European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

Creation of an image outline structure to store the segmented picture using the image attribute association link technique.

D.Saravanan [2] Dr.Dennis Joseph [3] Dr. J. Prince Vijai [4] Dr. Siva G.V [5] KVSSN Murty
Faculty of Operations & IT ICFAI Business School (IBS), Hyderabad
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India

ABSTRACT:
A user is allowed to set a password or PIN, either in terms of numbers or text. This type of authentication is easy to remember and user-friendly. These passwords are stored in the database in an unreadable format, meaning the information is converted into a secret text method. Only authorized users have access to the process of reconverting this secret hidden message because they possess the private keys used for both conversion and de-conversion of the inputs. Today's technology enables users to use images as an alternative to textual messages. Face recognition is a popular authentication technique, often followed by user biometrics, and this type of input is stored in the form of images. The proposed paper suggests storing information in terms of images and using a procedure to retrieve the original or hidden information. This technique provides users with a more convenient method, eliminating the need to remember textual information. Experimental design and outputs have verified that the technique is unique and reliable.

Key terms: Text type code word, Hidden images, Image divisions, Secrete key, Image extraction, Image Secrete code.

1.Introduction

Traditional numerical, model detection, and knowledge discovery methods often operate on the assumption of a hit-and-miss approach when autonomously extracting pieces of information from a dataset. Many of these methods are designed to glean insights from data samples, creating ordered information sets derived from representative examples within the dataset. However, in today's diverse data landscape, encompassing realms like internet applications, customer relationships, societal networks, and environmental science, information is often characterized by complex relationships. This complexity is a key consideration in various data mining applications. The focus of these applications is to discern relationships within input data and leverage the advantages of diverse datasets. The proposed work addresses the transformation of information using a concealed message transformation technique, enabling the communication of information from sender to receiver. This technique is employed to identify relationships within datasets and correct any generated images. The process involves dividing the given image input set into smaller segments, which are then stored for further processing. For a user to execute the entire operation, it is carried out in two steps. Firstly, the given input sets are divided into smaller segments, encapsulating the entire information within smaller information segments. Secondly, the process generates a table containing basic information about the segmented objects. In most cases, an image dataset contains multiple attributes, and in many instances, only a few or one of these attributes are used. These captured pieces of information are organised and stored in table formats. The proposed procedure aims to facilitate the effective extraction of information from a complex dataset.

2.Existing System

In the existing system, current data is presented in diverse forms across various applications like the World Wide Web, market trend analysis, Facebook, and other databases. These applications often deal with multi-relational and interrelated datasets. Traditional data, including numerical data, machine learning, pattern detection, and knowledge extraction methods, typically operate by considering a random sample of independent

objects from the provided datasets. Many of the aforementioned methods focus on extracting knowledge from the given sets.

2.1Drawback of existing system

1. Passwords or secret codes are generated only as text.
2. It is easy to predict and crack the inputs.
3. There is no proper mechanism for the stored input sets.
4. The user is forced to remember the passcode.
5. It is easy to guess and easy to break the countersign.
6. In a few cases, the input sets are numerical.

3.Proposed system:

Traditionally, users were allowed to set secret codes in terms of text or numbers only. This required users to input the key whenever they wanted to extract information from the stored dataset. The system would then check the credentials and other parameters. If the input information matched the stored passkey, the user could continue; otherwise, they were prompted to re-enter the credentials. This approach proved complicated for users who struggled to remember textual information and posed a risk of being easily deciphered by hackers. Additionally, anyone in close proximity to the user during the input of the passkey could trace or gain insights into the inputs. Furthermore, these inputs were stored in the backend as is, making it easy for hackers or technologically informed individuals to read the stored content.

To address these complexities, the proposed system introduces a novel approach where the secret code is created in terms of pictures. However, these pictures are not stored as single entities. Instead, the coded objects are initially divided into smaller pieces and then embedded into regular pictures at various locations. Only the authorized user, armed with the necessary clues, can retrieve the needed content. This method allows users to store information in a highly protected manner. Even if hackers attempt to access the information, they can only retrieve the normal images and remain unaware of the implanted pictures. While the initial stage of image implantation may take some time, it offers the advantage of more secure data storage. The procedure involves dividing the coded picture into smaller units, implanting these units into regular pictures at various locations, and creating a composition of objects. In a single image view, any user can only perceive the normal image, but only the authorized user can discern the various implanted images. When users need to extract this hidden information, proper clues enable them to retrieve the needed content. This method empowers users to store hidden information securely without the burden of remembering specific inputs.

3.1 Advantage of the proposed system:

1. User no longer remember the input message.
2. Generating the hidden image sets is easy.
3. Information is not stored in a single place.
4. No prior or domain knowledge is required.
5. The generation of clues is easy for any user.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

4. Proposed architecture

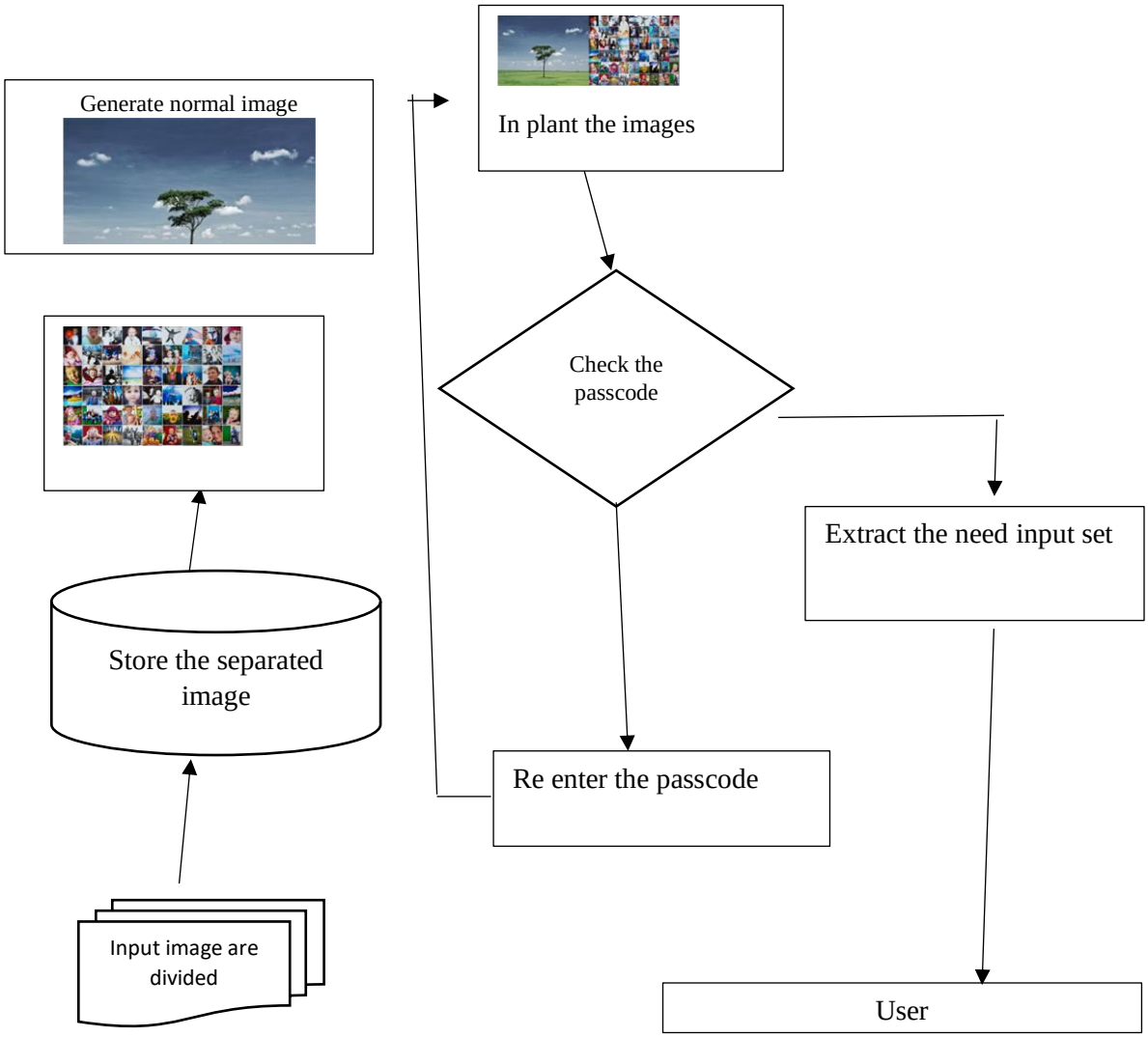

Fig. 1 proposed Architecture

Traditionally, all inputs are given in text form, such as passwords or any clues provided in textual terms. However, these methods are easily cracked by hackers due to the weak strength of the input. Most of this text-based information provides easy clues to hackers, and the information stored on the backend lacks security. This means that, other than highly secure data, the rest of the information is stored as is, allowing anyone to access server information and all credentials easily. This is one of the major drawbacks of the existing technique. To overcome this, our proposed method stores information in the form of images. Even these images are not stored as single pictures; the input images are divided into smaller pieces and then stored in another image. Generally, users can only see the front images and are unaware of the presence of secret images. Only authorised users can decode and retrieve the images, improving authentication and providing effective protection. During the segmentation process, the system identifies relationships among the images. Through these associations, users can extract the images. This process is similar to an interpersonal databank, where datasets are stored in multiple databanks and users generate interpersonal links to access the needed content. Similarly, the built-in

images are divided into smaller pieces. Each segmented image allows users to identify the associations, helping the system locate where the real information is stored.

5. Experimental setup

5.1 Notations and definitions:

In the proposed technique, information is created and stored in terms of pictures. Each picture element contains various attributes, such as the position of the picture, light strength at a particular period, hue differences between one picture and another, and many more. All these attributes help users differentiate one object set from another and also distinguish between identical object sets. Therefore, it is crucial to handle these attributes properly, this process is shown in the fig 2. Many researchers have utilised one or more sets of attributes in their processes, whether they involve storing or retrieving objects. It is essential for users to maintain proper records or tables to store these attributes for further operations.

5.2 Find the distance between the objects

The entire operation is performed through the use of images. Instead of using a single image, the given input or the image being concealed is divided into smaller pieces, and relationships among these pieces are identified. This procedure allows users to store these pieces in different locations. Hence, it is essential to establish links among the segmented images, aiding users in retrieving data quickly. In our relational data bank, inputs are stored in multiple locations and spaces. However, the procedure enables users to create links, connecting all the necessary datasets. Therefore, when a user submits any query, it retrieves the information collectively this process is shown in the fig 3 and 4. A similar approach is adopted here; before uploading the image that the user wants to hide, it is necessary to identify the correlation among the images. This reduces the burden on the user when extracting the original content from the stored input set and also reduces searching time.

5.3 Analyzing the relationships among the objects

After selecting the input objects, it is necessary for the user to understand the size and how these objects are embedded in the picture. Even though the objects are divided into smaller pieces, the information needs to fit into the selected picture. In this procedure, it does not embed single images; instead, it stores a number of images based on the user's design. To achieve this, it is essential to identify the storage and size requirements this shown into the fig 5. In this module, the user measures the initial outline of the selected picture. Based on the outcome, the input images are segmented and stored. In later cases, it can be extended, and the rest of the images are stored successfully.

5.4 Create the hidden objects

After obtaining the reduced outline, the original image that the user wants to hide is successfully incorporated into the selected object. With the outline acquired from the previous module, the user can now locate the picture that was actually uploaded into the object. The next step involves suggesting an information graph and computing the necessary distributions. The final outputs are shown in the fig 6 and 7.

Conclusions and future enhancement:

The proposed two-step image-hiding technique bears similarities to our relational databases. In relational databases, information is allowed to be stored in multiple places, and through the procedure, a common link is created to interconnect all the tables. At any point, when a user sends a single query or any input, the system generates outputs from all the data available in the existing tables. Similarly, in this approach, images are segmented and stored in different places, and the system identifies associations among the inputs. This aids the user in extracting the needed output. The two-step method allows users to first identify the outline or drawing of the picture. In the next step, using the image attributes, the information that needs to be hidden is segmented and placed in the template created in the previous step. However, two potential drawbacks need to be addressed in future processes. Firstly, the segmentation of images and the identification of relationships among the pieces may be time-consuming. Secondly, the creation of a link every time segmented pieces are spread across multiple

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

locations can pose challenges for researchers. Efforts should be made to address these drawbacks and streamline the process for more effective and less time-consuming operations in the future.

Fig. 2 Key generation process

Fig 3. Getting Users personal information

Fig 4. Generation of Users id

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 2 (2024)
http://eelet.org.uk

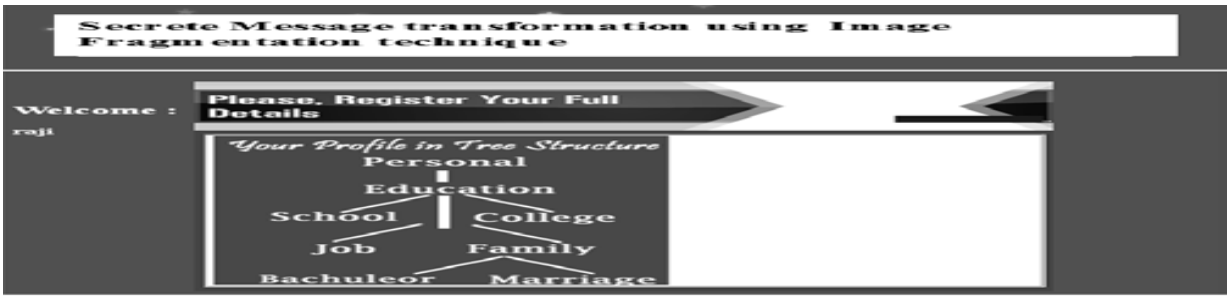

Fig 5. User's information view

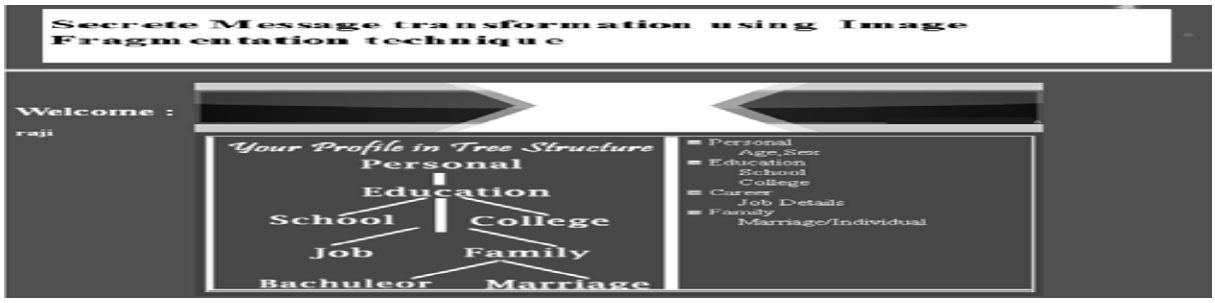

Fig 6. A particular user view information

Fig 7. Admin view of user

References:

C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007

A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services ondemand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004

D. Saravanan, Dr. S. Srinivasan,. , Matrix Based Indexing Technique for video data, Journal of computer science, 9(5),2013, 534-542,2013

D. Saravanan, Dr. S. Srinivasan. Video image retrieval using data mining Techniques, Journal of computer applications (JCA), Vol V,Issue 01, 2012. 39-42,2012.

Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems, vol. 28, no. 1-2, pp.177 – 189, 2000

N. Laranjeiro and M. Vieira, “Towards fault tolerance in web services compositions,” in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.

J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez-Peris, “Ws-replication: a framework for highly available web services,” in Proc. of the WWW, New York, NY, USA, 2006.

Norris, K. Coleman, A. Fox, and G. Candea, “Oncall: Defeating spikes with a free-market application cluster,” in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.