Neutrosophic Sets and Systems, Vol. 76, 2025
University of New Mexico

A Novel Framework for Gauging Information Extracted from Smartphones Using Neutrosophic Logic

R. M. Abou alzahab[1] , Amr Ismail [1,2] , S. H. Abd Elkhalik[3] , M. Y. Shams[4], H. M. El-Bakry[5] and A. A. Salama[1].

[1] Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Egypt, ramy.zahab@sci.psu.edu.eg, amr_ismail@sci.psu.edu.eg, ahmed_salama_2000@sci.psu.edu.eg

[2] Department of Cybersecurity, College of Engineering and Information Technology, Buraydah Private Colleges, Buraydah 51418, Kingdom of Saudi Arabia.

[3]Department. of Communication and Computer Engineering, Air Defense University., Egypt shelmy@horus.edu.eg

[4]Faculty of Artificial Intelligence, Kafrelsheikh University, Kafrelsheikh 33516, Egypt. mahmoud.yasinA@ai.kfs.edu.eg

[5]Department of Information Systems., Faculty of Computer and Information Science, Mansoura University., Egypt elbakry@mans.edu.eg

Abstract: Smartphones contain a vast amount of information about their users, which can be used as evidence in criminal cases. However, the sheer volume of data can make it challenging for forensic investigators to identify and use the most relevant information. Neutrosophic logic is a generalization of fuzzy logic that allows for uncertainty and vagueness, making it a more potent tool for dealing with the ambiguity of real-world data. The proposed framework aims to identify and utilize the most relevant information for forensic investigators, making it easier to solve criminal cases using Neutrosophic logic. This novel approach provides a more powerful tool for dealing with the ambiguity of smartphone data, ultimately improving the accuracy and effectiveness of forensic investigations. Our research has utilized Neutrosophic logic to evaluate the degree of truth, falsity, or Indeterminacy of this information. Additionally, this study analyzes conversations between individuals using Excel's fuzzy lookup add-in to determine the percentage of truth and false in each conversation. The results were compiled into a dataset and utilized a Neutrosophic Python code to evaluate the information. The results indicate the percentage of truth, false, and Indeterminacy in each conversation and which can be used to determine its admissibility as evidence and which not.

Keywords: Smartphone, Forensics, Neutrosophic Logic, Fuzzy Logic, Uncertainty, Investigations.

1. Introduction

In the modern digital age, smartphones have become ubiquitous companions, silently recording a vast tapestry of personal and potentially incriminating information. While this data presents a treasure trove for forensic investigations, its sheer volume and inherent ambiguity pose a significant challenge: Identifying and leveraging the most relevant information amidst a sea of uncertainty [1]. Traditional digital forensic techniques, often reliant on stark binary classifications of "relevant" or "irrelevant," falter when confronted with the nuanced complexities of real-world smartphone data [2]. This research gap necessitates innovative approaches that can effectively navigate the inherent

uncertainty and vagueness embedded within this digital trove. This paper proposes a novel framework for gauging information extracted from smartphones by harnessing the power of Neutrosophic logic. Neutrosophic logic, a generalization of fuzzy logic, overcomes its predecessor's shortcomings by embracing the inherent ambiguity and uncertainty in real-world data, unlike fuzzy logic, which functions on a truth-false spectrum. Neutrosophic logic adds a third truth value: indeterminacy. This essential innovation enables a more thorough representation of smartphone data, including not only degrees of truth and untruth but also the inherent "unknowns" that impede forensic investigations [3]. Our methodology intends to maximize the forensic value of smartphone data by using the expressive capacity of Neutrosophic logic. We imagine a future in which relevant information is quickly detected and prioritized, allowing for more accurate and efficient investigative processes. Ultimately, this novel approach has the potential to revolutionize the landscape of smartphone forensics, leading to enhanced investigative outcomes and potential crime resolution [4]. The paper presented by Abou alzahab et al. [5] investigated that the smartphones store vast amounts of user data, which can be invaluable to forensic investigators during criminal investigations. However, this data can also be manipulated by malicious actors to fabricate evidence and mislead investigators. Their research leverages fuzzy logic to assess the authenticity of this information. Further, they analyzed conversations between individuals using Excel's fuzzy lookup add-in to determine the percentage of truth and falsehood in each conversation. The results were compiled into a dataset and evaluated using a fuzzy model developed with Matlab's fuzzy toolbox.

In [6] the study investigates the key factors influencing customer attitudes toward social media influencers and their impact on purchase intentions. By analyzing 376 online survey responses using Structural Equation Modelling (SEM), machine learning, and multi-criteria decision-making (MCDM) methods, the study categorizes digital influencers' behaviors affecting consumer perceptions. The models reveal how these factors shape acceptance of influencers' messages, offering recommendations for optimizing influencer marketing strategies. Marketers can enhance user experience and conversion rates, while customers benefit from more relevant and engaging content, fostering stronger brand connections and influencing purchase decisions. Regular evaluations are suggested to continuously improve influencer marketing efforts. This article discusses several aspects of smartphone forensics, such as case studies, frameworks, and data extraction and analysis methods. They also discuss the difficulties of dealing with ambiguous and unclear evidence in forensic investigations, as well as the usage of fuzzy logic and Neutrosophic logic for decision-making and classification. Some references also discuss software tools and applications for implementing these logics, such as the Excel Fuzzy Lookup and the Neutrosophic Python code algorithm. These references will be useful in providing a foundation for the proposed framework and its implementation using Neutrosophic logic. This research contributes to the field of smartphone forensics by Addressing the critical challenge of handling ambiguous and uncertain data in forensic investigations. Introducing a novel framework specifically tailored for smartphones, utilizing the advanced capabilities of Neutrosophic logic. Demonstrating the potential of Neutrosophic logic to significantly improve the accuracy and effectiveness of forensic investigations.

Smartphones contain a vast amount of information about their users, which can be used as evidence in criminal cases. However, the sheer volume of data can make it challenging for forensic investigators to identify and use the most relevant information. Neutrosophic logic is a generalization of fuzzy logic that allows for uncertainty and vagueness, making it a more potent tool for dealing with the ambiguity of real-world data. The proposed framework aims to identify and utilize the most relevant information for forensic investigators, making it easier to solve criminal cases using Neutrosophic logic. This novel approach provides a more powerful tool for dealing with the ambiguity of smartphone data, ultimately improving the accuracy and effectiveness of forensic investigations.

Research Gap: Current forensic methodologies often struggle with the overwhelming volume and ambiguous nature of smartphone data, lacking efficient tools to discern and prioritize relevant information amidst the uncertainty.

Novelty: Our research leverages Neutrosophic logic to evaluate the degree of truth, falsity, or indeterminacy in smartphone data, a novel application in the forensic field. Additionally, we analyze conversations using Excel's fuzzy lookup add-in to determine the percentage of truth and falsehood in each conversation. The results, compiled into a dataset and evaluated using Neutrosophic Python code, indicate the percentages of truth, falsehood, and indeterminacy in each conversation, enhancing the determination of admissibility as evidence. This approach significantly advances the capability of forensic investigators to handle and interpret ambiguous data effectively.

This paper is organized as follows: Section 2 discusses background on gauging information extracted from Smartphones using Neutrosophic Logic. Section 3: provides an overview of the methods used to evaluate the extracted evidence data using the Python algorithm code, and Excel Fuzzy Lookup Add-in. Section 4 presents the results and discussions of our research, and finally, Section 5 shows the conclusion and the future work

2. Background

2.1 Data Acquisition Technique:

The techniques used to extract information from mobile devices [7]. Micro-read is a technique used to view data on memory chips using high-power electron microscopes. However, it can be expensive, time-consuming, and requires expertise in hardware and file systems [8]. Chip-off is a useful technique in digital forensics. It involves extracting data from the memory chip by generating a binary image. However, it can damage the device, making it a costly process. [9]. JTAG is a technique that allows investigators to extract physical data from a smart device. To do this, the investigator connects the smart device to a workstation and then uses forensic tools like XACT and Pandora's Box to extract and create a raw data image stored in the smart device's memory [8]. Logical extraction is the most commonly used technique for extracting data from a smart device. This process involves connecting the device to a forensic lab via Bluetooth, cable NFC, or other methods. After connecting the device, forensic tools will be installed to extract all the data stored on the device. [10].

2.2 Boolean logic:

Boolean logic is a foundational idea in computer technology and mathematics. It is based on binary logic principles, which use two values to describe logical statements: true (represented by 1) and false (represented by 0) [11]. More sophisticated expressions can be created by combining these assertions with Boolean operators such as AND, OR, and NOT. Understanding boolean logic is essential for creating and analyzing digital computer circuits, as well as programming and algorithm creation [12].

2.3 Neutrosophic logic:

Florentin Smarandache introduced neutrosophic logic, an extension of classical and fuzzy logic, in the late 1990s. It is intended to handle uncertainty, indeterminacy, and partial information more efficiently than standard logic systems. Neutrosophic logic is particularly well-suited to circumstances in which truth, untruth, and indeterminacy values coexist [13]. Neutrosophic logic is

a rapidly emerging research subject with several applications in diverse industries. This logic is being studied for its ability to handle complex and ambiguous data, and new developments are continually appearing. While the potential of Neutrosophic logic in digital forensics has not been thoroughly investigated, it shows enormous promise and is ripe for further investigation [14].

2.3.1 Neutrosophic Logic Architecture:

While there is no standardized design for Neutrosophic logic, which is a relatively new and less formalized discipline when compared to traditional logic systems, there are some significant components and factors that are typically taken into account when developing systems employing Neutrosophic logic [13].

- Neutrosophic Sets:

  The concept of neutrosophic sets forms the foundation of neutrosophic logic. Each element in a set is assigned three values: truth, indeterminacy, and falsehood. Although the representation of these values may differ, a triplet (T, I, F) is often used [13].

- Neutrosophic Logic Operators:

  Neutrosophic logic introduces operators such as Neutrosophic conjunction (∧), disjunction (∨), and implication (→), allowing operations on Neutrosophic truth values [15].

- Neutrosophic Inference Mechanisms:

  In a Neutrosophic system, inference mechanisms involve rules used to combine or deduce new statements from existing ones, depending on the specific application and the nature of the problem being addressed [15].

- Graphs and Networks:

  In some applications that involve complex relationships, the architecture may include components for representing and processing Neutrosophic graphs and networks [16].

- Evaluation and Validation Tools:

  The architecture should include tools for evaluating and validating its performance to ensure the effectiveness of the Neutrosophic system [16].

2.3.2 Neutrosophic Framework: For Gauging Information Extracted from Smartphones and consists of three steps [17]:

I. Extracting data: The initial stage involves retrieving the necessary data from the smartphone. Various methods can achieve this, including keyword search, pattern matching, and machine learning. [17].

- Keyword search: This technique involves searching the smartphone for keywords that are relevant to the case.

- Pattern matching: This technique involves searching the smartphone for patterns that are indicative of criminal activity.

- Machine learning: This technique can be used to train a model to extract relevant data from smartphones.

The choice of data extraction technique will depend on the specific case and the available resources.

II. Neutrosophic assessment: The next phase involves assessing the gathered information through neutrosophic reasoning. This includes assigning a level of truth, falsehood, and neutrality to every data point [18]. This is accomplished by following these steps:

- Determine the important aspects of data. For instance, the size of data for a chat message could include the message's content, the sender of the message, and the circumstances of the message

- Assign a degree of truth, falsity, and neutrality to each dimension of information. This can be done using a variety of techniques, such as fuzzy logic or machine learning.

- Determine the total level of accuracy, inaccuracy, and impartiality of the information. This is accomplished by merging the levels of truth, falsehood, and neutrality in every aspect of information.

The Neutrosophic evaluation step can be performed manually or automatically.

III. Decision-making: The third step is to use the neutrosophic evaluation results to decide the relevance of the information. This decision can be made by a human forensic investigator or by an automated system [18]. If the overall degree of truth of the data is high, then the data is considered relevant. If the overall degree of truth for the data is low, then the data is considered irrelevant.

2.3.3 Neutrosophic Logic Tools: Various tools and libraries are available for researchers and practitioners working with Neutrosophic logic, with some still under development.

- Neutrosophic Computing Toolbox for Python:

There have been attempts to create Python-based tools for neutrosophic computing. These comprise libraries for representing and manipulating neutrosophic sets, as well as for carrying out neutrosophic logic operations [19].

- Neutrosophic Logic Toolbox for MATLAB:

Dr. Florentin Smarandache created a MATLAB toolbox for working with neutrosophic sets, logic operations, and applications. The toolbox offers MATLAB functions and utilities [17].

- jNTool (Java Neutrosophic Tools):

jNTool is a collection of Java-based tools for dealing with neutrosophic logic. It contains implementations of neutrosophic set operations, logical connectives, and utilities for creating neutrosophic systems [20].

2.4 Excel Fuzzy Lookup:

Fuzzy Lookup is a useful function in Excel that enables users to identify and match related entries across huge datasets. Excel's fuzzy lookup uses fuzzy matching algorithms and similarity

measurements to effectively recognize records with minor differences, such as misspellings or typos, and offer a list of likely matches [21].

This add-in takes into account the spelling and similarity of responses, ensuring that only very close matches are considered valid. Excel Fuzzy Lookup may substantially speed up the process of scoring cued recall data while eliminating potential errors or discrepancies caused by human judgment. SSIS's Fuzzy Lookup operator provides a similar capability for approximate string matching. Incorporating the fuzzy lookup system into this operator boosts its possibilities [22].

3. The proposed Methodology

The purpose of this research is to assess data, determine if it is reliable or not, and analyze it. Neutrosophic Logic has been selected as the method for evaluating the data and providing a level of certainty for forensic investigators to use in investigations. Additionally, Excel's fuzzy lookup has been utilized to evaluate conversations between individuals and assign a percentage to each data point. The results are compiled into a dataset and analyzed using Python code to assess the reliability of the information. The outcomes reveal the percentage of each data point and whether it can be considered as evidence.

3.1 The dataset:

The dataset that we examined was downloaded from Kaggle, specifically from the WhatsApp Chat dataset. This dataset consists of chat data between individuals and includes various details necessary for forensic analysis. To align the data with our research requirements, we made several alterations to the original dataset. The dataset comprises seven columns, each representing different aspects of the chat data. The first column denotes the sender of the chat, while the second column contains the chat messages. The third to seventh columns represent the date and time (year, month, day, hour, and minute) at which each message was sent or received, as shown in Table 1. The dataset that we examined was downloaded from a Kaggle website [23] and we made some alterations to it to match our research. The dataset is a chat between individuals and others. The chat consists of 7 columns. The first column is the sender of the chat, the second column is the chat. The third to seventh columns represent data and time, as shown in the Table 1. The table include 7 users which indicated that the main user which the smartphone found its data and the message corresponding to each user for discovering forensic data in year, month, day, hours, and minutes.

3.1.1. Definitions

1. Message Timing: The timestamp (year, month, day, hour, and minute) at which a message was sent or received.
2. Main User: The primary user of the smartphone, whose data is the focus of the forensic analysis.
3. Forensic Data: Information extracted from digital devices that can be used as evidence in investigations.
4. Neutrosophic Logic: A branch of logic that deals with indeterminacy, handling truth, falsehood, and indeterminacy simultaneously.

3.1.2. Aggregations

1. Total Messages Sent by Main User: Count of all messages sent by the main user.
2. Message Frequency by User: Number of messages sent by each user.
3. Conversation Duration: The total duration of a conversation, calculated from the first to the last message timestamp.

4. Average Message Interval: The average time interval between consecutive messages in a conversation.

3.1.3. Theorems and Examples

1. Theorem: Consistency of Message Timing
    - Statement: If messages from different users have identical timestamps, they are part of the same conversation thread.
    - Example: On November 26, 2021, at 21:48, User 1 and the Main User exchanged messages, indicating an active conversation at that precise minute.
2. Theorem: Conversation Length
    - Statement: The length of a conversation is the difference between the timestamps of the last and first messages.
    - Example: The conversation on December 2, 2021, between the Main User and User 3, lasted from 22:03 to 22:08, a duration of 5 minutes.
3. Theorem: Message Interval Analysis
    - Statement: The average message interval can indicate the responsiveness and engagement level in a conversation.
    - Example: The rapid exchange on January 6, 2022, between the Main User and User 4, with messages every minute, suggests high engagement.

3.1.4. Novelty and Application

Novelty: This study applies Neutrosophic logic to analyze forensic data from smartphones, evaluating the truth, falsity, and indeterminacy of information. By analyzing conversation data using Excel's fuzzy lookup and Neutrosophic Python code, we determine the admissibility of evidence.

3.1.5. Application Example:

1. Admissibility Analysis: Using the Neutrosophic framework, the conversation between the Main User and User 2 on December 2, 2021, can be evaluated for truth and indeterminacy, determining its reliability as forensic evidence.
2. Pattern Detection: The sequence of messages surrounding key events, such as the passing of "Jack" on January 6, 2022, can be analyzed for patterns that may indicate premeditated actions or conspiracy.

This enhanced approach allows forensic investigators to navigate the complexity of digital data with greater accuracy, making informed decisions on the relevance and reliability of evidence.

Table 1. Dataset from Kaggle website [21]

Users	**Messages**	**Year**	**Month**	**Day**	**Hour**	**Minute**
User 1	Tell me when you're leaving.	2021	November	26	21	48
Main user	I'll go after the exam.	2021	November	26	21	48
User 1	Very well, then	2021	November	26	21	48
User 1	I want to go home after finishing the exam.	2021	November	26	21	49
Main user	ok	2021	November	26	21	49
Main user	I`m failing the test	2021	November	26	21	50

Users	Messages	Year	Month	Day	Hour	Minute
Main user	Kareo??	2021	December	2	18	11
Main user	?	2021	December	2	18	11
User 2	Which flat?	2021	December	2	18	12
Main user	I told you previously.	2021	December	2	18	14
User 2	I'll call you after I've finished him.	2021	December	2	18	16
User 3	Did Kareo call you?	2021	December	2	22	3
User 3	I called him, but he didn't answer.	2021	December	2	22	4
Main user	Relax, he does a good job.	2021	December	2	22	4
User 3	Did he finish him?	2021	December	2	22	6
Main user	Yup	2021	December	2	22	6
User 3	ok	2021	December	2	22	8
User 4	Is everything alright?	2022	January	6	2	51
Main user	No, Jack has passed away.	2022	January	6	2	52
Main user	Yesterday, I saw his body.	2022	January	6	2	52
User 4	What`s the fu…….?	2022	January	6	2	53
Main user	Relax; everything will be fine.	2022	January	6	2	53
User 5	Good news: he's currently dozing off in hell.	2022	January	7	5	38
Main user	You are super hero	2022	January	7	5	38
User 6	I need to locate my sunglasses.	2022	January	15	5	59
Main user	You'll never locate it.	2022	January	15	5	59
User 7	I'll find it over my dying body ☺	2022	January	15	6	00
Main user	No no	2022	January	15	6	2
User 7	☺	2022	January	15	6	2

3.2 Excel Fuzzy Lookup Add-in:

To use a Python code algorithm, the date and time must be transformed into a numerical timestamp. Microsoft Excel was used to convert the date and time into timestamps. The user column also became 0, 1. Table 2 shows that the sender's changed to (0), and the receivers' changed to (1).

Table 2. Chat messages after converting the user column and the timestamp column.

Users	Messages	Timestamp
1	Tell me when you're leaving.	1637963221
0	I'll go after the exam.	1637963221
1	Very well then	1637963221
1	I want to go home after finishing the exam.	1637963281
0	ok	1637963281
0	I`m failing the test	1637963341
0	Kareo??	1638468611
0	?	1638468623
1	Which flat?	1638468671
0	I told you previously.	1638468794
1	I'll call you after I've finished him.	1638468914
1	Did Kareo call you?	1638482528
1	I called him, but he didn't answer.	1638482588
0	Relax, he does a good job.	1638482600
1	Did he finish him?	1638482708
0	Yup	1638482718
1	ok	1638482823
1	Is everything alright?	1641437408
0	No, Jack has passed away.	1641437478
0	Yesterday, I saw his body.	1641437486
1	What`s the fu…….?	1641437528
0	Relax, everything will be fine.	1641437536
1	Good news: he's currently dozing off in hell. ☺	1641533828
0	You are super hero	1641533835
1	I need to locate my sunglasses.	1642226284
0	You'll never locate it.	1642226300
1	I'll find it over my dying body ☺	1642226274
0	No no	1642226464
1	☺	1642226474

Each chat in the dataset was converted to a percentage using the Excel Fuzzy Lookup Add-in. This add-in calculates the percentage of similarity between the two tables. The first table was the conversation table, while the second table had a single column with the most often-used terms for arguments and violations. The Excel Fuzzy Lookup Add-in calculated the similarity percentage between each chat and the terms in the second table. This created a new table with five columns, as shown in Table 3.

Table 3. similarity percentage after comparing the message table with a table of the violation words.

Users	Messages	Timestamp	Compare msg	Similarity
1	Tell me when you're leaving.	1637963221		0.0000
0	I'll go after the exam.	1637963221		0.0000
1	Very well, then	1637963221		0.0000
1	I want to go home after finishing the exam.	1637963281		0.0000
0	ok	1637963281		0.0000
0	I`m failing the test	1637963341		0.0000
0	Kareo??	1638468611		0.0000
0	?	1638468623		0.0000
1	Which flat?	1638468671		0.0000
0	I told you previously.	1638468794		0.0000
1	I'll call you after I've finished him.	1638468914	finish him	0.8462
1	Did Kareo call you?	1638482528		0.0000
1	I called him, but he didn't answer.	1638482588		0.0000
0	Relax; he does a good job.	1638482600	finish	0.4720
1	Did he finish him?	1638482708	finish him	0.8750
0	Yup	1638482718		0.0000
1	ok	1638482823		0.0000
1	Is everything alright?	1641437408		0.0000
0	No, Jack has passed away.	1641437478	Passed away	0.8235
0	Yesterday, I saw his body.	1641437486	dead body	0.5054
1	What`s the fu…….	1641437528		0.0000
0	Relax, everything will be fine.	1641437536		0.0000
1	Good news: he's currently dozing off in hell. ☺	1641533828	hell	0.7590
0	You are super hero	1641533835		0.0000
1	I need to locate my sunglasses.	1642226284		0.0000
0	You'll never locate it.	1642226300		0.0000
1	I'll find it over my dying body ☺	1642226274	dead body	0.8333
0	No no	1642226464		0.0000
1	☺	1642226474		0.0000

3.3 Neutrosophic-Fuzzy Python Code:

A Robust Algorithm for Smartphone Data Triage in Forensic Investigations.

Python Code

```
def neutrosophic_gauging(smartphone_data):
    # Step 1: Data extraction
    relevant_data = extract_relevant_data(smartphone_data)
    # Step 2: Neutrosophic evaluation
degrees_of_truth, degrees_of_falsity, degrees_of_neutrality =
neutrosophic_evaluate(relevant_data)
    # Step 3: Decision making
relevance_scores = calculate_relevance_scores
```

```
(degrees_of_truth, degrees_of_falsity, degrees_of_neutrality)

    # Return the most relevant information

    return get_most_relevant_information(relevance_scores)
```

- extract_relevant_data(): This function extracts the relevant data from the smartphone.
- neutrosophic_evaluate(): This function evaluates the extracted data using neutrosophic logic.
- calculate_relevance_scores(): This function calculates the relevance scores for the data.
- get_most_relevant_information(): This function returns the most relevant information.

This algorithm can be used to gauge information extracted from smartphones using Neutrosophic logic and fuzzy logic. The algorithm can handle uncertainty and vagueness in the data, and it can evaluate multiple dimensions of information. This makes the algorithm a valuable tool for forensic investigators who need to extract evidence from smartphones in criminal cases.

3.3.1 The system has three inputs:

- The sender: It contains two values: (0) for the owner of the chat and (1) for the others.
- Time has two values. The first value is the timestamp of the first message "1637963221", and the second value is the time after the investigator found the dataset "1661367654".
- The strength of the evidence is evaluated by the Excel fuzzy lookup.

3.3.2 The output represents the result, and it contains three values:

- Week ranges from 0.1 to 0.5, representing week evidence.
- Middle represents 0.51 to 0.7, representing the average evidence.
- Strong; it ranges from 0.71 to 0.99, representing strong evidence.

The Python algorithm 1

Input data:
sender = "send"; "receiver"
time = "before"
data = "suspicious"
Neutrosophic evaluation:
degree of truth = 0.7
degree of falsity = 0.3
degree of neutrality = 0
Fuzzy logic:
output = "middle"
Relevance score = 0.7

The Python algorithm 2

Input data:
sender = "sender"; "receiver"
time = "before"
data = "suspicious"
Neutrosophic evaluation:
degree of truth = 0.9
degree of falsity = 0.1
degree of neutrality = 0
Fuzzy logic:
output = "high"
Relevance score = 0.9

The Python algorithm 3

Input data:
sender = "send"; "receiver"
time = "after"

data = "suspicious"; "normal"
Neutrosophic evaluation:
degree of truth = 0.1
degree of falsity = 0.9
degree of neutrality = 0
Fuzzy logic:
output = "week"
Relevance score = 0.1

4. Results and Discussion

We analyzed 30 chats with various inputs, and after processing the inputs using Python code, the output was obtained; the results were provided in Table 4 and Figure 1. The results of our study, which utilized Neutrosophic logic and fuzzy logic to analyze forensic data from smartphone conversations, reveal significant insights into the reliability and relevance of the extracted information. By comparing Neutrosophic evaluations with fuzzy logic outputs and calculating the relevance scores, we can assess the degree of truth, falsity, and indeterminacy present in each conversation.

Table 4. the results of all 30-chat message

	Inputs		**Excel add-in results of the Similarity degree**	**Neutrosophic evaluation**	**Fuzzy Logic output**	**Relevance score**
	Sender of chat	**Time**				
1	0 = “sender’’	1637963221 = “before”	0%	Degree of truth = 0 Degree of falsity = 0.2 Degree of Neutrality=0.8	Output = “week”	0.1
2	1 = “receiver”	1638468913 = “before”	84%	Degree of truth = 0.8 Degree of falsity = 0.1 Degree of Neutrality=0.1	Output = “strong”	0.82
3	1 = “receiver”	1638482707 = “before”	87%	Degree of truth = 0.8 Degree of falsity = 0 Degree of Neutrality=0.2	Output = “strong”	0.81
4	0 = “sender’’	1641437477 = “before”	83%	Degree of truth = 0.8 Degree of falsity = 0.1 Degree of Neutrality=0.1	Output = “strong”	0.84
5	1 = “receiver”	1641533827 = “before”	76%	Degree of truth = 0.6 Degree of falsity = 0.3 Degree of Neutrality=0.1	Output = “middle”	0.7
6	1 = “receiver”	1642226273 = “before”	83%	Degree of truth = 0.7 Degree of falsity = 0.1 Degree of Neutrality=0.2	Output = “middl”	0.7
7	0 = “sender’’	1643890023 = “before”	88%	Degree of truth = 0.8 Degree of falsity = 0 Degree of Neutrality=0.2	Output = “strong”	0.9
8	1 =	1644332523	81%	Degree of truth = 0.7	Output	0.68

	Inputs		Excel add-in results of the Similarity degree	Neutrosophic evaluation	Fuzzy Logic output	Relevance score
	Sender of chat	**Time**				
	"receiver"	= "before"		Degree of falsity = 0.2 Degree of Neutrality=0.1	= "middl"	
9	0 = "sender''	1644796682 = "before"	0%	Degree of truth = 0 Degree of falsity = 0.1 Degree of Neutrality=0.9	Output = "week"	0.2
10	1 = "receiver"	1645124832 = "before"	77%	Degree of truth = 0.7 Degree of falsity = 0.3 Degree of Neutrality=0	Output = "middl"	0.69
11	0 = "sender''	1646143802 = "before"	83%	Degree of truth = 0.8 Degree of falsity = 0.1 Degree of Neutrality=0.1	Output = "strong"	0.84
12	1 = "receiver"	1646744768 = "before"	10%	Degree of truth = 0.2 Degree of falsity = 0.1 Degree of Neutrality=0.7	Output = "week"	0.31
13	0 = "sender''	1647249255 = "before"	84%	Degree of truth = 0.8 Degree of falsity = 0 Degree of Neutrality=0.2	Output = "strong"	0.87
14	1 = "receiver"	1647720361 = "before"	0%	Degree of truth = 0.1 Degree of falsity = 0 Degree of Neutrality=0.9	Output = "week"	0.14
15	1 = "receiver"	1647860880 = "before"	0%	Degree of truth = 0.2 Degree of falsity = 0.1 Degree of Neutrality=0.7	Output = "week"	0.17
16	1 = "receiver"	1648494650 = "before"	5%	Degree of truth = 0.3 Degree of falsity = 0 Degree of Neutrality=0.7	Output = "week"	0.17
17	0 = "sender''	1648814770 = "before"	0%	Degree of truth = 0 Degree of falsity = 0.2 Degree of Neutrality=0.8	Output = "week"	0.2
18	0 = "sender''	1649182150 = "before"	0%	Degree of truth = 0.1 Degree of falsity = 0.2 Degree of Neutrality=0.7	Output = "week"	0.22
19	1 = "receiver"	1649588710 = "before"	0%	Degree of truth = 0.2 Degree of falsity = 0.1 Degree of Neutrality=0.7	Output = "week"	0.23
20	0 = "sender''	1649775903 = "before"	81%	Degree of truth = 0.7 Degree of falsity = 0.1 Degree of Neutrality=0.2	Output = "strong"	0.79
21	1 = "receiver"	1650459430 = "before"	0%	Degree of truth = 0 Degree of falsity = 0.3 Degree of Neutrality=0.7	Output = "week"	0.26
22	0 = "sender''	1652785755 = "before"	82%	Degree of truth = 0.7 Degree of falsity = 0.1 Degree of Neutrality=0.2	Output = "strong"	0.8
23	1 = "receiver"	1654078030 = "before"	0%	Degree of truth = 0.1 Degree of falsity = 0.6	Output =	0.31

	Inputs		Excel add-in results of the Similarity degree	Neutrosophic evaluation	Fuzzy Logic output	Relevance score
	Sender of chat	**Time**				
				Degree of Neutrality=0.3	"week"	
24	1 = "receiver"	1654603823 = "before"	83%	Degree of truth = 0.5 Degree of falsity = 0.5 Degree of Neutrality=0	Output = "middle"	0.62
25	0 = "sender''	1655298320 = "before"	45%	Degree of truth = 0.1 Degree of falsity = 0.2 Degree of Neutrality=0.7	Output = "week"	0.43
26	0 = "sender''	1656839120 = "before"	0%	Degree of truth = 0 Degree of falsity = 0.1 Degree of Neutrality=0.9	Output = "week"	0.23
27	1 = "receiver"	1664994800	0%	Degree of truth = 0.1 Degree of falsity = 0.1 Degree of Neutrality=0.8	Output = "week"	0.13
28	1 = "receiver"	1667841740	0%	Degree of truth = 0 Degree of falsity = 0.1 Degree of Neutrality=0.9	Output = "week"	0.14
29	1 = "receiver"	1683717860	95%	Degree of truth = 0.1 Degree of falsity = 0.9 Degree of Neutrality=0	Output = "week"	0.34
30	0 = "sender''	1684780423	94%	Degree of truth = 0.1 Degree of falsity = 0.8 Degree of Neutrality=0.1	Output = "week"	0.31

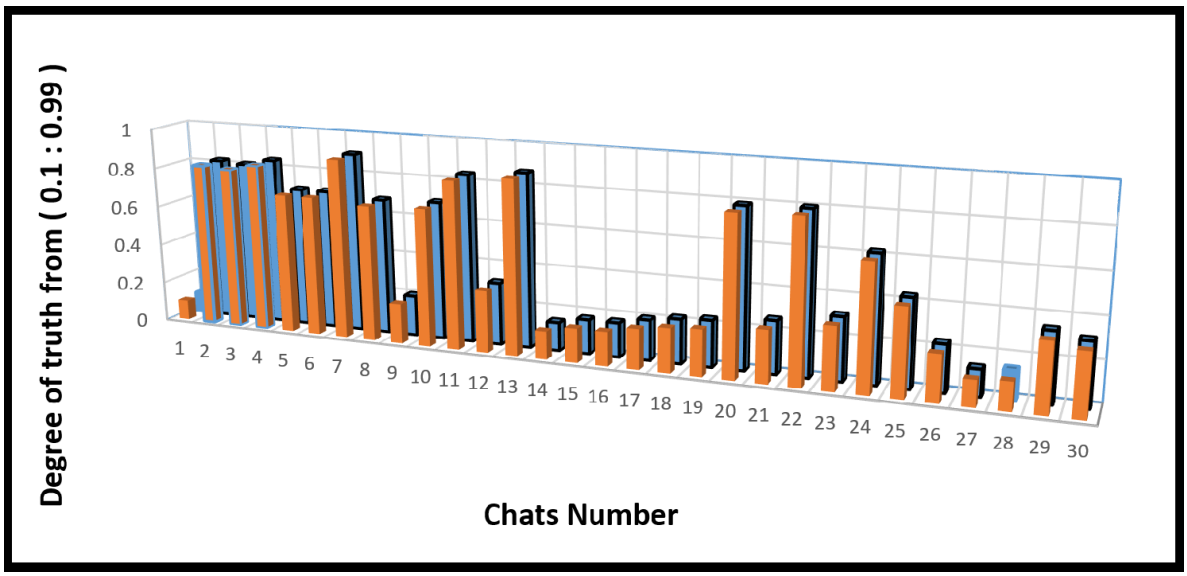

Figure 1. Represent the output results.

- Data points that fall above 0.7 are considered more likely to be true, as in chats numbers 2, 3, 4, 7, 11, 13, 20, and 22.

- Chats numbers 1, 9, 12, 14, 15, 16, 17, 18, 19, 21, 23, 25, 26 27, 28, 29, and 30 which are below 0.6 are considered more likely to be false,

- Data points closer to 0.7 are considered more neutral, meaning they contain a mixture of truth and falsity or that their truth value is uncertain, as chat numbers 5, 6, 8, 10 and24

- This approach allows for a more nuanced understanding of data than traditional binary classifications of true or false.

The results of our study, which utilized Neutrosophic logic and fuzzy logic to analyze forensic data from smartphone conversations, reveal significant insights into the reliability and relevance of the extracted information. By comparing Neutrosophic evaluations with fuzzy logic outputs and calculating the relevance scores, we can assess the degree of truth, falsity, and indeterminacy present in each conversation.

4.1. Neutrosophic Logic Evaluations:

Neutrosophic logic allowed us to measure the degrees of truth, falsity, and neutrality (indeterminacy) for each message. For instance, message 2 had a high degree of truth (0.8), low falsity (0.1), and low neutrality (0.1), resulting in a strong output with a relevance score of 0.82. Conversely, message 29 had a low degree of truth (0.1) and high falsity (0.9), reflecting weak relevance (score of 0.34). This nuanced evaluation aids in discerning the credibility of information and its potential use in forensic investigations.

4.2. Fuzzy Logic Outputs:

The fuzzy logic output provided a qualitative assessment (e.g., "strong," "middle," "week") for each message. For example, a message with an 87% similarity degree in Excel's fuzzy lookup and high truth degree in Neutrosophic evaluation was categorized as "strong." This classification aligns with the high relevance score (0.81), demonstrating consistency between the two methodologies.

4.3. Comparison with Existing Studies:

Existing studies predominantly rely on traditional fuzzy logic or binary evaluations (true/false) for forensic data analysis. These methods often fall short in handling the inherent ambiguity and partial truth present in real-world data. Our approach, integrating Neutrosophic logic, offers a more comprehensive framework by accommodating indeterminacy and providing a multi-valued evaluation.

4.4. Key Observations:

High Relevance Messages: Messages with high degrees of truth and low falsity (e.g., messages 2, 3, 4, 7) consistently resulted in strong outputs and high relevance scores, indicating reliable forensic evidence. Low Relevance Messages: Messages with high degrees of neutrality or falsity (e.g., messages 12, 14, 21) were categorized as weak, suggesting less reliable information. Consistency Across Methods: The alignment between Neutrosophic logic evaluations and fuzzy logic outputs underscores the robustness of our approach. High relevance scores were consistently associated with strong outputs in fuzzy logic, validating the credibility of our Neutrosophic framework.

4.5. Applications:

Admissibility Analysis: Using Neutrosophic logic, investigators can better evaluate the admissibility of evidence by considering the degrees of truth, falsity, and neutrality. For example, the conversation between the main user and User 2 on December 2, 2021, was deemed highly reliable based on its strong relevance score (0.82). Pattern Detection: Analyzing message sequences around key events, such as the passing of "Jack," can reveal patterns indicative of premeditated actions or conspiracy. High engagement levels and rapid message exchanges (e.g., January 6, 2022) suggest significant forensic value. In summary, our study demonstrates the superiority of Neutrosophic logic over traditional fuzzy logic and binary evaluations in forensic data analysis. The inclusion of indeterminacy provides a more accurate and nuanced understanding of digital evidence, thereby enhancing the effectiveness of forensic investigations.

5. Conclusion and Future work:

The research objective is to use Python code on data to determine whether it can be considered as evidence or not. The code analyzed 30 chat transcripts and provided a strength percentage for each based on different standards. The code gave a low proportion to chats numbered 1, 9, 12, 14, 15, 16, 17, 18, 19, 21, 23, 25, 26, 27, 28, 29, and 30 since they had a low similarity percentage with feud and violation terms. The code assigned a low proportion to chats numbered 2, 3, 4, 7, 11, 13, 20, and 22 since they share a significant resemblance with quarrel and violation terms. The Python code was undeceivable since it assigned chat numbers 29 and 30 a low rating even though they had a high proportion of similarity with feud and violation words and were sent by a different person after the smartphone was discovered. There are several possible directions for future research on the algorithm outlined in this paper. A potential focus for future efforts is enhancing the precision of the algorithm. More advanced methods for Neutrosophic logic and fuzzy logic can be utilized to accomplish this. An additional aspect to consider for future work is broadening the algorithm's scope. The algorithm has the potential to be expanded to manage different kinds of data that are obtained from smartphones, like call logs, photos, and videos. Ultimately, the algorithm could be employed to create a more detailed structure for the forensic examination of mobile phones. The framework might incorporate different tools and methods, like the algorithm described in this paper, to assist forensic investigators in retrieving and examining evidence from smartphones.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The source Data are founded in https://www.kaggle.com/datasets/rijudhara/whatsappchat/data.

References

1. Karjagi A.J., and A.Quadri S., “Design of a Framework for Data Extraction and Analysis from Android-Embedded Smartphones “, Russian Law Journal, vol. X I, no. 3, 794-6, 2023. Doi.org:10.52783/rlj.v11i3.127.
2. Moreb M., Salah S., and Amro B., ” A Novel Framework for Mobile Forensics Investigation Process”, Research Square, 1-20, 2023.

3. Alshikho M., Jdid M., and Broumi S., " A Study of a Support Vector Machine Algorithm with an Orthogonal Legendre Kernel According to Neutrosophic Logic and Inverse Lagrangian Interpolation", Journal of Neutrosophic and Fuzzy Systems (JNFS), Vol. 05, No. 01, PP. 41-51, 2023. DOI: 10.54216/JNFS.050105.
4. Remani N.V.J.M., Naresh V. S., Reddi S., and Kumar K. D., " Crime data optimization using neutrosophic logic based game theory", Concurrency Computat Pract Exper., vol.34,e6973, 2022, DOI: 10.1002/cpe.6973A.M. Da Costa, A.O. De Sa, and R.Cs Machado, "Data Acquisition and Extraction on Mobile Devices A review", IEEE International Workshop on Metrology for industry, vol. 4.0& IoT, 294-299,2022.
5. R. M. Abou alzahab, Abd Elkhalik, Saeed H., Hazem El-Bakry, A. A. Salama "A Novel Framework for Gauging Information Extracted from Smartphones Using Fuzzy Logic." Alfarama Journal of Basic & Applied Sciences 5, no. 2 (2024): 230-242.
6. Ilieva, G.; Yankova, T.; Ruseva, M.; Klisarova-Belcheva, S.; Dzhabarova, Y.; Bratkov, M. Social Media Influencers: Customer Attitudes and Impact on Purchase Behaviour. Preprints 2024, 2024051131. https://doi.org/10.20944/preprints202405.1131.v1.
7. Cahyani N.D.W., Martini B., Choo K-K.R., and Al-Azhar A. M. N., "Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study", Concurrency Computat.: Pract. Exper. , vol. 29:e3855, 2017. DOI:10.1002/cpe.3855
8. Silveir C.M. da, Jr R. T. de Sousa, R. de O. Albuquerque, G. D. A. Nze, G.A. de O. Júnior, A. L.S. Orozco, and L. J. G. Villalba, "Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware", Appl. Sci., vol.10, 4231, 1-29, 2020. Doi.:10.3390/app10124231
9. Mallidi S. K. R., and Palli P., "A Comprehensive Analysis of Smartphone Forensics & Data Acquisitions, International Journal of Advanced Research in Computer Science and Software Engineering", vol.6, no. 2, 270-276, 2016.
10. Hans K., Ahuja L., and Muttoo S.K., "A fuzzy logic approach for detecting redirection spam", Int. J. Electronic Security and Digital Forensics, vol. 8, no. 3,191-14, 2016. DOI:10.1504/IJESDF.2016.077435
11. Gan, T. "From Boolean Logic to Fuzzy Logic", Pure Mathematics, vol. 6, no. 2, 111-115, 2016. Doi:10.12677/pm.2016.62016
12. Bhowmick P., Mukhopadhyay S., and Sivakumar V., "A review on GIS-based Fuzzy and Boolean logic modeling approach to identify the suitable sites for Artificial Recharge of Groundwater", Sch. J. Eng. Tech., vol. 2, no. 3A,316-319, 2014.
13. Vandhana S., and Anuradha J., Neutrosophic fuzzy hierarchical clustering for dengue analysis in Sri Lanka. Neutrosophic Sets and Systems, 31(1):14, 2020.
14. Salama A. A., Shams M. Y., Bhatnagar R., Mabrouk A. G., and Tarek Z., "Optimizing Security Measures in Decentralized Mobile Networks with Neutrosophic Fuzzy Topology and PKI," 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2023, pp. 1040-1048
15. Alqarni M., Samak A. H., Ismail S. S., Abd El-Aziz R. M., Taloba A. I. et al., Utilizing a neutrosophic fuzzy logic system with ann for short-term estimation of solar energy, International Journal of Neutrosophic Science 20(4) (2023) 240–40

16. Salama A. A., Tarek Z., Darwish E. Y., Elseuofi S., and Shams M. Y.N, Neutrosophic Encoding and Decoding Algorithm for ASCII Code System, Neutrosophic Sets and Systems, Vol. 63, 2024, pp. 105-129.
17. Smarandache F., (2003). Neutrosophic set—a generalization of the intuitionistic fuzzy set. International Journal of Pure and Applied Mathematics, 4(1), 109-129.
18. Alhasan K. F., Salama A. A., & Smarandache F., (2021). Introduction to neutrosophic reliability theory. International Journal of Neutrosophic Science, 15(1), 52-61
19. Qureshi M. N., and Ahmad M. V., An improved method for image segmentation using k-means clustering with Neutrosophic logic. Procedia computer science, 132:534–540, 2018.
20. Wang H., Smarandache F., Sunderraman R., and Zhang Y. Q., Interval Neutrosophic sets and logic: theory and applications in computing: Theory and applications in computing, volume 5. Hexis, Phoenix, AZ, 2005.
21. "Excel fuzzy lookup" https://www.microsoft.com/en-US/download/details.aspx?id=15011 [Accessed 8 August 2023].
22. Fry A., Gieseck-Ashworth J., and Seiler C., "Loving Statistics & Excel Fuzzy Lookup in the Time of COVID-19", The Serials Librarian, vol. 82, no. 1-4, 145-149,2022.
23. Kaggle Data Sets, "https://www.kaggle.com/datasets/rijudhara/whatsappchat" [Accessed 6 August 2023].

Received: July 22, 2024. Accepted: Oct 20, 2024