НЕЙРОІНФОРМАТИКА ТА ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ

NEUROINFORMATICS AND INTELLIGENT SYSTEMS

UDC 004.9

OPTIMIZING AUTHENTICATION SECURITY IN INTELLIGENT SYSTEMS THROUGH VISUAL BIOMETRICS FOR ENHANCED EFFICIENCY

Batiuk T.– Postgraduate student of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine.

Dosyn D. – Dr. Sc., Professor of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine.

ABSTRACT

Context. The primary objective of this article is to explore aspects related to ensuring security and enhancing the efficiency of authentication processes in intelligent systems through the application of visual biometrics. The focus is on advancing and refining authentication systems by employing sophisticated biometric identification methods.

Objective. A specialized intelligent system has been developed, utilizing a Siamese neural network to establish secure user authentication within the existing system. Beyond incorporating fundamental security measures such as hashing and secure storage of user credentials, the contemporary significance of implementing two-factor authentication is underscored. This approach significantly fortifies user data protection, thwarting most contemporary hacking methods and safeguarding against data breaches. The study acknowledges certain limitations in its approach, possibly affecting the generalizability of the findings. These limitations provide avenues for future research and exploration, contributing to the ongoing evolution of authentication methodologies in intelligent systems.

Method. The two-factor authentication system integrates facial recognition technology, employing visual biometrics for heightened security compared to alternative two-factor authentication methods. Various implementations of the Siamese neural network, utilizing Contrastive loss function and Triplet loss function, were evaluated. Subsequently, a neural network employing the Triplet loss function was implemented and trained.

Results. The article emphasizes the practical implications of the developed intelligent system, showcasing its effectiveness in minimizing the risk of unauthorized access to user accounts. The integration of contemporary authentication methodologies ensures a secure and robust user authentication process.

Conclusions. The implementation of facial recognition technology in authentication processes has broader social implications. It contributes to a more secure digital environment by preventing unauthorized access, ultimately safeguarding user privacy and data. The study's originality lies in its innovative approach to authentication, utilizing visual biometrics within a Siamese neural network framework. The developed intelligent system represents a valuable contribution to the field, offering an effective and contemporary solution to user authentication challenges.

KEYWORDS: 2FA authentication, Siamese network model, Triplet Loss algorithm, facial recognition systems.

ABBREVIATIONS

SNN is a Siamese neural network;
TLA is a triplet Loss algorithm;
2FA is a two factor authentication;
CLA is a contrastive loss algorithm;
BI is a biometric identification;
DCM is a discrepancy classification matrix;
AIM is an anchor image scheme;
DF is a data frame;
FRT is a facial recognition technology.

NOMENCLATURE

Dw is an Euclidean distance;
I is a set of identifiers;
Y is a boolean image value;
M is a function looking for higher image identifier value from inputs;
m is a spare value that is less than 1;
p is a spare value that is higher than 0;
Gw are the coordinates of one point;
X is an image initial value;
N is a negative sample;
P is a positive sample;
A is an anchor sample;
f^a is an anchor function;
f^p is a positive function;
f^n is a negative function;
ω is a difference class operator;
$F\gamma$ is an approach that describes vector representation;

DOI 10.15588/1607-3274-2024-3-6

$F\mu$ is an approach that describes the pure entities interaction;

α is a parameter that determines the minimum distance among the positive and negative values;

C_l is a convolution layer;

P_l is a pooling layer;

D_l is a dropout layer;

F_l is a fully loaded layer;

H_λ is a hidden embedding;

C_α are convolution parameters;

P_β are pooling parameters;

D_k are dropout parameters;

χ_1 are user login and password;

χ_2 are generated cookies;

χ_3 are authentication data logs;

χ_4 is a user token;

χ_5 are the storage requirements;

λ_1 is a user identification operator;

λ_2 is a first factor authentication operator;

λ_3 is a second factor authentication operator;

λ_4 is an authentication verification operator;

λ_5 is an access permission operator;

φ_1 are rules and configurations governing the authentication process;

φ_2 are previously saved or registered credentials associated with the user account.

INTRODUCTION

In the context of the rapid evolution and integration of intelligent systems, the security and efficiency of authentication processes emerge as pivotal challenges. This article is dedicated to addressing these challenges by advancing authentication systems through the incorporation of sophisticated visual biometrics and contemporary machine learning methodologies. The primary objective is to develop an intelligent system utilizing a Siamese neural network to guarantee robust user authentication. Beyond the implementation of fundamental security measures like hashing and password storage, the adoption of two-factor authentication employing facial recognition technology is essential. This approach substantially elevates security levels, rendering many modern hacking techniques infeasible.

The primary aim of this research is to enhance authentication systems within intelligent frameworks by leveraging visual biometrics. The implementation of advanced authentication techniques is explored, specifically the adoption of a two-factor system employing facial recognition technology integrated with a Siamese neural network. The overarching goal is to establish a trustworthy, secure, and efficient intelligent system, mitigating the risk of unauthorized access and ensuring a high degree of user account protection. To systematically approach this objective, the main tasks are delineated. The foremost task involves creating and training a model for facial recognition using Siamese neural network technology. The rationale behind choosing a Siamese neural network is justified based on its efficacy in comparing two objects and generating vector representations, particularly crucial for biometric identification.

Architecturally, the Siamese neural network comprises two branches that learn collaboratively, processing two input images and producing vector representations of the system user's face. The utilization of the Triplet Loss function in training ensures that vector representations for the same user are proximate, while those for different users are distant.

The role of training and optimization is crucial when utilizing a dataset comprising pairs of face images for both training and testing phases. This process must be fine-tuned to adapt the model weights during training. Following the acquisition of a trained model, a distinct dataset is essential to validate the model's efficacy, ascertain the accuracy of face recognition, and evaluate the quality of the generated vector representations.

In the successful implementation of two-factor authentication, particularly emphasizing the technology of searching, recognizing, and comparing users' faces, several pivotal steps and details demand consideration. Defining specific security and speed requirements for the system is paramount. The choice of face recognition technology for the second stage of two-factor authentication needs careful consideration. With an understanding of the chosen technology, developing a mechanism for searching, recognizing, and comparing faces and seamlessly integrating it with the Siamese neural network is imperative. The implementation of two-factor authentication, where the first factor is the login and password, and the second is facial recognition, constitutes a crucial part of the process. Once a functional model of two-factor authentication is established, optimizing existing biometric identification methods becomes necessary. This involves exploring the latest advancements in biometric identification and selecting optimal means of authentication to enhance accuracy and speed.

The final significant step involves integrating the neural network into the intelligent system. This encompasses creating an interface for seamless interaction between the neural network and the intelligent system, ensuring the automated operation of the system utilizing facial recognition for authentication and storing user data in the database. Consideration must be given to storing not only general user information but also a photo of the user's face and its factors, facilitating a subsequent comparison with the user's webcam image during logins. Once a fully functional system is in place, thorough evaluation and testing across diverse datasets and conditions become crucial. This process enables data collection on system performance, allowing for an assessment of accuracy and security, including potential vulnerabilities to attacks and challenges. Each stage is meticulously designed to culminate in the development of an effective and secure authentication system based on facial recognition and advanced biometric identification methods.

DOI 10.15588/1607-3274-2024-3-6

The scientific paper outlines an innovative approach in the development of an intelligent system, amalgamating advancements in biometric identification and machine learning. A notable innovation lies in the utilization of a Siamese neural network for facial recognition, a method designed to account for each user's unique features, thereby ensuring heightened identification accuracy. The implementation and training of this neural network using the Triplet Loss Function represent a groundbreaking step in enhancing biometric methods. Furthermore, the incorporation of face search, recognition, and comparison technology into the framework of two-factor authentication introduces an additional layer of innovation, elevating the security level by making visual biometrics a more dependable and secure authentication method.

The scientific endeavor also dedicates attention to optimizing biometric identification methods through the application of advanced algorithms and techniques, thereby contributing to the increased accuracy and efficiency of face recognition. The integration of various stages, including neural network development, two-factor authentication implementation, and biometric identification optimization, into a unified intelligent system exemplifies an innovative strategy in addressing security and authentication challenges within intelligent systems. This comprehensive scientific approach aims to create an effective and reliable system capable of minimizing the risk of unauthorized access and ensuring a high level of user security.

1 PROBLEM STATEMENT

The intelligent system of optimizing authentication security through visual biometrics is represented by a tuple simulation model:

$$N = < Dw, I, Y, M, Gw, X, F\gamma, F\mu >,$$

where $Y = \{y_1, y_2, y_3, y_4\}$, $X = \{x_1, x_2, x_3, x_4\}$, $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$, $\Phi = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.

A SNN type of neural network architecture consisting of two identical subnetworks with shared parameters. It is designed for tasks involving the comparison of input patterns to determine their similarity or dissimilarity:

$$C_l = f^a \circ f^p \circ f^n,$$
$$P_l = m(p(\omega(\varphi_1, \varphi_2, \varphi_3), \chi_1, \chi_2), \lambda_1).$$
$$D_l = F_l \circ H_\lambda \circ m,$$

A TLA loss function train models for comparing objects in vector space: $C_\alpha = \omega \circ p \circ m$, so

$$P_\beta = f^a(f^p(f^n(C_\alpha, \chi_3, \chi_4, \chi_5), \lambda_4, \lambda_5), \varphi_2).$$

A security 2FA process that requires two forms of identification before granting access to an application:

$$D_k = \alpha \circ \omega \circ p \circ H_\lambda,$$
$$M = \lambda_1(\varphi_2(\lambda_2(\varphi_4(y_1, x_1), y_2), x_2), \varphi_1).$$

The DCM matrix is evaluating classified instances of the performance of classification models:

$$F\gamma = C_l \circ P_l \circ D_l \circ F_l,$$
$$F\mu = y_3(\lambda_3(y_4(\lambda_4(C_\alpha, P_\beta), D_k), x_3), \varphi_4).$$

2 REVIEW OF THE LITERATURE

The publication [1] has significantly contributed to the field of cybersecurity and automated vulnerability detection. The authors advocate for the application of graph neural networks to automatically assign Common Weakness Enumeration identifiers to vulnerabilities. A notable strength of the article lies in the utilization of graph neural networks, enabling the model to effectively scrutinize the relationships among various vulnerabilities and their characteristics. Employing graph structures holds the potential to enhance the precision of vulnerability identification and classification. The authors showcase a well-articulated overview of existing methods for vulnerability detection and CWE identifier assignment, reflecting their profound understanding of the domain. While the proposition to employ graph neural networks in this context is original and promising, a more comprehensive discussion on the limitations and potential risks associated with this approach would be beneficial. Additional insights into specific parameters of graph neural networks, as well as details on training and validation methods, would enhance the reader's comprehension of model stability and robustness. The paper introduces an innovative perspective on vulnerability detection and automated CWE identifier assignment.

On a separate note, work [2] introduces a novel approach to developing an intelligent system for socialization, considering personal interests and leveraging SEO technologies and machine learning methods. The article's positive aspects include the incorporation of SEO technologies within a social platform for user interaction and the application of machine learning methods for analyzing and recommending personal interests, showcasing the authors' high level of technical competence. The structured and logically presented information enables readers to easily grasp the concepts discussed. However, to enrich the understanding of the technical implementation of the intelligent system, more specific details are warranted. These could encompass insights into the chosen machine learning algorithms, the rationale behind selecting SEO technologies, and their significance in this particular context.

In the publication [3], the authors delve into the application of Siamese Trackers based on deep features for visual tracking tasks. The article underscores crucial aspects of utilizing deep features and Siamese models to enhance the precision and efficiency of object tracking

DOI 10.15588/1607-3274-2024-3-6

within a video stream. The strengths of the article include a lucid problem formulation and the apt choice of Siamese Trackers for addressing visual tracking challenges. Notably, the rationale behind employing deep features, enabling high tracking accuracy in diverse conditions, deserves special attention. The authors provide a comprehensive review of various facets of Siamese Tracker implementation, encompassing deep network architectures, loss functions, and model updating methods. This renders the article valuable for both researchers and practitioners seeking advancements in visual object tracking technologies. Additionally, it's worth mentioning that the paper could further elevate its value through subsequent research that compares Siamese Trackers [4] with contemporary visual tracking methods, evaluating their effectiveness under different conditions. This work constitutes a significant contribution to the field of visual tracking, leveraging Siamese Trackers and deep features to enhance real-world object tracking outcomes.

In the context of the publication [5], the authors explore a crucial aspect of employing Siamese neural networks in regression and uncertainty quantification tasks. They introduce a novel approach to enhance Siamese neural network performance through similarity-based pairing. A key strength of this work lies in the successful integration of the similarity concept to bolster the accuracy and reliability of Siamese neural networks in regression tasks. The authors conduct a thorough analysis of the impact of various pairing methods on results, showcasing that similarity-based pairing contributes to enhanced neural network performance. An additional merit of the article is the exploration of Siamese neural networks for uncertainty quantification, a current research frontier. The presentation of compelling results and the indication of using similarity to enhance uncertainty estimation reliability in regression problems make this article a valuable addition to the methodology of employing Siamese neural networks in regression and uncertainty quantification. Similarity-based pairing emerges as an effective approach for enhancing their performance.

In their publication [6], the authors introduce an innovative method for detecting clones in Java code using a Siamese neural network based on bytecode. The article meticulously explores the challenge of identifying clones in software, a critical task in software development and maintenance. Notably, the use of bytecode to represent Java code and the application of a Siamese neural network for discerning similarities between code segments are key strengths. This approach allows consideration of both structural and semantic aspects of clones, potentially enhancing detection accuracy. An additional advantage lies in the implementation of a Siamese neural network method for bytecode comparison, facilitating the identification of more complex clone forms, including altered clones that traditional methods might struggle to detect. The work also provides a comprehensive overview of current clone detection methods, comparing their advantages and disadvantages, making it valuable for readers familiar with the field. The clear and logical structure of the article aids in understanding the methodology and results. Well-defined experimental stages and obtained results substantiate the efficacy of the proposed method. This article [7] introduces an intriguing and promising approach to clone detection in Java code using Siamese neural networks based on bytecode, potentially contributing significantly to the field of software analysis.

In the case of the publication [8], the article addresses the challenge of object visual tracking and proposes an effective and resource-efficient method using the differentiated search of neuroarchitecture approach. The focus is on achieving high tracking efficiency with limited computing resources. A notable strength is the utilization of the DNAS method to autonomously identify the optimal neuroarchitecture for visual tracking tasks. This automated model selection process is crucial for achieving efficiency within resource constraints. The article [9] elaborates on the differentiated neuroarchitecture search and model lightness approaches in detail to ensure high real-time performance. The authors introduce effective mechanisms for reducing model volume and computational complexity, making it adaptable to variable conditions. The results achieved demonstrate a commendable level of efficiency and speed for the proposed method compared to other visual tracking approaches. Experimental findings further affirm the competitiveness of the developed model.

3 MATERIALS AND METHODS

During the course of this project, it is essential to delineate two primary objectives. Firstly, it involves the creation, training, and testing of a Siamese neural network tasked with two main functions: detecting a face in a user's photo and comparing two photos to ascertain the user's authenticity during login attempts. Secondly, the focus shifts to implementing the developed neural network within the intelligent system [10] and configuring its seamless operation as a two-factor authentication module for users.

The Siamese neural network belongs to a distinctive class of deep neural networks crafted specifically for tackling comparison tasks. Its nomenclature draws parallels with "Siamese twins", reflecting a shared origin but individual characteristics. The fundamental concept behind a Siamese neural network is to learn the similarity or dissimilarity between two input patterns. The architecture comprises two or more identical subnets that share parameters. Each subnet processes a distinct input sample, extracting its crucial features. The resulting representations are then compared to discern similarities or differences between the input data. A primary application of Siamese neural networks [11] lies in visual comparison tasks, encompassing activities like face recognition, object detection, and addressing tracking challenges. The architecture facilitates the study of neural representations to gauge the similarity degree between

DOI 10.15588/1607-3274-2024-3-6

two input samples, rendering it effective for comparison and classification tasks. For our implementation, we employ an input layer followed by a 2D convolutional layer and a 2D pooling layer [12]. The data undergoes smoothing, and a compression layer is introduced. Ensuring the optimal functioning of this layer involves normalizing its values. The object size is set at 128 units. Combining these two models involves utilizing the scalar product of objects. Given that the features are already normalized, their values fall within the 0 to 1 range, facilitating straightforward comparisons with the target labels.

The contrast loss function [13] exhibits certain drawbacks that necessitate consideration. Notably, it is sensitive to hyper-parameters, implying that its effectiveness hinges on factors such as the distance between positive and negative samples, demanding meticulous tuning. Achieving a balance between positive and negative pairs is essential for the effective training of the contrast loss function, a task that can prove challenging with real data. The computational burden escalates significantly when dealing with a large number of pairs, especially in scenarios involving extensive data volumes and intricate models. Furthermore, the quality of vector representations provided by the model markedly influences the outcomes of the contrast loss function; inadequate learning of useful features by the model can result in suboptimal results.

In the context of a large number of classes, the selection of effective pairs for comparison becomes challenging, potentially impeding the effectiveness of the learning process. Therefore, for optimal performance, it is advisable to consider a more contemporary function, such as the triplet loss function (Triplet loss function [14]). This type of loss function is frequently employed in Siamese neural networks to train models for comparing objects in vector space. The fundamental concept behind the triplet loss is to ensure that vector representations of similar objects are in close proximity, while vector representations of dissimilar objects are distinctly separated in space.

The triplet loss function takes into account three samples: a positive and a negative sample for a specific object, along with a negative sample for another object (trivially negative). The objective is to minimize the distance between the vector representations of the positive and anchor (trivially negative) patterns, simultaneously increasing the distance between the vector representations of the anchor and the complex negative pattern. Figure 1 provides a conceptual illustration of the triplet loss function, featuring a pivotal input [15] (anchor), as well as positive and negative objects at the input.

Figure 1 illustrates a diagram outlining the process of initializing two-factor authentication for users in the intelligent system. This involves capturing an image, conducting a facial recognition search, and subsequently storing the media key in the database.

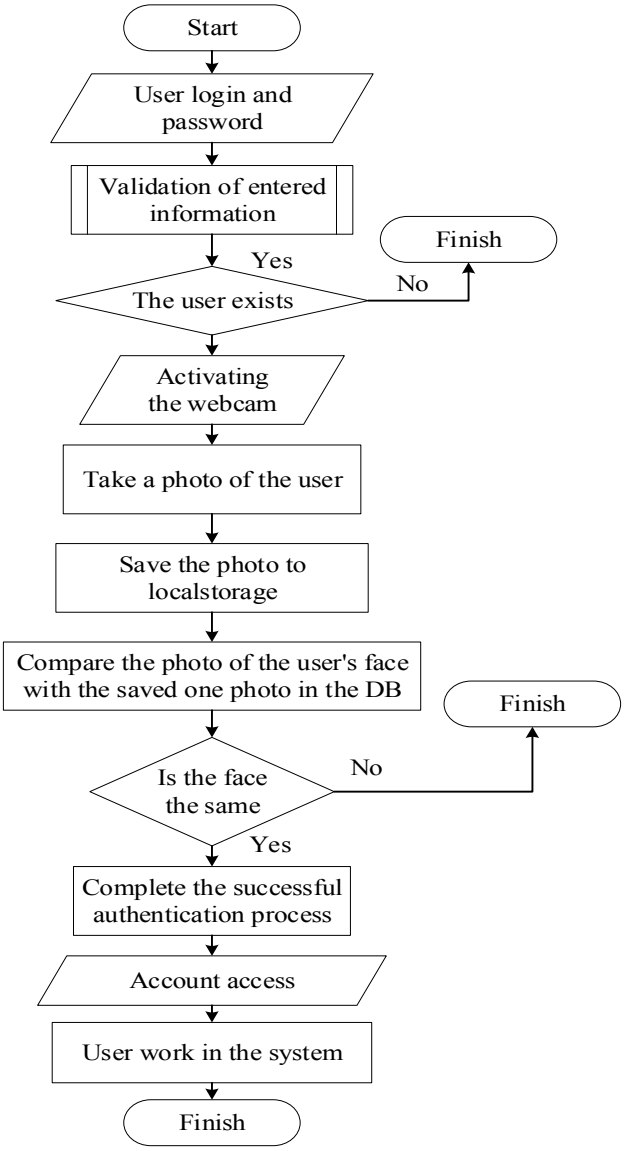

Figure 1 – Process of initializing two-factor authentication

Figure 2 depicts a diagram detailing the user authentication process. This process involves validating the entered login and password, saving the user's photo, captured using a web camera, in local storage, and comparing the current photo with the one already stored in the database [16] containing the user's facial information. In the event of a successful match, the user gains access to the available functionality within the intelligent system.

The Siamese neural network with a triplet loss function offers several advantages, particularly its efficacy in handling limited data by utilizing three images for training instead of pairs. This model [17] can effectively generalize features crucial for distinguishing various classes or instances in input data. The triplet loss function addresses the challenge of managing similarity and dissimilarity in the feature vector space by minimizing the distance between positive pairs and maximizing the distance between negative pairs. Its

DOI 10.15588/1607-3274-2024-3-6

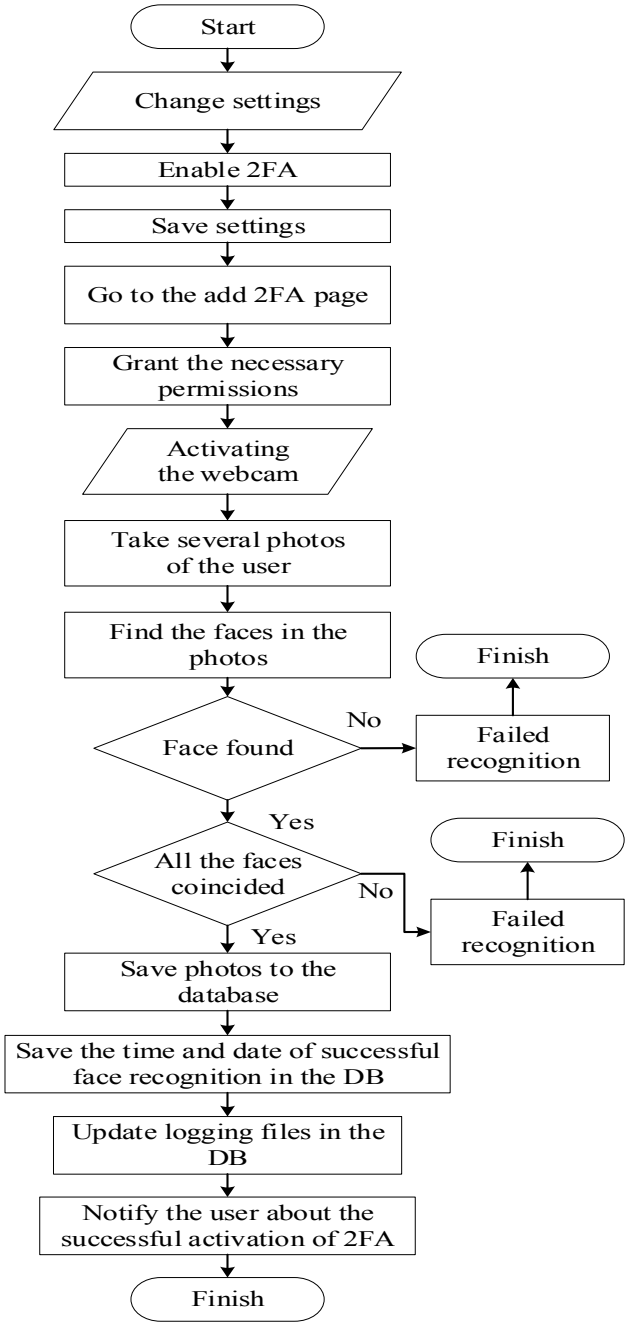

Figure 2 – The user authentication process

versatility makes the model suitable for various tasks, including face recognition, object extraction, or pattern recognition, aligning well with our requirement for a unified format [18] for processing user photos and extracting facial features.

However, there are certain drawbacks to the Siamese neural network with a triplet loss function. The model's sensitivity to hyper-parameter choices, such as triplet size and parameters of the triplet loss function, may necessitate additional tuning. While this is not critical within the scope of the intelligent system being developed, as it will process standardized photos, it should be initially configured. Dealing with a large amount of data [19] may pose challenges in selecting effective triplets for learning, potentially leading to increased computational complexity. However, this is not a significant concern for the current system, as it processes only two photos at a time for each user—the current photo captured using a web camera and a photo saved in the database. In the case of improper triplet selection for training, the model may not be efficiently trained, and, conversely, like many other models, Siamese neural networks may be susceptible to overfitting [20], especially with limited data. This consideration is crucial when implementing the Siamese neural network and selecting datasets for model training.

4 EXPERIMENTS

Throughout the project, a pivotal task involves the creation of a Siamese neural network, which, following testing, will be integrated into an intelligent system. The implementation will be carried out using the Python 3.10 programming language, and the PyCharm IDE has been selected for code development. The initial step encompasses downloading a dataset comprising photos and corresponding user labels essential for training and testing the neural network. The dataset encompasses a total of 5000 images featuring 50 unique elements [21], signifying 50 users with facial images captured from various angles and expressing different emotions. Each image measures 128 by 128 pixels and features a black background behind the user faces. Moreover, all images are presented in grayscale. The pixel values have been scaled to fit within the interval from 0 to 1, and each user in the dataset has been assigned a corresponding ID ranging from 0 to 49.

Following that, the data undergoes reformatting, wherein each image in the dataset is transformed into a one-dimensional array of size 4096 * (128 * 128). The training and test datasets are constructed by partitioning images [22] from the initial dataset. Additionally, a DataFrame is established, encompassing subject IDs for the training dataset. A DataFrame, a primary data structure in the pandas library for data processing and analysis, structures data in a two-dimensional array akin to a table, facilitating the organization of data into rows and columns. Each row in the DataFrame corresponds to a single sample in the training dataset, playing a crucial role in the subsequent exploration and analysis of dependencies between subject identifiers and properties and indicators in the neural network.

The subsequent step involves the generation of triplets for application in a Siamese neural network. A function is crafted, taking three arguments: the path to the image directory, a dictionary where keys represent folders (classes) and values signify the number of files in each folder, and the maximum number of files to consider for each folder. An empty list is initialized to store the triplets, and a list of all created folders [23] is formed based on the dictionary keys. Tuples for the anchor and positive image within the current folder at specified indices are implemented, and a variable for the negative image folder is assigned, initially equal to the current

DOI 10.15588/1607-3274-2024-3-6

folder. Tuples for positive and negative images are selected, and all triplets are appended to the collective list. Ultimately, the program function returns a list comprising all created triplets.

Figure 3 depicts a diagram illustrating the projection of people's faces onto a plane using the principal component analysis method. Each point on the diagram corresponds to an individual's face, with the two axes representing the first two principal components determining the primary directions of variation among the face images. The X-axis corresponds to the first principal component, and the Y-axis to the second principal component. Each point represents the face of a specific individual, and the placement of dots signifies facial variations within the sample. Proximity between points [24] indicates facial similarity, while distance signifies facial diversity. Different colors denote distinct individuals, distinguished by identifiers, providing a visually clear demarcation between different persons.

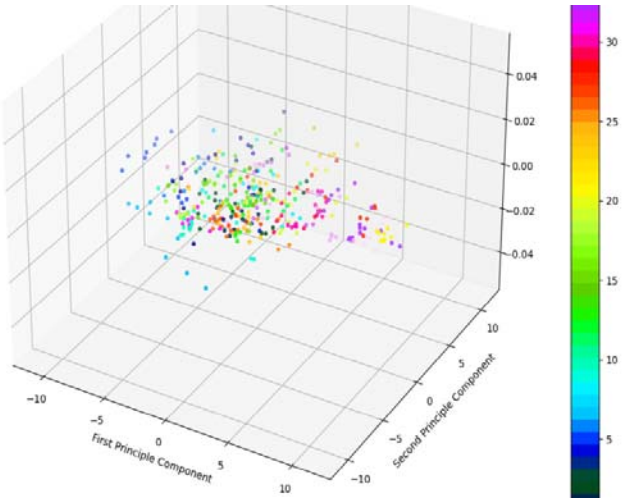

Figure 3 – Projection of people's faces using the principal component analysis method

Subsequently, it is imperative to define various functions and models for implementing a Siamese neural network with a triplet loss function. A function was crafted to retrieve a batch of image triplets, taking into account a list of triplets, the number of triplets in each batch, a boolean value indicating whether image preprocessing should occur. Calculations were made to determine the number of steps required to obtain all batches of triplets [25], and lists for the anchor, positive, and negative images in the current batch were initialized. The anchor, positive, and negative images for the current triplet were retrieved, and images for each category were added to their respective lists. This process yielded a batch of triplets in (128, 128, 3) format suitable for utilization in a neural network. Following the creation of a function to obtain an image coding model (feature extractor), a class was implemented to compute distances between coded images.

With the function in place for acquiring the image coding model, another function was introduced to obtain a Siamese neural network based on the coding model and a specialized distance layer. This resulted in the acquisition and testing of a Siamese neural network model. Figure 4 depicts a diagram illustrating the discrepancy matrix for classification results using the feature extractor method based on distances between coded images. Along the horizontal and vertical axes are user face numbers [26] corresponding to different faces. Each matrix cell denotes the number of faces that were correctly classified (on the diagonal) or incorrectly classified (off the diagonal). The color of each cell signifies the number of faces classified for the corresponding image pair (anchor class, predicted class), with darker colors indicating a higher number of faces in the corresponding class. This matrix facilitates the evaluation of how effectively the model classifies faces for each individual.

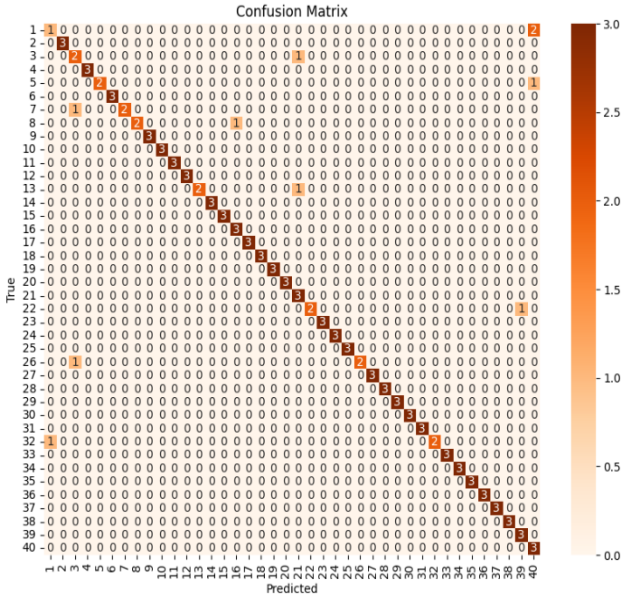

Figure 4 – Discrepancy matrix for classification results

The subsequent step involved declaring a Siamese neural network model class, creating a corresponding class that inherits from the general data model class of the TensorFlow library, and defining methods for training and testing the model, calculating losses, and initializing parameters. An object of the Siamese neural network model class was instantiated, and an optimizer with specific parameters was defined. With a completed model, a testing function for triplets was defined, evaluating the model's accuracy [27] on test triplets. This evaluation included accuracy on the test set of triplets and the average values of distances for correct and incorrect pairs. The training process was conducted for a specified number of epochs, specifically 512 epochs. For each epoch, calculations were performed on the derived value of the average loss of the training set of triplets.

5 RESULTS

The model underwent testing on a set of triplets, and various metrics such as accuracy, average distances, and standard deviations were computed. Model weights were

DOI 10.15588/1607-3274-2024-3-6

saved upon improvement in accuracy on the test set, and the final step in training involved saving the ultimate model weights after completing all epochs. The primary objective [28] was to train a Siamese neural network utilizing a triplet loss function to address the task of comparing a user's face in two photos and determining whether the response is positive or negative within a specified context. The model endeavors to minimize losses for correct pairs of user faces (anchor positive images) and maximize distances for incorrect pairs of user faces (anchor negative images).

Figure 5 illustrates a diagram depicting a curve, where the X-axis represents completeness, and the Y-axis represents accuracy. Each point on this curve corresponds to a specific decision threshold for the classification model. Accuracy indicates the fraction of positive cases correctly labeled by the model, while completeness denotes the fraction of positive cases actually detected by the model. The accuracy-completeness [29] curve elucidates how accuracy and completeness evolve at different thresholds for solving the problem. The area beneath this curve serves as an indicator of the model's quality, with a larger value signifying better performance. Additionally, the diagram highlights the area between the curve and the X-axis, colored purple, signifying the average accuracy score averaged across all classes.

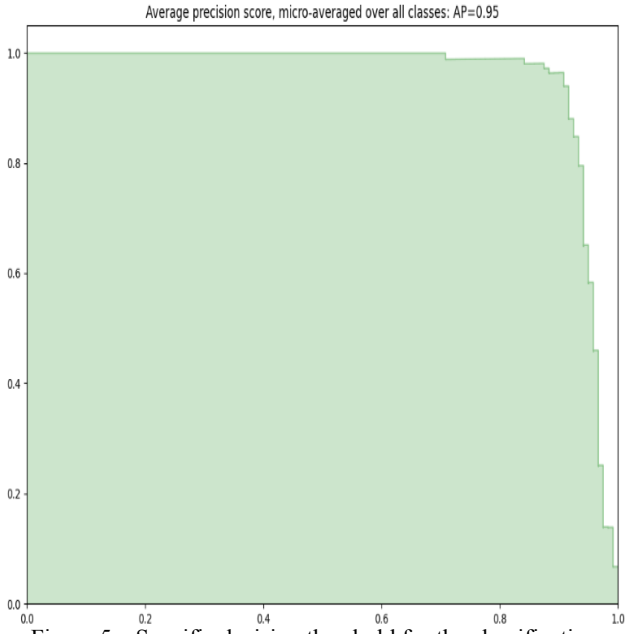

Figure 5 – Specific decision threshold for the classification model

Figure 6 illustrates an instance of a comparison between the anchor image and the input similarity check function. As evident from the figure, the two photos depict the same user, leading to a positive prediction. Within this display, each pixel is represented by a shade based on the magnitude of the difference between corresponding pixels in the first two images.

Darker areas signify less difference, while lighter areas indicate greater dissimilarity. Consequently, this analysis helps ascertain whether the photos represent the same person.

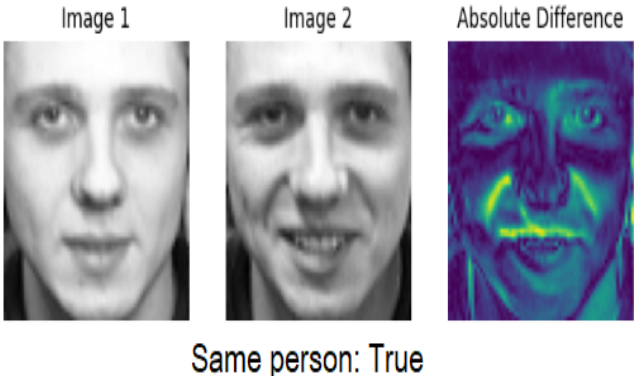

Figure 6 – Comparison between the anchor image and the input similarity check function

6 DISCUSSION

A novel encoding function was devised, building upon the architecture of the original encoding model. This process involved traversing the coding layers of the initial model and transferring their weights to equivalent layers in the new encoding structure. The weights of the resulting encoded model were saved, and a description of the encoding layer's architecture was generated. After obtaining embeddings for the provided sets of facial images, the squared distance between face embeddings was computed, and classification was carried out based on a threshold value, yielding an array with predictions of 0 or 1. Two lists of predictions [30] (positive and negative) were generated, corresponding to similar and dissimilar pairs of user faces. All available test triplet packages underwent testing, and an image classification function was implemented to derive predictions for positive (similar) and negative (dissimilar) pairs of user faces. The final step in assessing the Siamese neural network with triplet loss function involved invoking the metrics function to evaluate and visualize the model's performance.

The relationship between training losses and the number of iterations is a critical aspect of understanding the behavior and performance of machine learning models. In Figure 7, each data point represents the loss at a specific iteration, providing insight into the model's convergence and learning process. On the horizontal axis, we have the iterations or steps involved in the training process. These iterations typically correspond to epochs in the context of deep learning models, where one epoch refers to a complete pass through the entire training dataset. As training progresses, the model adjusts its parameters to minimize the loss function, aiming to improve its predictive capabilities. The vertical axis displays the corresponding loss values at each iteration. These losses represent the discrepancies between the model's predictions and the actual target values in the training data. Lower loss values indicate better alignment

DOI 10.15588/1607-3274-2024-3-6

between predictions and targets, reflecting improved model performance.

The depicted loss function undergoes a hyperbolic decline in the initial iterations, showcasing rapid improvement as the model learns from the training data. This phase of rapid reduction in loss signifies the model's ability to capture relevant patterns and features from the data. However, as training continues, the rate of decrease in loss gradually diminishes, eventually reaching a plateau. This plateau indicates that the model has learned most of the salient features present in the training data, and further adjustments to parameters yield diminishing returns in terms of reducing loss. The stabilization of losses on the plateau suggests that the model has converted to a stable solution, where further training iterations are unlikely to significantly improve performance on the training data. Analyzing this convergence behavior provides valuable insights into the training dynamics and helps assess the overall efficacy of the training process. In summary, the visualization of training losses over iterations serves as a powerful tool for monitoring model training, understanding convergence behavior, and evaluating the effectiveness of machine learning algorithms.

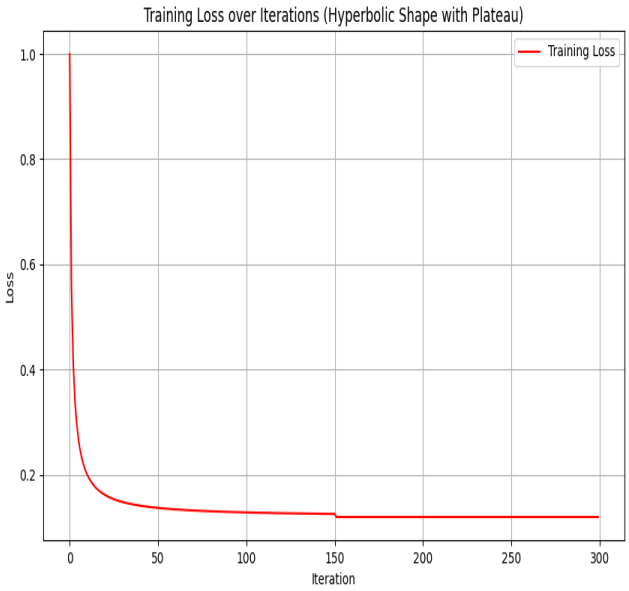

Figure 7 – Training Loss over iterations

In Figure 8 the ROC (Receiver operating characteristic curve) is used to evaluate the performance of a binary classification model across different thresholds. It plots the true positive rate (sensitivity) against the false positive rate (1 – specificity) for various threshold values. It helps in visualizing the trade-off between sensitivity and specificity of a classifier across different threshold values. The ROC curve is particularly useful when you need to understand how well a classifier can distinguish between two classes. Imbalanced datasets are common in many real-world applications, including biometric recognition tasks addressed by Siamese networks. The ROC curve remains a valuable tool for evaluating model performance in such scenarios. It allows practitioners to assess the classifier's ability to correctly classify both rare and abundant classes, ensuring robust performance across the entire spectrum of class distributions.

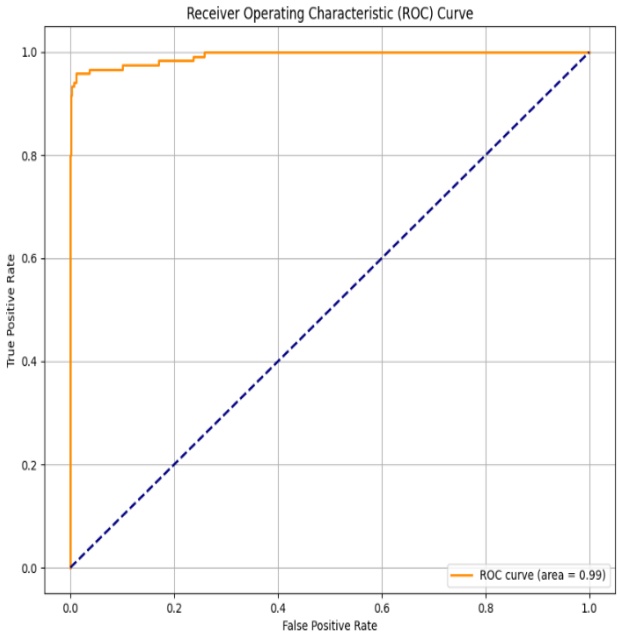

Figure 8 – The performance of a binary classification model across different thresholds

The precision-recall curve in Figure 9 illustrates the trade-off between precision and recall for different threshold values of a classifier. It provides insights into the classifier's performance, particularly in cases of class imbalance where the positive class is rare. The precision-recall curve is more informative when dealing with imbalanced datasets, as it focuses on the positive class prediction accuracy.

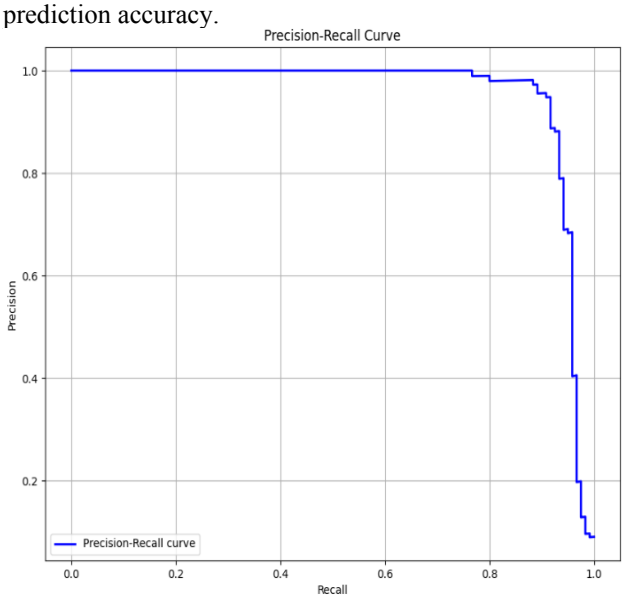

Figure 9 – Trade-off between precision and recall for different threshold values

DOI 10.15588/1607-3274-2024-3-6

Learning curves provide insights into how well a Siamese Neural Network is learning from the training data and how its performance generalizes to unseen validation data as the amount of training data increases. These curves help diagnose potential issues related to model bias or variance, which are crucial for optimizing the SNN's performance.

The blue line represents the average training accuracy of the SNN as a function of the number of training samples. It shows how well the model fits the training data. The green dashed line illustrates the average validation accuracy of the SNN across different training sample sizes. It indicates how well the model generalizes to unseen data.

The shaded regions around the mean lines (blue and green) represent the variability or uncertainty in the accuracy estimates. They are computed as the standard deviation of the accuracy scores across different cross-validation folds. If both the training and validation accuracies are low and converge to a similar value, it suggests that the model may have high bias. In the context of SNNs, this could mean that the network architecture or complexity is insufficient to capture the underlying patterns in the data.

A significant gap between the training and validation accuracies indicates potential overfitting. If the training accuracy is substantially higher than the validation accuracy, it suggests that the model is memorizing the training data and failing to generalize to new data points.

Learning curves help determine the optimal amount of training data required to achieve satisfactory performance. If the validation accuracy plateaus or starts decreasing with additional training data, collecting more data may not be beneficial. If the SNN exhibits high bias, increasing model complexity, adding more layers, or tuning hyper-parameters may help improve performance.

To address overfitting, techniques such as regularization, dropout, or reducing model complexity can be employed. Additionally, collecting more diverse training data or applying data augmentation techniques may also help. In Figure 10 X-axis label denotes the quantity of data used for training the SNN.Y-axis label represents the model's classification performance.

CONCLUSIONS

Throughout the research and development of an authentication system utilizing visual biometrics with a Siamese neural network, a thorough analysis of security aspects and the effectiveness of the authentication process in intelligent systems was undertaken. A pivotal step in this research involved exploring and weighing alternatives to implementing the Siamese neural network, considering both the contrast loss function and the triplet loss function. Through an examination of existing scientific literature, the principal advantages and drawbacks of Siamese neural network loss functions were identified. It was crucial to discern the optimal method for integrating the neural network into an intelligent system. Consequently, the triplet loss function emerged as the preferred choice for training the model, ensuring a high level of accuracy in user face recognition.

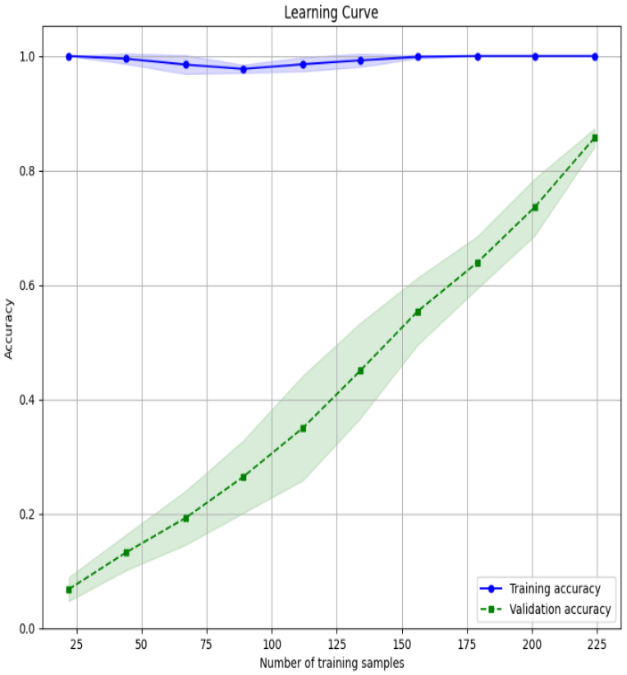

Figure 10 – Model's performance on the training and validation sets as a function of training instances

The essential characteristics of Siamese neural networks were elucidated using diagrams, outlining the operation of the neural network as both a monolithic element and a service within an intelligent system. Block diagrams and a sequence diagram were employed to illustrate the system's operational algorithm and the HTTP requests between its components. Following conceptual design, the programming code was crafted, and a Siamese neural network with a triplet loss function was trained and tested.

This network exhibited dual functionality, capable of both searching for a user's face in a single photo and comparing multiple photos to determine if they belong to the same user-an imperative requirement for the seamless integration of a neural network into an intelligent system. Moreover, the system's capabilities were expanded to include two-factor authentication, employing facial search, recognition, and comparison technologies. This expansion not only elevated security levels but also enhanced the efficiency and reliability of the authentication process.

The integration of the Siamese neural network into the intelligent system yielded an effective tool for user face recognition, along with the storage and comparison of data during authentication. This approach minimizes the risk of unauthorized access, ensuring the security of user accounts. Consequently, the developed system stands as an effective and secure instrument for user authentication, proficient in mitigating security threats within intelligent systems. This approach holds promise for enhancing the protection of confidential information and ensuring robust system access control.

DOI 10.15588/1607-3274-2024-3-6

REFERENCES

1. Zhu Zhiliang et al. Video Object Segmentation Using Multi-Scale Attention-Based Siamese Network, *Electronics,* 2023. Vol. 12, No. 13, P. 2890. DOI: 10.3390/electronics12132890
2. Zhen Pan et al. A Radio Environment Map Updating Mechanism Based on an Attention Mechanism and Siamese Neural Networks, *Sensors,* 2022, Vol. 22, No. 18, P. 6797. DOI: 10.3390/s22186797
3. Zhang Yumeng [et al.] Similarity-based pairing improves efficiency of siamese neural networks for regression tasks and uncertainty quantification, *Journal of Cheminformatics,* 2023, Vol. 15, No. 1. DOI: 10.1186/s13321-023-00744-6
4. He Xiangdong et al. An Uncalibrated Image-Based Visual Servo Strategy for Robust Navigation in Autonomous Intravitreal Injection, *Electronics,* 2022, Vol. 11, No. 24, P. 4184. DOI: 10.3390/electronics11244184
5. Ding Weiping et al. Brain age prediction based on resting-state functional MRI using similarity metric convolutional neural network, *IEEE Access*, 2023, P. 1. DOI: 10.1109/access.2023.3283148
6. Batiuk T., Vysotska V., Lytvyn V. Intelligent System for Socialization by Personal Interests on the Basis of SEO Technologies and Methods of Machine Learning, *CEUR Workshop Proceedings, 4th Intern. Conf. on Computational Linguistics and Intelligent Systems COLINS 2020*, 2020, Vol. 2604, pp. 1237–1250.
7. Batiuk T. et al. Intelligent System for Socialization of Individual's with Shared Interests based on NLP, Machine Learning and SEO Technologies, *CEUR Workshop Proceedings, 6th Intern. Conf. on Computational Linguistics and Intelligent Systems, COLINS 2022*, 2022, Vol. 3171, pp. 572–631.
8. Kumari Tulika et al. Generating popularity-aware reciprocal recommendations using Siamese Bi-Directional Gated Recurrent Units network, *Vietnam Journal of Computer Science,* 2023. DOI: 10.1142/s2196888823500045
9. Batiuk T., Dosyn D. Intelligent system for clustering users of social networks based on the message sentiment analysis, *Journal of Lviv Polytechnic National University "Information Systems and Networks"*, 2023, Vol. 13, pp. 121–138. DOI: 10.23939/sisn2023.13.121
10. Batiuk T., Vysotska V. Technology for personalities socialization by common interests based on machine learning methods and seo-technologies, *Radio Electronics, Computer Science, Control,* 2022, No. 53 (2), pp. 121–138. DOI: 10.15588/1607-3274-2022-2-6
11. Lim S.-C., Huh J.-H., Kim J.-C. Siamese Trackers Based on Deep Features for Visual Tracking, *Electronics,* 2023, Vol. 12, No. 19, P. 4140. DOI: 10.3390/electronics12194140
12. Seydi S. T., Shah-Hosseini R., Amani M. A Multi-Dimensional Deep Siamese Network for Land Cover Change Detection in Bi-Temporal Hyperspectral Imagery, *Sustainability*, 2022, Vol. 14, No. 19, P. 12597. DOI: 10.3390/su141912597
13. Roodsari S. M. et al. Shape Sensing of Optical Fiber Bragg Gratings Based on Deep Learning, Machine Learning: Science and Technology, 2023. DOI: 10.1088/2632-2153/acda10
14. Park S. K. et al. Binary Dense SIFT Flow Based Position-Information Added Two-Stream CNN for Pedestrian Action Recognition, *Applied Sciences,* 2022, Vol. 12, No. 20, P. 10445. DOI: 10.3390/app122010445
15. Zarębski Sebastian et al. Siamese Neural Networks on the Trail of Similarity in Bugs in 5G Mobile Network Base Stations, *Electronics,* 2022, Vol. 11, No. 22, P. 3664. DOI: 10.3390/electronics11223664
16. Karuppasamy R., Velusamy G., Soosaimarian R., Raj P. A Novel Approach of Dynamic Vision Reconstruction from fMRI Profiles Using Siamese Conditional Generative Adversarial Network, *Brazilian Archives of Biology and Technology,* 2023, Vol. 66. DOI: 10.1590/1678-4324-2023220330
17. Liu Peng et al. Graph neural network based approach to automatically assigning common weakness enumeration identifiers for vulnerabilities, *Cybersecurity,* 2023, Vol. 6, No. 1. DOI: 10.1186/s42400-023-00160-1
18. Gao Peng et al. Efficient and Lightweight Visual Tracking with Differentiable Neural Architecture Search, *Electronics*, 2023, Vol. 12, No. 17, P. 3623. DOI: 10.3390/electronics12173623
19. Sharma Neha et al. Siamese Convolutional Neural Network-Based Twin Structure Model for Independent Offline Signature Verification, *Sustainability*, 2022, Vol. 14, No. 18, P. 11484. DOI: 10.3390/su141811484
20. Lis K., Niewiadomska-Szynkiewicz E., Dziewulska K. Siamese Neural Network for Keystroke Dynamics-Based Authentication on Partial Passwords, *Sensors*, 2023, Vol. 23, No. 15, P. 6685. DOI: 10.3390/s23156685
21. Hong J.-W., Kim S.-H., Han G.-T. Detection of Multiple Respiration Patterns Based on 1D SNN from Continuous Human Breathing Signals and the Range Classification Method for Each Respiration Pattern, *Sensors,* 2023, Vol. 23, No. 11, P. 5275. DOI: 10.3390/s23115275
22. Zhu Jinting et al. Task-Aware Meta Learning-Based Siamese Neural Network for Classifying Control Flow Obfuscated Malware, *Future Internet,* 2023, Vol. 15, No. 6. P. 214. DOI: 10.3390/fi15060214
23. Fan Jiwei et al. PSiamRML: Target Recognition and Matching Integrated Localization Algorithm Based on Pseudo-Siamese Network, *International Journal of Aerospace Engineering*, 2023, Vol. 2023, pp. 1–16. DOI: 10.1155/2023/1135946
24. Tchynetskyi S., Polishchuk B., Vysotska V. Sentiment analysis technology for user feedback support in e-commerce systems based on machine learning, *Radio Electronics, Computer Science, Control*, 2023, No. 3, P. 104. DOI: 10.15588/1607-3274-2023-3-11
25. Du Guocai et al. High-Performance Siamese Network for Real-Time Tracking, *Sensors,* 2022, Vol. 22, No. 22, P. 8953. DOI: 10.3390/s22228953
26. Marattukalam Felix et al. Deep Learning-Based Wrist Vascular Biometric Recognition, *Sensors,* 2023, Vol. 23, No. 6, P. 3132. DOI: 10.3390/s23063132
27. Vasconcellos Eduardo M. M. et al. Siamese Convolutional Neural Network for Heartbeat Classification Using Limited 12-lead ECG Datasets, *IEEE Access,* 2023, P. 1. DOI: 10.1109/access.2023.3236189
28. Liu Dali et al. Design of Siamese Network for Underwater Target Recognition with Small Sample Size, *Applied Sciences*, 2022, Vol. 12, No. 20, P. 10659. DOI: 10.3390/app122010659
29. Kummerow André et al. Siamese Sigmoid Networks for the open classification of grid disturbances in power transmission systems, *IET Smart Grid,* 2022. DOI: 10.1049/stg2.12083

Accepted 22.04.2024.
Received 14.08.2024.

DOI 10.15588/1607-3274-2024-3-6

УДК 004.9

ОПТИМІЗАЦІЯ АВТЕНТИФІКАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ВІЗУАЛЬНОЮ БІОМЕТРИКОЇ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БЕЗПЕКИ

Батюк Т. М. – аспірант кафедри «Інформаційні системи та мережі», Національний університет «Львівська політехніка», Львів, Україна.

Досин Д. Г. – д-р техн. наук, старший науковий співробітник, професор кафедри «Інформаційні системи та мережі», Національний університет «Львівська політехніка», Львів, Україна.

АНОТАЦІЯ

Актуальність. Основною метою цієї статті є дослідження аспектів, пов'язаних із забезпеченням безпеки та підвищенням ефективності процесів автентифікації в інтелектуальних системах шляхом застосування візуальної біометрії. Основна увага приділяється вдосконаленню та вдосконаленню систем автентифікації за допомогою складних методів біометричної ідентифікації.

Метою дослідження було створення спеціалізованої інтелектуальної системи, яка використовує сіамську нейронну мережу для встановлення безпечної автентифікації користувача в існуючій системі. Окрім впровадження основних заходів безпеки, таких як хешування та безпечне зберігання облікових даних користувача, підкреслюється сучасне значення впровадження двофакторної автентифікації. Такий підхід значно посилює захист даних користувачів, перешкоджаючи більшості сучасних методів злому та захищаючи від витоку даних. Дослідження визнає певні обмеження у своєму підході, що, можливо, впливає на можливість узагальнення результатів. Ці обмеження відкривають можливості для майбутніх досліджень і розвідок, сприяючи поточній еволюції методологій автентифікації в інтелектуальних системах.

Метод. Система двофакторної автентифікації інтегрує технологію розпізнавання обличчя, використовуючи візуальну біометрію для підвищення безпеки порівняно з альтернативними методами двофакторної автентифікації. Було оцінено різні реалізації сіамської нейронної мережі, що використовують контрастну функцію втрат і функцію триплетних втрат. Згодом була реалізована та навчена нейронна мережа, що використовує триплетну функцію втрат.

Результати. У статті наголошується на практичних наслідках розробленої інтелектуальної системи, демонструється її ефективність у мінімізації ризику несанкціонованого доступу до облікових записів користувачів. Інтеграція сучасних методологій автентифікації забезпечує безпечний і надійний процес автентифікації користувачів.

Висновки. Впровадження технології розпізнавання обличчя в процесах автентифікації має ширші соціальні наслідки. Це сприяє створенню більш безпечного цифрового середовища, запобігаючи несанкціонованому доступу, зрештою захищаючи конфіденційність користувачів і дані. Оригінальність дослідження полягає в інноваційному підході до автентифікації з використанням візуальної біометрії в рамках сіамської нейронної мережі. Розроблена інтелектуальна система є цінним внеском у цю сферу, пропонуючи ефективне та сучасне рішення проблем автентифікації користувачів.

КЛЮЧОВІ СЛОВА: Аутентифікація 2FA, модель сіамської мережі, алгоритм Triplet Loss, системи розпізнавання лиць.

ЛІТЕРАТУРА

1. Video Object Segmentation Using Multi-Scale Attention-Based Siamese Network / Zhiliang Zhu [et al.] // Electronics. – 2023. – Vol. 12, No. 13. – P. 2890. DOI: 10.3390/electronics12132890
2. A Radio Environment Map Updating Mechanism Based on an Attention Mechanism and Siamese Neural Networks / Pan Zhen [et al.] // Sensors. – 2022. – Vol. 22, No. 18. – P. 6797. DOI: 10.3390/s22186797
3. Similarity-based pairing improves efficiency of siamese neural networks for regression tasks and uncertainty quantification / Yumeng Zhang [et al.] // Journal of Cheminformatics. – 2023. – Vol. 15, No. 1. DOI: 10.1186/s13321-023-00744-6
4. An Uncalibrated Image-Based Visual Servo Strategy for Robust Navigation in Autonomous Intravitreal Injection / Xiangdong He [et al.] // Electronics. – 2022. – Vol. 11, No. 24. – P. 4184. DOI: 10.3390/electronics11244184
5. Brain age prediction based on resting-state functional MRI using similarity metric convolutional neural network / Weiping Ding [et al.] // IEEE Access. – 2023. – P. 1. DOI: 10.1109/access.2023.3283148
6. Batiuk T. Intelligent System for Socialization by Personal Interests on the Basis of SEO Technologies and Methods of Machine Learning / T. Batiuk, V. Vysotska, V. Lytvyn // CEUR Workshop Proceedings, 4th Intern. Conf. on Computational Linguistics and Intelligent Systems COLINS 2020. – 2020. – Vol. 2604. – P. 1237–1250.
7. Intelligent System for Socialization of Individual's with Shared Interests based on NLP, Machine Learning and SEO Technologies / T. Batiuk [et al.] // CEUR Workshop Proceedings, 6th Intern. Conf. on Computational Linguistics and Intelligent Systems, COLINS 2022. – 2022. – Vol. 3171. – P. 572–631.
8. Generating popularity-aware reciprocal recommendations using Siamese Bi-Directional Gated Recurrent Units network / Tulika Kumari [et al.] // Vietnam Journal of Computer Science. – 2023. DOI: 10.1142/s2196888823500045
9. Batiuk T. Intelligent system for clustering users of social networks based on the message sentiment analysis / Taras Batiuk, Dmytro Dosyn // Journal of Lviv Polytechnic National University "Information Systems and Networks". – 2023. – Vol. 13. – P. 121–138. DOI: 10.23939/sisn2023.13.121
10. Batiuk T. Technology for personalities socialization by common interests based on machine learning methods and seo-technologies / T. Batiuk, V. Vysotska // Radio Electronics, Computer Science, Control. – 2022. – No. 53 (2). – P. 121–138. DOI: 10.15588/1607-3274-2022-2-6
11. Lim S.-C. Siamese Trackers Based on Deep Features for Visual Tracking / Su-Chang Lim, Jun-Ho Huh, Jong-Chan Kim // Electronics. – 2023. – Vol. 12, No. 19. – P. 4140. DOI: 10.3390/electronics12194140
12. Seydi S. T. A Multi-Dimensional Deep Siamese Network for Land Cover Change Detection in Bi-Temporal Hyperspectral Imagery / Seyd Teymoor Seydi, Reza Shah-

DOI 10.15588/1607-3274-2024-3-6

Hosseini, Meisam Amani // Sustainability. – 2022. – Vol. 14, No. 19. – P. 12597. DOI: 10.3390/su141912597
13. Shape Sensing of Optical Fiber Bragg Gratings Based on Deep Learning / Samaneh Manavi Roodsari [et al.] // Machine Learning: Science and Technology. – 2023. DOI: 10.1088/2632-2153/acda10
14. Binary Dense SIFT Flow Based Position-Information Added Two-Stream CNN for Pedestrian Action Recognition / Sang Kyoo Park [et al.] // Applied Sciences. – 2022. – Vol. 12, No. 20. – P. 10445. DOI: 10.3390/app122010445
15. Siamese Neural Networks on the Trail of Similarity in Bugs in 5G Mobile Network Base Stations / Sebastian Zarębski [et al.] // Electronics. – 2022. – Vol. 11, No. 22. – P. 3664. DOI: 10.3390/electronics11223664
16. Karuppasamy R. A Novel Approach of Dynamic Vision Reconstruction from fMRI Profiles Using Siamese Conditional Generative Adversarial Network / Rathi Karuppasamy, Gomathi Velusamy, Raja Soosaimarian Peter Raj // Brazilian Archives of Biology and Technology. – 2023. – Vol. 66. DOI: 10.1590/1678-4324-2023220330
17. Graph neural network based approach to automatically assigning common weakness enumeration identifiers for vulnerabilities / Peng Liu [et al.] // Cybersecurity. – 2023. – Vol. 6, No. 1. DOI: 10.1186/s42400-023-00160-1
18. Efficient and Lightweight Visual Tracking with Differentiable Neural Architecture Search / Peng Gao [et al.] // Electronics. – 2023. – Vol. 12, No. 17. – P. 3623. DOI: 10.3390/electronics12173623
19. Siamese Convolutional Neural Network-Based Twin Structure Model for Independent Offline Signature Verification / Neha Sharma [et al.] // Sustainability. – 2022. – Vol. 14, No. 18. – P. 11484. DOI: 10.3390/su141811484
20. Lis K. Siamese Neural Network for Keystroke Dynamics-Based Authentication on Partial Passwords / Kamila Lis, Ewa Niewiadomska-Szynkiewicz, Katarzyna Dziewulska // Sensors. – 2023. – Vol. 23, No. 15. – P. 6685. DOI: 10.3390/s23156685
21. Hong J.-W. Detection of Multiple Respiration Patterns Based on 1D SNN from Continuous Human Breathing Signals and the Range Classification Method for Each Respiration Pattern / Jin-Woo Hong, Seong-Hoon Kim, Gi-Tae Han // Sensors. – 2023. – Vol. 23, No. 11. – P. 5275. DOI: 10.3390/s23115275
22. Task-Aware Meta Learning-Based Siamese Neural Network for Classifying Control Flow Obfuscated Malware / Jinting Zhu [et al.] // Future Internet. – 2023. – Vol. 15, No. 6. – P. 214. DOI: 10.3390/fi15060214
23. PSiamRML: Target Recognition and Matching Integrated Localization Algorithm Based on Pseudo-Siamese Network / Jiwei Fan [et al.] // International Journal of Aerospace Engineering. – 2023. – Vol. 2023. – P. 1–16. DOI: 10.1155/2023/1135946
24. Tchynetskyi S. Sentiment analysis technology for user feedback support in e-commerce systems based on machine learning / S. Tchynetskyi, B. Polishchuk, V. Vysotska // Radio Electronics, Computer Science, Control. – 2023. – No. 3. – P. 104. DOI: 10.15588/1607-3274-2023-3-11
25. High-Performance Siamese Network for Real-Time Tracking / Guocai Du [et al.] // Sensors. – 2022. – Vol. 22, No. 22. – P. 8953. DOI: 10.3390/s22228953
26. Deep Learning-Based Wrist Vascular Biometric Recognition / Felix Marattukalam [et al.] // Sensors. – 2023. – Vol. 23, No. 6. – P. 3132. DOI: 10.3390/s23063132
27. Siamese Convolutional Neural Network for Heartbeat Classification Using Limited 12-lead ECG Datasets / Eduardo M. M. Vasconcellos [et al.] // IEEE Access. – 2023. – P. 1. DOI: 10.1109/access.2023.3236189
28. Design of Siamese Network for Underwater Target Recognition with Small Sample Size / Dali Liu [et al.] // Applied Sciences. – 2022. – Vol. 12, No. 20. – P. 10659. DOI: 10.3390/app122010659
29. Siamese Sigmoid Networks for the open classification of grid disturbances in power transmission systems / André Kummerow [et al.] // IET Smart Grid. – 2022. DOI: 10.1049/stg2.12083

DOI 10.15588/1607-3274-2024-3-6