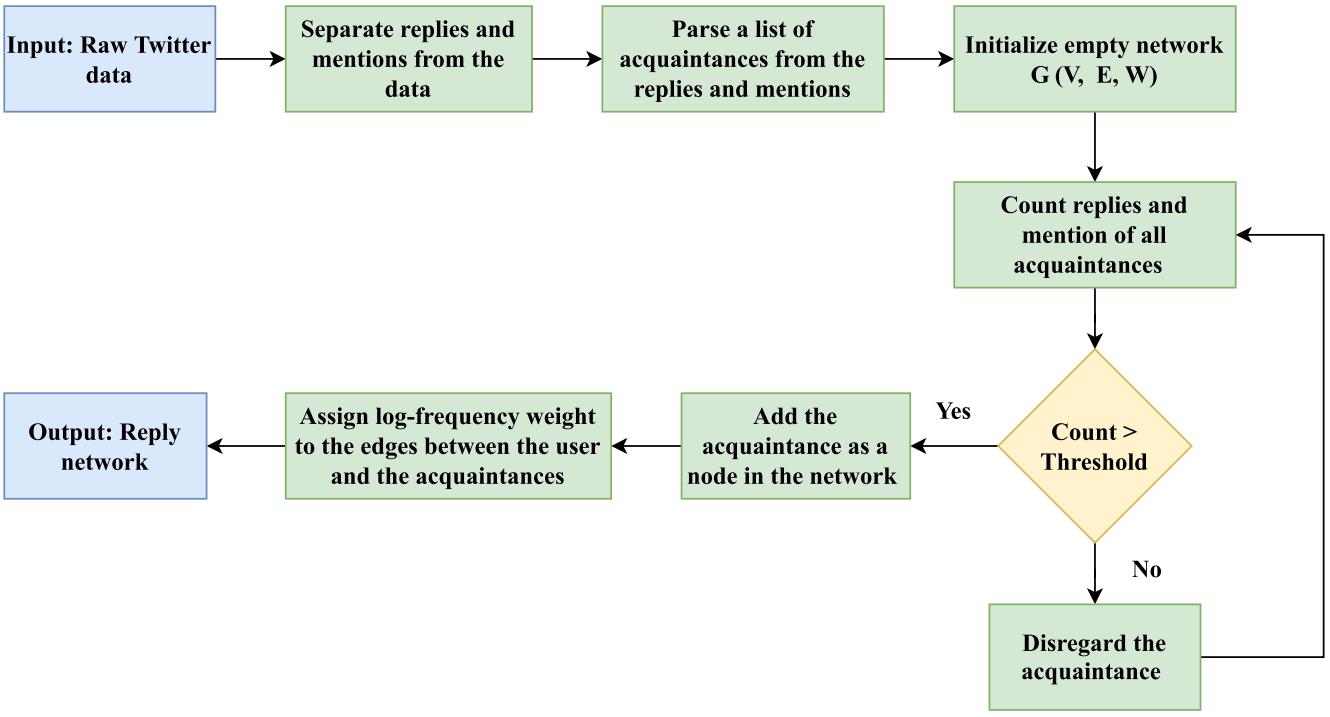



**FIGURE 5.** The flowchart of generating the reply network.

demonstrate the user's preferences towards the trends, as the main topics of the posts are directly related to the hashtags. The trendy topic network or hashtag network is produced from this contextual information. A set of nodes is created from the frequently used hashtags. An edge between a user and a node is formed based on their hashtag-sharing relationship. As the hashtag network is built for user identification, hashtags that are commonly shared by the users are insignificant for this network. Usually, the edges of constantly used but comparatively distinct hashtags get higher weights.

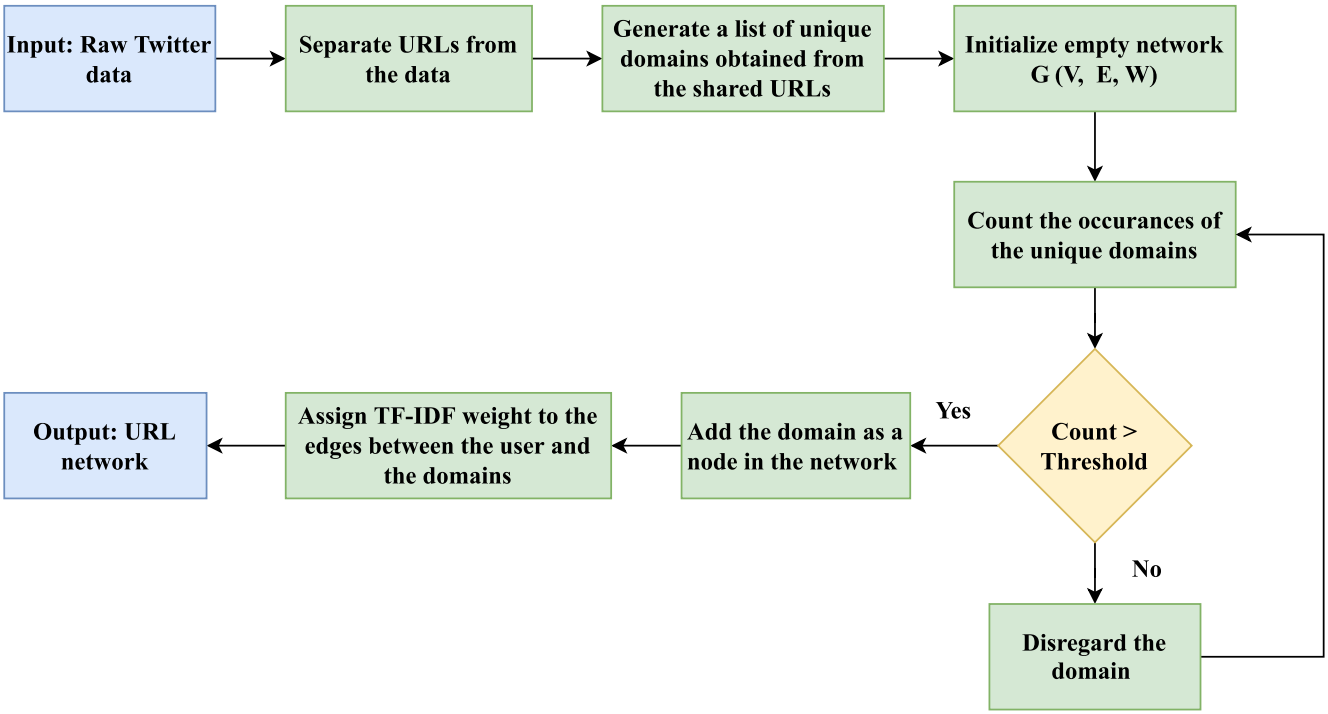



**FIGURE 6.** The flowchart of generating the URL network.

The process of its generation is identical to the URL network generation method depicted in Fig. 6.

### C. FUSION OF SBB TRAITS

A multimodal biometric system can be designed by fusing individual SBB traits for better identification performance [14], [32]. Let $N$ be the total number of users present in the template set. In the developed system, an individual SBB trait matcher provides a vector of $N$ matching scores for every sample of the test set considering that SBB trait. As we have used the similarity-based score level fusion, the closest score is the best match. While working with a multi-trait SBB system, we observe matching scores from all SBB traits and apply a score level fusion algorithm to determine the best match.

The simplest score level fusion technique is the sum rule algorithm. The summations of the matching scores obtained from individual SBB traits are considered as the fused scores. However, all traits involved in a multimodal system do not perform equally. Hence, instead of assigning the same weight to all available matchers, higher weights can be allocated to the more significant traits. In our previous research [17], we have experimented with different rank level and score level fusion algorithms and concluded that the weighted sum rule (WSR) score level fusion algorithm [33] performed best for our multi-trait SBB system. Therefore, we fuse the matching scores using the weighted sum rule algorithm. A genetic algorithm can be used to determine the optimal weights to achieve the highest recognition rate. Then, the summation is calculated using Equation 1 to get the fused score. Finally, the highest combined matching score is considered the best match.

Here, $M$ is the total number of SBB trait matchers. $S_{ic}$ is the combined score for $i^{th}$ testing sample for each identity. $S_{im}$ is the matching score obtained from the $m$ matcher for $i^{th}$ testing sample for each identity. $W_m$ is the weight for the $m$ SBB trait matcher.

$$S_{ic} = \sum_{m=1}^{M} S_{im} W_m \tag{1}$$

### D. GENETIC ALGORITHM

A Genetic Algorithm (GA) is a meta heuristic-based searching approach to find the fittest individuals for a locally optimal solution [34]. The iterative process of GA starts with a random initial population as the first generation. Each candidate solution present in the population is known as a chromosome, and the genes of that chromosome represent the properties of the chromosome. GA calculates the quality of a chromosome through a fitness or objective function, and the best individuals are chosen as the next generation population. The optimal weights for the SBB traits are calculated using the GA to achieve the highest identification accuracy. The main phases of GA in our proposed system are as follows:

- The initial population is created randomly from the pool of available uniformly distributed chromosomes within a range of 0.0 to 1.0. The uniform distribution increases the diversity of the population and helps to find the

auspicious search region. Each chromosome consists of seven genes to represent the weights of the SBB traits.

- As the main inspiration of GA is natural selection, the fittest individuals are expected to have high chances to survive in the next generations. Therefore, the fitness of all chromosomes present in a population is evaluated every generation through an objective function. The objective function calculates and cross-validates the recognition accuracy of the proposed system, considering the properties of each candidate solution. The combination that results in the highest accuracy of the proposed system is considered as the fittest individual of the population.
- The selection operator selects a certain number of the fittest individuals from a population so that they can pass their genes to the next generations to generate a better population. We have used the Elitism selection method to retain 40% of the fittest chromosomes unchanged in the next generation [35]. Elitism selection ensures that a certain portion of the best individuals is preserved for the next generation.
- The crossover or recombination operator in GA combines the genetic information of two parents to generate two new offspring. In a new generation, 40% of the population is selected from the previous generation as parents and 60% of the new population is produced through a crossover. This corresponds to a crossover rate of 0.6. As the number of SBB traits is seven in our system, we have an equal number of genes in the chromosome of a parent. Considering the small number of genes, we have chosen the single-point crossover method for the proposed system [36]. In the single-point crossover, a random point is selected, and the chromosomes of both parents are swapped before and after that point to produce two new offspring solutions. The algorithm ensures all combinations of parents get involved in the offspring generation.
- The last evolutionary operation is a mutation to ensure the diversity in the child solutions. We have used the Uniform mutation technique to a randomly selected gene of the chromosome [37]. As the summation of all the genes has to be 1, adding a random value from a uniform range of 0 to 1 is suitable for our method.

All the above GA operators are used to improve the population and performance quality of the next generation.

### E. WORKFLOW OF THE PROPOSED SYSTEM

The overall system architecture is demonstrated in Fig. 7. The system processes the raw Twitter data after taking the input. Then, the data is divided into training data and testing data. The pre-processed training and testing data are given to the SBB trait generator module to generate the writing profiles, structural profiles, lexical profiles, reply networks, retweet networks, trendy topic networks and URL networks. The system is trained with the templates generated from the training data and tested with the SBB traits generated from the test data by matching the stored templates.

The training and testing SBB traits are provided to the matching score generation module to generate the similarity score. The matching score generation module has individual matchers for matching the traits. The Multinomial Naïve Bayes (MNB) algorithm is appropriate for contrasting vectorized textual contents [19]. Therefore, the test writing profiles are matched using the MNB algorithm and generate the similarity scores. The structural profiles and lexical profiles are represented as statistical numerical data. The Cosine distance, Euclidean distance and Manhattan distance are three popular algorithms for calculating distances between two numerical vectors [30]. The Manhattan distance outperformed the other two algorithms for our SBB system. Fig. 8 shows the accuracy of structural and lexical profiles using all three algorithms. The structural and lexical test profiles are compared with the corresponding template profiles using the Manhattan distance. The reply, retweet, trendy topic, and URL networks use a network similarity checking algorithm to generate the matching scores [9]. The output of the matching score generation module is seven $NXN$ matrices, where $N$ is the total number of users.

The individual matching scores are then combined using the weighted sum rules score level fusion algorithm with a genetic algorithm. The genetic algorithm selects the optimal weights to achieve the highest accuracy in user identification. The final decision of user identification is made based on the fused scores.

## IV. EXPERIMENTAL RESULT

This section provides necessary experimentation to analyze the permanence of the proposed social behavioral biometric user recognition system. We have designed three experiments to answer the research questions stated in Section I. We have implemented the system using Python 3.6. All experiments have been carried out on the Windows 10 operating system, 1.8 GHz Quad-Core Intel Core i5 processor with 8GB RAM.

### A. DATASET

As the goal of this research is to analyze the performance deterioration of SBB traits over the years, the process of dataset collection has been designed accordingly. We have collected data of the Twitter users whose profiles and tweets are publicly available from 2016 to 2020. The dataset consists of all tweets and interactions of the same 100 Twitter users for the last five years (2016 to 2020). The interactions contain tweeting behavior, inter-user communication through retweets, replies and mentions, shared URLs and hashtags, timestamps, etc. A developer account has been created on Twitter and the premium version of the full archive search API has been used to collect the data.

We have prepared four types of train and test sets to conduct these experiments. The first one has one year of a gap between the train and test set. For example, if the

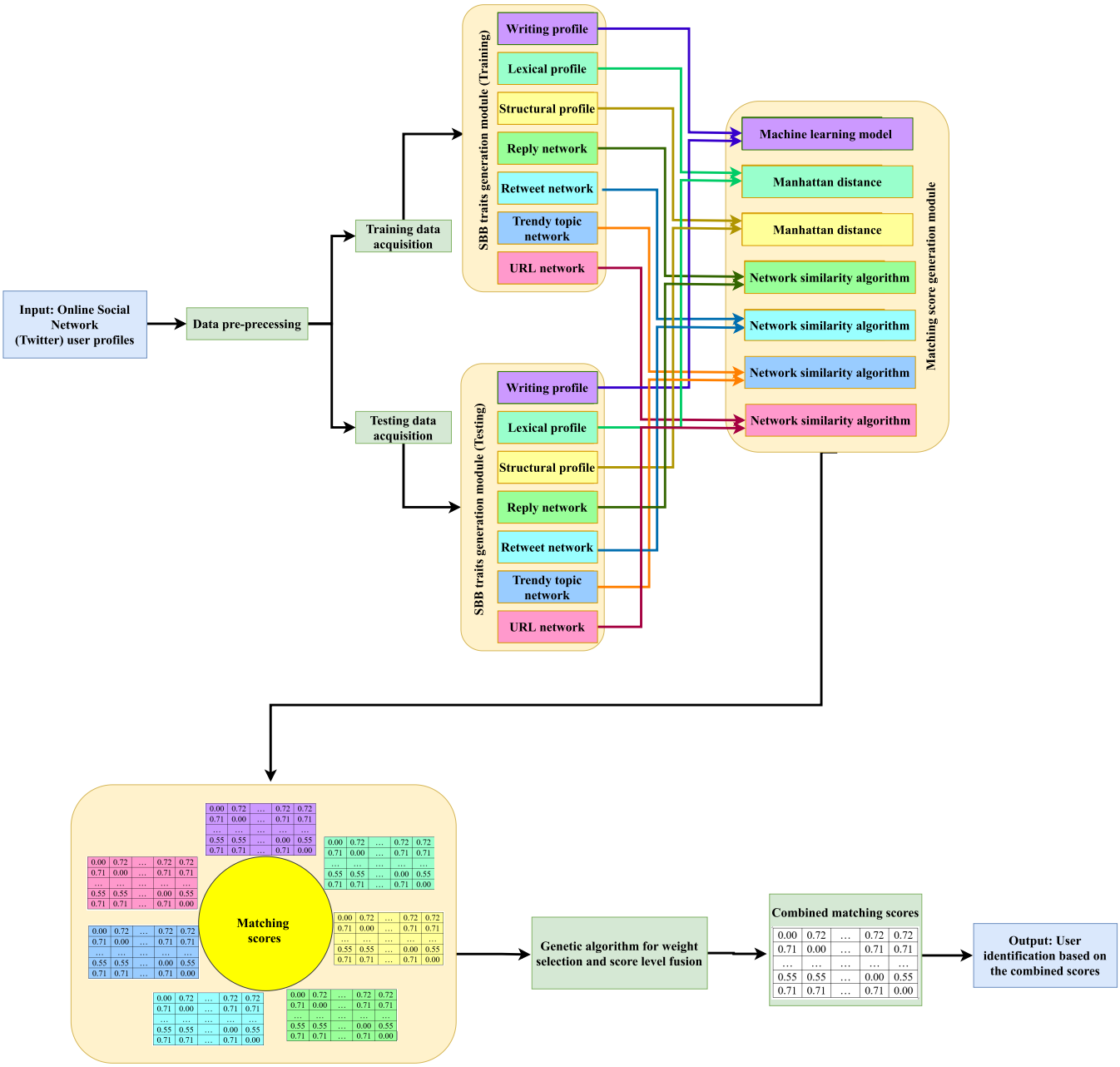



**FIGURE 7.** The system architecture of the proposed social behavioral biometric system.

biometric system is trained with the Twitter data of 2016, the system performance will be evaluated with the data of 2017. Similarly, the other combinations are, the training data year is 2017 and the testing data year is 2018, the training data year is 2018 and the testing data year is 2019, the training data year is 2019 and the testing data year is 2020.

The second type of train-test set contains two-year gaps between training and testing data. If the system is trained with the template from 2016, the performance will be tested with the data of 2018 and similar for other years. The third type has three years of gap between training and testing set data, and the last one contains four years of gap between both sets of data.

### B. PERFORMANCE COMPARISON OF STANDALONE SOCIAL BEHAVIORAL BIOMETRIC TRAITS OVER DIFFERENT YEAR GAPS

This experimentation answers the first research question, "How is the performance of an individual Social Behavioral Biometric trait affected over time and which trait is more stable?". The proposed system uses seven SBB traits, namely, writing profile, lexical profile, structural profile,

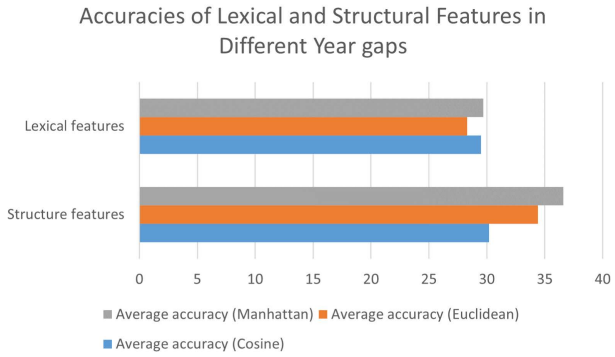



**FIGURE 8.** Accuracy of structural and lexical profiles using cosine distance, euclidean distance and manhattan distance algorithm.

**TABLE 3.** Accuracy, precision, recall and f-measure of the writing profile over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 95.50 | 93.63 | 95.50 | 94.21 |
| Two years | 94.33 | 92.14 | 94.33 | 92.80 |
| Three years | 90.50 | 87.20 | 90.50 | 88.17 |
| Four years | 89.00 | 85.08 | 89.00 | 86.23 |

**TABLE 4.** Accuracy, precision, recall and f-measure of the lexical profile over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 39.25 | 30.61 | 39.25 | 33.20 |
| Two years | 28.00 | 20.78 | 28.00 | 22.92 |
| Three years | 19.50 | 13.73 | 19.50 | 15.35 |
| Four years | 17.00 | 13.83 | 17.00 | 14.83 |

**TABLE 5.** Accuracy, precision, recall and f-measure of the structural profile over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 49.50 | 39.10 | 49.50 | 42.19 |
| Two years | 32.33 | 22.86 | 32.33 | 25.54 |
| Three years | 25.00 | 15.99 | 25.00 | 18.41 |
| Four years | 21.00 | 13.42 | 21.00 | 15.37 |

**TABLE 6.** Accuracy, precision, recall and f-measure of the reply network over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 89.75 | 86.31 | 89.75 | 87.31 |
| Two years | 86.33 | 81.92 | 86.33 | 83.15 |
| Three years | 81.00 | 74.19 | 81.00 | 76.20 |
| Four years | 78.00 | 71.89 | 78.00 | 73.48 |

**TABLE 7.** Accuracy, precision, recall and f-measure of the retweet network over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 79.25 | 76.25 | 79.25 | 76.96 |
| Two years | 71.00 | 65.86 | 71.00 | 67.18 |
| Three years | 64.50 | 56.35 | 64.50 | 58.53 |
| Four years | 62.00 | 53.92 | 62.00 | 56.11 |

**TABLE 8.** Accuracy, precision, recall and f-measure of the hashtag network over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 65.25 | 58.69 | 65.25 | 60.49 |
| Two years | 55.33 | 47.61 | 55.00 | 49.68 |
| Three years | 50.00 | 41.10 | 50.00 | 43.65 |
| Four years | 47.00 | 37.54 | 47.00 | 40.07 |

**TABLE 9.** Accuracy, precision, recall and f-measure of the URL network over different year gaps.

| Year gap | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| One year | 54.25 | 44.39 | 54.25 | 46.88 |
| Two years | 39.00 | 28.84 | 39.00 | 31.10 |
| Three years | 30.50 | 20.56 | 30.50 | 22.62 |
| Four years | 25.00 | 16.15 | 25.00 | 17.73 |

reply network, retweet network, hashtag network and URL network. The goal of this experiment is to analyze the accuracy, precision, recall and f-measure of the SBB traits over the years. The performance of individual SBB traits is measured and observed with all types of training and testing dataset combinations. The accuracy, precision, recall and f-measure of writing profile, lexical profile, structural profile, reply network, retweet network, hashtag network and URL network are manifested in Table 3, Table 4, Table 5, Table 6, Table 7, Table 8 and Table 9, respectively.

In this experiment, we evaluated the SBB traits without applying any fusion algorithm on the matching scores to observe the performance change of the individual SBB traits of our system over the years. When the system is tested with the data collected after one year of training data acquisition, the highest individual accuracy of 95.50% is achieved from the writing profiles. Usually, users write tweets in informal languages that mostly contain their own preferred words. Therefore, the writing profiles vary from user to user notably. These result in high accuracy in user identification. The reply and retweet network can achieve 89.75% and 79.25% accuracy, which is significantly conducive for the proposed system. The reply network presents user's closely connected virtual friend circles. The retweet network captures the retweeting behavior of a user. Due to the change in retweeting behavior of the users, the user identification performance of the retweet network is less than the reply network and writing profile.

The system could identify more than 50% of the test users individually using the hashtag network and URL network in the same training and testing scenario. The hashtag network captures user's interest in the current trends. However, Twitter trends change frequently within a year, and users get attached to the new trends. The shared URL or link with the Twitter post shows a user's interest in any webpage. Time has an impact on our preferences and interests, so as on the hashtag and URL networks. Therefore, after one year, the hashtag networks and URL networks are less accurate than the writing profile, reply and retweet networks. Almost 40% of the test users can be identified using the structural profile and lexical

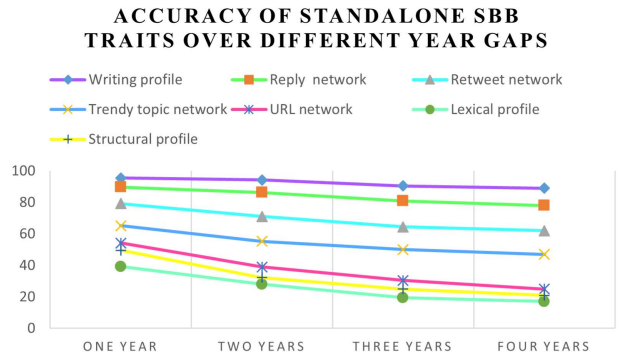



**FIGURE 9.** User recognition accuracy of individual SBB traits over different year gaps between the training and testing datasets.

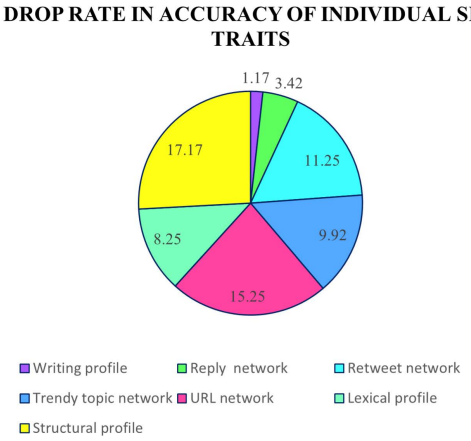



**FIGURE 10.** Comparison of accuracy deterioration of individual SBB traits.

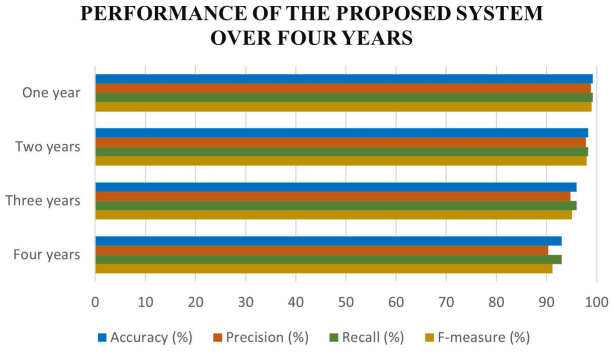



**FIGURE 11.** Comparison of accuracy, precision, recall and f-measure of the proposed system over four years.

profile of the users considering the same test dataset. The writing styles of tweets extracted from the structural and lexical features contain some unique characteristics which are helpful for user identification. However, considering the length restriction of tweets, tweets hold less stylistic information than large texts, which affects the performances of structural and lexical profiles. The SBB traits carry the same pattern in their performance when these are tested individually with the data collected after two, three and four years of the training data. Fig. 9 demonstrates the linearity of the performance degradation with the increment of year gaps.

Behavioral patterns of users are expected to be changed over the years. Therefore, the user identification performance of all SBB traits deteriorates over time. However, the writing profile emerged as the most stable biometric trait among other SBB traits. Despite testing the system with the data collected after four years of the training data, it achieved 89% accuracy standalone in user identification. The likely reason behind this is the writing profile depends on the user's frequently used vocabulary set. With time, people learn new words, but they also use their previous vocabulary knowledge. Changing the vocabulary skill of a person takes time which makes the performance of the writing profile stable. The reply and retweet networks also performed well under the same train-test condition. They achieved 78% and 62% of accuracy, respectively. In real life, the friends and connections people make in their life do not change completely within a couple of years. The circumstance is similar in the virtual social worlds also. Hence, the reply network could accurately identify users despite using the four years of old training data. The retweeting behavior of a person changes with time as people tend to follow more people based on current movements and trends, which impacts the performance of the retweet network. Across four years, Twitter trends and user preferences changed notably. Thus, it affects the performance of hashtag networks and URL networks. Also, with time some users write and structure their posts differently on social media to express their emotions, which reflects in the performance of the lexical and structural profiles.

Fig. 10 illustrates a comparative overview of all SBB traits during their change in accuracy of user identification. This figure presents the drop rate in the accuracy of a SBB trait compared to other traits between two types of datasets, when the system is training and testing data has a year gap of one, and the training and testing data has a two-year gap. The accuracy drop rate of the writing profile is less than 2% whereas the structural profile has the highest drop rate in user identification accuracy. This is likely due to the structural profile being dependent on the tweet organizing behavior of the users, which changes with recent experience, trend, community, etc.

Similar to other biometric modalities, social behavioral biometric traits experience template aging. However, when the system is trained with one year old data, all SBB traits have high recognition rates individually. Even after the system is trained with four years old data, most SBB traits perform reasonably. Therefore, we can conclude, this experiment proves the stability and temporal permanency of the SBB traits over the years, and identifies the most stable and less deteriorating SBB trait.

### C. EVALUATING IMPACT OF THE STRUCTURAL AND LEXICAL PROFILES ON SOCIAL BEHAVIORAL BIOMETRICS

This experiment answers research questions, "How much does the overall performance of the Social Behavioral Biometric system change over different year gaps?" and

**TABLE 10.** Comparison of accuracy, precision, recall and f-measure of the proposed SBB system (mega feature + structural profile + lexical profile fused with weighted sum rule + GA) with other researches when the system is trained with one year old data.

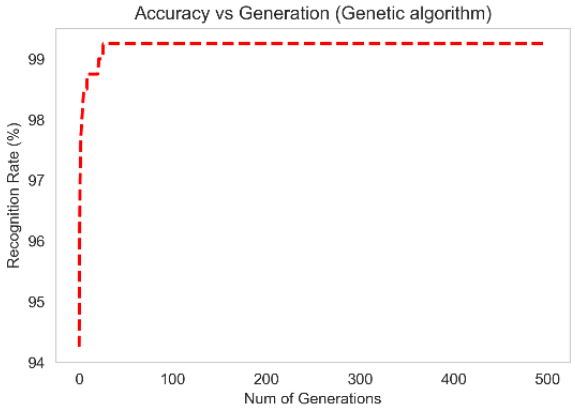
| Method and fusion algorithm | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| Mega feature* fused with Sum rule [17] | 95.25 | 94.10 | 95.25 | 94.43 |
| Mega feature fused with Weighted sum rule | 95.50 | 94.58 | 95.50 | 94.82 |
| Mega feature fused with Weighted sum rule + GA [17] | 97.75 | 96.90 | 97.75 | 97.14 |
| **Proposed system** | **99.25** | **98.88** | **99.25** | **99.00** |

*Mega feature = Writing profile + reply network + retweet network + hashtag network + URL network

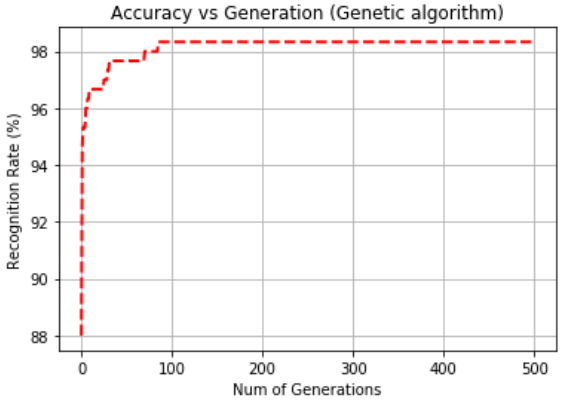
**TABLE 11.** Comparison of accuracy, precision, recall and f-measure of the proposed SBB system (mega feature + structural profile + lexical profile fused with weighted sum rule + GA) with other SBB systems when the system is trained with four years old data.

| Method and fusion algorithm | Accuracy | Precision | Recall | F-measure |
|---|---|---|---|---|
| Mega feature* fused with Sum rule [17] | 89.00 | 85.33 | 89.00 | 86.50 |
| Mega feature fused with Weighted sum rule | 89.00 | 85.00 | 89.00 | 86.33 |
| Mega feature fused with Weighted sum rule + GA [17] | 92.00 | 89.25 | 92.00 | 90.07 |
| **Proposed system** | **93.00** | **90.33** | **93.00** | **91.17** |

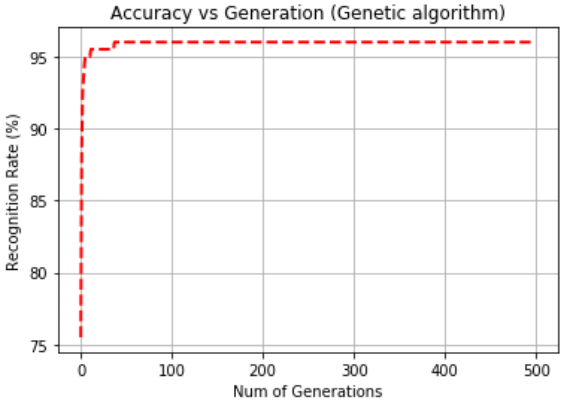
*Mega feature = Writing profile + reply network + retweet network + hashtag network + URL network



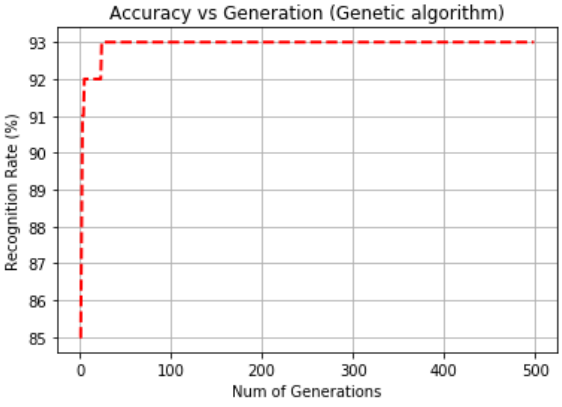

(a) When the year interval between the train and test dataset is one.




(b) When the year interval between the train and test dataset is two.




(c) When the year interval between the train and test dataset is three.

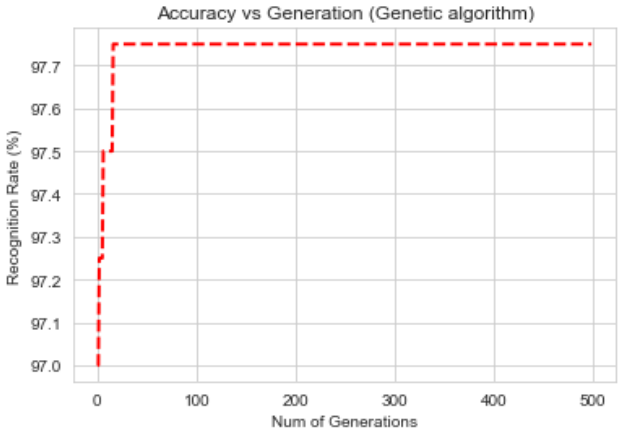



(d) When the year interval between the train and test dataset is four.

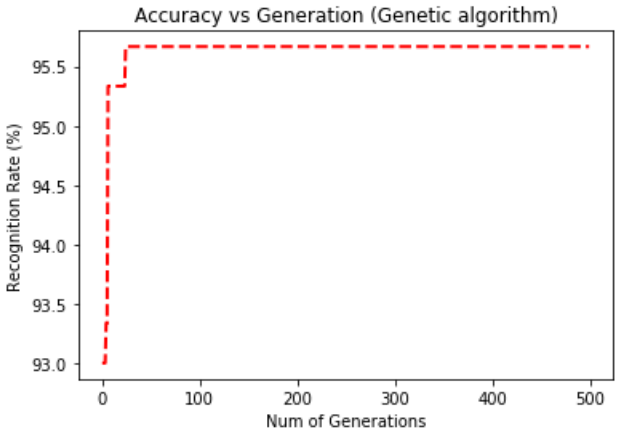
**FIGURE 12.** Accuracy of proposed SBB system with all seven traits vs number of generations of GA.

"Can the integration of the stylistic features negate the template aging effect of the Social Behavioral Biometric system?", respectively. The goal of this experiment is to compare and analyze the performance of the SBB system with and without these two SBB traits.

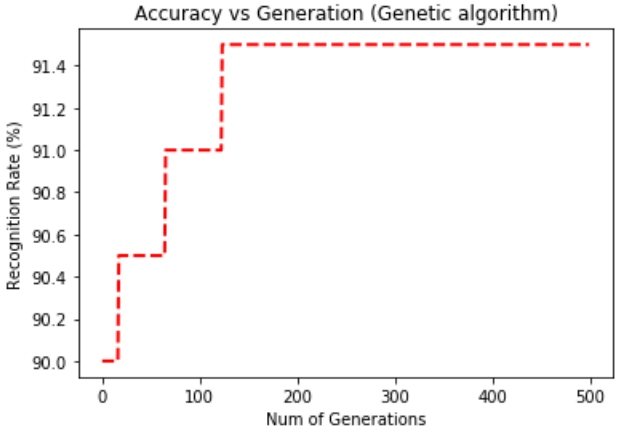
Fig. 11 displays the accuracy, precision, recall and f-measure of the SBB system that fused structural profile and lexical profile with the other five SBB traits. The new system achieved 99.25% of accuracy by combining seven SBB traits using a weighted sum rule score level fusion algorithm and



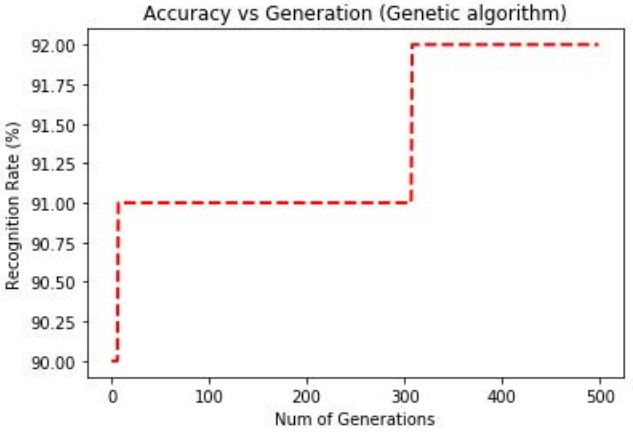

(a) When the year interval between the train and test dataset is one.




(b) When the year interval between the train and test dataset is two.




(c) When the year interval between the train and test dataset is three.




(d) When the year interval between the train and test dataset is four.

**FIGURE 13.** Accuracy of the SBB system without structural and lexical profiles vs number of generations of GA.

genetic algorithm. The precision, recall and f-measure of the proposed SBB system are also better than the previous SBB system with five traits. In Table 10, the accuracy, precision, recall and f-measure of the SBB system combining writing profile, reply network, retweet network, trendy topic network and URL network are demonstrated. The system achieved 97.75% of accuracy when it is tested with the data collected after one year of the training data and the accuracy drops to 92% when the system is trained with four years old data (Table 11).

Fig. 12 shows the accuracy of the proposed SBB system for the different combinations of year gaps between the training and testing data concerning the generations of the genetic algorithm. We ran the GA for each test dataset combination up to 500 generations and 3 times to get the locally optimal solution. Fig. 13 shows the accuracy of the SBB system combining five traits except for structural and lexical profiles vs the number of generations of GA under the same setting. It can be observed that the proposed SBB system reached the locally optimal solution faster than the SBB system with five traits, and this is accurate for all test cases. Also, we observed that the combination of seven traits resulted in better performance for all different year gap combinations of the test datasets.

Previously, we analyzed the individual performance of the structural profile and lexical profile. Though the standalone performance of both SBB traits is below 50%, they improved the overall system accuracy by 2%-4% in different training and testing scenarios and accelerated reaching the locally optimal solution. The structural and lexical profiles have the better distinguishing ability within a short period. Template aging has a large impact on these two traits. This reflects on the overall system performance as well. With the increase of time gap, structural and lexical profiles have less influence on the system performance. Therefore, it can be concluded from this experiment that structural profile and lexical profile have a highly positive impact on social behavioral biometrics.

### D. PERFORMANCE COMPARISON OF THE PROPOSED SYSTEM WITH PRIOR RESEARCHES

This experiment performs a comparative analysis of the proposed system with other SBB systems in literature and answers the final research question, ''Is it viable to improve the performance of the Social Behavioral Biometric system by incorporating a genetic algorithm with the score level fusion algorithm?''. We re-implemented recent SBB systems and evaluated the systems with our dataset to perform a fair comparison of the performance over the years. We compared the SBB systems with the least (one year) and the most year gaps (four years) between the training and testing data and manifested the result in Table 10 and Table 11, respectively.

$$Weight, W_i = \frac{A_i}{\sum_{k=1}^{k=n} A_k} \tag{2}$$

A unimodal SBB system combined five SBB traits, namely, writing profile, reply network, retweet network, URL network and hashtag network with sum rule score level algorithm. With the one year old training data, the system achieved 95.25% of accuracy and dropped to 89% when the training data have become four years old. A similar performance is observed when the same SBB traits are fused with a weighted sum rule algorithm. Here, the weights are determined based on their trait performance following the formula in Equation 2, where $A_i$ is the individual SBB trait accuracy. The SBB trait that contributes significantly gets a higher weight. The performance of the SBB system improved close to 3% for both training and testing dataset combination when the local optimal weights of the fusion algorithm are chosen by the genetic algorithm. This system was proposed by Tumpa and Gavrilova and it was the highest performing SBB system in literature [17]. The accuracy of 97.75% increased to 99.25% when the structural profile and lexical profile were integrated with the system. The system performance also improved by 1% for the four-year gaped train-test dataset combination. Similar behavior is observed for the precision, recall and f-measure score of the system.

The genetic algorithm has a significant impact on the social behavioral system performance. Table 10 and Table 11 report the performance of the overall SBB identification system with weights selected by the Genetic Algorithm. We observed that this method for weight selection improves the proposed SBB system recognition performance by an average of 2%-4%, which is observed over all years. This high performance over different years of data establishes the consistency of the proposed system. Also, a genetic algorithm is feasible to incorporate in the SBB system as it improves performance significantly.

## V. CONCLUSION AND FUTURE DIRECTION

Evaluating the effects of template aging of a biometric system has vital significance in biometric research. This research presents a social behavioral biometric system with high recognition performance and analyses the performance of the system as well as the individual SBB traits over the years. The experimental results established that proposed SBB system has stable performance over five years time span. The high accuracy, data availability and stability of the system prove that it can be used as a thriving biometric system in the digital world. Social Behavioral Biometric system has tremendous potential in the fields of cybersecurity, de-identification, psychological trait detection, continuous authentication, identity theft detection, author profiling, anomaly detection and other forensic applications. The proposed SBB system will also contribute to the smart society through user identification from their online social activities and unauthorized access prevention.

In the future, new features can be incorporated to improve the performance of the stylistic profiles of online social network users. The investigation of shared media files on online social networks may open scope for new idiosyncratic behavior of the users. Finally, additional methods can be explored to mitigate the effects of template aging on the performance of SBB.

## REFERENCES

[1] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, ''Evaluating behavioral biometrics for continuous authentication: Challenges and metrics,'' in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Apr. 2017, pp. 386–399.
[2] C. Bo, L. Zhang, T. Jung, J. Han, X.-Y. Li, and Y. Wang, ''Continuous user identification via touch and movement behavioral biometrics,'' in *Proc. IEEE 33rd Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2014, pp. 1–8.
[3] L. Marino, V. Alluri, A. Kumar, S. Li, A. Leider, and C. Tappert, ''Cognitive biometrics,'' in *Student-Faculty Research Day*. New York City, NY, USA: CSIS, Pace Univ., 2020, pp. 1–5.
[4] T. Neal, K. Sundararajan, and D. Woodard, ''Exploiting linguistic style as a cognitive biometric for continuous verification,'' in *Proc. Int. Conf. Biometrics (ICB)*, Feb. 2018, pp. 270–276.
[5] J. Chang, C.-C. Fang, K.-H. Ho, N. Kelly, P.-Y. Wu, Y. Ding, C. Chu, S. Gilbert, A. Kamal, and S.-Y. Kung, ''Capturing cognitive fingerprints from keystroke dynamics,'' *IT Prof.*, vol. 15, no. 4, pp. 24–28, 2013.
[6] M. Grimes and J. Valacich, ''Mind over mouse: The effect of cognitive load on mouse movement behavior,'' in *Proc. Int. Conf. Inf. Syst., Exploring Inf. Frontier*, 2015, pp. 1–14.
[7] A. Awad and Y. Liu, ''Cognitive biometrics for user authentication,'' in *Biometric-Based Physical and Cybersecurity Systems*. Cham, Switzerland: Springer, 2019, pp. 387–399.
[8] M. Sultana, P. P. Paul, and M. Gavrilova, ''A concept of social behavioral biometrics: Motivation, current developments, and future trends,'' in *Proc. Int. Conf. Cyberworlds*, Oct. 2014, pp. 271–278.
[9] M. Sultana, P. P. Paul, and M. L. Gavrilova, ''User recognition from social behavior in computer-mediated social context,'' *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 3, pp. 356–367, Jun. 2017.
[10] M. Raghuram, K. Akshay, and K. Chandrasekaran, ''Efficient user profiling in Twitter social network using traditional classifiers,'' in *Intelligent Systems Technologies and Applications*. Cham, Switzerland: Springer, 2016, pp. 399–411.
[11] V. Kaushal and M. Patwardhan, ''Emerging trends in personality identification using online social networks—A literature survey,'' *ACM Trans. Knowl. Discovery Data*, vol. 12, no. 2, pp. 1–30, Mar. 2018.
[12] M. A. Wani, N. Agarwal, and P. Bours, ''Sexual-predator detection system based on social behavior biometric (SSB) features,'' *Proc. Comput. Sci.*, vol. 189, pp. 116–127, Jul. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921011704
[13] R. Kaur, S. Singh, and H. Kumar, ''Authorship analysis of online social media content,'' in *Proc. 2nd Int. Conf. Commun., Comput. Netw.* Singapore: Springer, 2019, pp. 539–549.
[14] M. M. Monwar and M. Gavrilova, ''Markov chain model for multimodal biometric rank fusion,'' *Signal, Image Video Process.*, vol. 7, no. 1, pp. 137–149, Jan. 2013.

[15] J. Harvey, J. Campbell, S. Elliott, M. Brockly, and A. Adler, "Biometric permanence: Definition and robust calculation," in *Proc. Annu. IEEE Int. Syst. Conf. (SysCon)*, Apr. 2017, pp. 1–7.
[16] D. Shanmugapriya and G. Padmavathi, "A survey of biometric keystroke dynamics: Approaches, security and challenges," *Int. J. Comput. Sci. Inf. Secur.*, vol. 5, pp. 115–119, Oct. 2009.
[17] S. Tumpa and M. Gavrilova, "Score and rank level fusion algorithms for social behavioral biometrics," *IEEE Access*, vol. 8, pp. 157663–157675, 2020.
[18] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, vol. 479. Berlin, Germany: Springer, 2006.
[19] S. N. Tumpa and M. Gavrilova, "Linguistic profiles in biometric security system for online user authentication," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2020, pp. 1033–1038.
[20] N. Pokhriyal, K. Tayal, I. Nwogu, and V. Govindaraju, "Cognitive-biometric recognition from language usage: A feasibility study," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 134–143, Jan. 2017.
[21] F. Alonso-Fernandez, N. M. S. Belvisi, K. Hernandez-Diaz, N. Muhammad, and J. Bigun, "Writer identification using microblogging texts for social media forensics," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 3, no. 3, pp. 405–426, Jul. 2021.
[22] R. Kaur, S. Singh, and H. Kumar, "TB-CoAuth: Text based continuous authentication for detecting compromised accounts in social networks," *Appl. Soft Comput.*, vol. 97, Dec. 2020, Art. no. 106770.
[23] F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Social behaviometrics for personalized devices in the Internet of Things era," *IEEE Access*, vol. 5, pp. 12199–12213, 2017.
[24] A. Saleema and S. Thampi, "User recognition using cognitive psychology based behavior modeling in online social networks," in *Proc. Int. Symp. Signal Process. Intell. Recognit. Syst.* Singapore: Springer, 2019, pp. 130–149.
[25] H. M. G. Adorno, G. Rios, J. P. P. Durán, G. Sidorov, and G. Sierra, "Stylometry-based approach for detecting writing style changes in literary texts," *Computación y Sistemas*, vol. 22, no. 1, pp. 47–53, Mar. 2018.
[26] F. Can and J. M. Patton, "Change of writing style with time," *Comput. Hum.*, vol. 38, no. 1, pp. 61–82, Feb. 2004.
[27] W. Zhang, T. Yoshida, and X. Tang, "A comparative study of TF*IDF, LSI and multi-words for text classification," *Expert Syst. Appl.*, vol. 38, no. 3, pp. 2758–2765, Mar. 2011.
[28] K. Kowsari, K. Jafari, M. Heidarysafa, S. Mendu, L. Barnes, and D. Brown, "Text classification algorithms: A survey," *Information*, vol. 10, no. 4, p. 150, 2019.
[29] T. Neal, K. Sundararajan, A. Fatima, Y. Yan, Y. Xiang, and D. Woodard, "Surveying stylometry techniques and applications," *ACM Comput. Surv.*, vol. 50, no. 6, pp. 1–36, Nov. 2018.
[30] N. M. Sharon Belvisi, N. Muhammad, and F. Alonso-Fernandez, "Forensic authorship analysis of microblogging texts using N-Grams and stylometric features," in *Proc. 8th Int. Workshop Biometrics Forensics (IWBF)*, Apr. 2020, pp. 1–6.
[31] L. Olejnik, C. Castelluccia, and A. Janc, "On the uniqueness of web browsing history patterns," *Ann. Telecommun.*, vol. 69, nos. 1–2, pp. 63–74, 2014.
[32] M. M. Monwar, M. Gavrilova, and Y. Wang, "A novel fuzzy multimodal information fusion technology for human biometric traits identification," in *Proc. IEEE 10th Int. Conf. Cognit. Informat. Cognit. Comput. (ICCI-CC)*, Aug. 2011, pp. 112–119.
[33] N. Damer, A. Opel, A. Shahverdyan, M. Marsico, and A. Fred, "An overview on multi-biometric score-level fusion-verification and identification," in *Proc. 2nd Int. Conf. Pattern Recognit. Appl. Methods*, Barcelona, Spain, 2013, pp. 647–653.
[34] S. Mirjalili, "Genetic algorithm," in *Evolutionary Algorithms and Neural Networks*. Cham, Switzerland: Springer, 2019, pp. 43–55.
[35] S. Yadav and A. Sohal, "Comparative study of different selection techniques in genetic algorithm," *Int. J. Eng., Sci. Math.*, vol. 6, no. 3, pp. 174–180, 2017.
[36] M. Srinivas and L. M. Patnaik, "Genetic algorithms: A survey," *Computer*, vol. 27, pp. 17–26, Jun. 1994.
[37] M. Srinivas and L. M. Patnaik, "Adaptive probabilities of crossover and mutation in genetic algorithms," *IEEE Trans. Syst., Man, Cybern.*, vol. 24, no. 4, pp. 656–667, Apr. 1994.

**SANJIDA NASREEN TUMPA** received the B.Sc. degree in computer science and engineering (CSE) from the Military Institute of Science and Technology (MIST), Bangladesh, in 2014, and the M.Sc. degree in CSE from the Bangladesh University of Engineering and Technology (BUET), Bangladesh, in 2019. She is currently pursuing the M.Sc. degree in computer science with the University of Calgary, Canada, under the supervision of Prof. Marina L. Gavrilova.

She worked with the Department of CSE, MIST, as a Faculty Member, from 2015 to 2019. She has published over 15 conference papers, in addition to two journals and four book chapters. Her research interests include social network analysis, biometrics, privacy, natural language processing, and machine learning. She received the prestigious Alberta Graduate Excellence Scholarship (AGES) Award during her M.Sc. degree with the University of Calgary.

**MARINA L. GAVRILOVA** (Senior Member, IEEE) is currently a Full Professor with the Department of Computer Science, University of Calgary, the Head of the Biometric Technologies Laboratory, and a Board Member of ISPIA. Her publications include over 200 journals and conference papers, edited special issues, books and book chapters in the areas of image processing, pattern recognition, machine learning, biometric and online security. She has founded ICCSA—an international conference series with LNCS/IEEE, co-chaired a number of top international conferences. She is the Founding Editor-in-Chief of *LNCS Transactions on Computational Science* journal. She is on the Editorial Boards of the *Visual Computer*, *International Journal of Biometrics*, and six other journals. She has given over 50 keynotes, invited lectures, and tutorials at major scientific gatherings and industry research centers, including at Stanford University, SERIAS Center, Purdue; Microsoft Research, USA; Oxford University, U.K.; Samsung Research, South Korea; and others. She currently serves as an Associate Editor for IEEE Access, IEEE Transactions on Computational Social Systems, the *Visual Computer*, and the *International Journal of Biometrics*. She was appointed by the IEEE Biometric Council to serve on IEEE Transactions on Biometrics, Behavior, and Identity Science Committee.