

GRAPHICAL PASSWORD AUTHENTICATION USING IMAGE STEGANOGRAPHY

M. Sumithra^{1a}, B. Buvaneswari^{2b}, *M.Nivethitha^{3c}, E.Asmitha^{3d}, N.kaviya^{3e}

¹Associate Professor, Department of Information Technology, Panimalar Engineering College

²Professor, Department of Information Technology, Panimalar Engineering College

³II yr students, Department of Information Technology, Panimalar Engineering College

Abstract. User authentication and permission are important components of computer and information security in the modern IT world. Access to computer systems relied on the use of alphanumeric passwords, but users have trouble remembering a password that is long and random-looking. A password is therefore a highly significant part of this authentication. Alphanumeric characters have been used to create graphical passwords. In order to sway user preference, our system combines the click-point approach with the persuasive feature. In conjunction with the visual steganography approach, it is challenging for the user to decipher. To increase the security of the authentication system, image steganography, the technique of concealing data within an image, is used.

Keywords: Graphical password, steganography, image steganography.

I. INTRODUCTION

One of the procedures for computer system authentication is a graphic password. To build a secure environment for our digital gadgets, we need computer security. cite the following three crucial areas where human-computer interaction is crucial: operation security, creation of secure operations, system development for security, and authentication. Here, the issue of authentication is the main focus. User authentication is a crucial and essential, essential part of the majority of computer security solutions. User authentication is undoubtedly a real-world issue. This issue needs to be resolved from the standpoint of a service provider while taking into account practical limitations like the available hardware and software infrastructures. Motivated by this, graphical password schemes have been proposed as a possible alternative to text-based schemes. partly due to the fact that humans remember pictures better than text; psychological studies back up this assumption. Aside from the workstation and web log-in application. Mobile phones and ATM machines now use graphics But in this essay, We'll concentrate on a different option: employing a collection of images as passwords. Better defense against dictionary assaults. light, Because of these benefits, graphical passwords are gaining popularity. passwords as well.

a. Graphical Password

Graphical passwords refer to using pictures as passwords. This system uses a random set of images from which the users select some of them in a specific order to form the password. Such a password is easier to remember and more secure than traditional alphanumeric passwords. Nonetheless, it is noted that graphical password approaches do have some drawbacks, with those being the main ones. It is prone to shoulder surfing attacks because passwords are made of photos To "shoulder surf" someone is to look over their shoulder in order to obtain their passwords. A hostile observer may be able to obtain the user's password credentials when the user enters a password using a keyboard, mouse, touch screen, or any other conventional input device. Our suggested method offers some protection against shoulder surfing and other potential threats. The structure of the essay is as follows.

II. LITERATURE SURVEY

User authentication is the key component of cyber security. In order to defend systems from different types of assaults, password protection is often provided. Regular text passwords made up of a combination of letters, numbers, and special characters are the most frequent type of authentication. Often, users choose text-based passwords that are easy to remember (such as their birthdate, phone number, etc.). Although easy to use, the approach is vulnerable to multiple attacks. Graphic passwords are used in the alternate authentication mechanism. These passwords contain graphics, which are easier to remember than the long strings of characters seen in text passwords.[1]

Security of data and computers is greatly aided by passwords, which are the fundamental elements of the authentication procedure. The most common method of computer authentication uses an alphanumeric username and password, but it has a few drawbacks. To overcome the flaws of traditional methods, visual or graphical password systems have been developed as viable substitutes for text-based schemes. Shoulder surfing is more likely to occur with graphical password schemes than with conventional alphanumeric text passwords. While entering their passwords in a public place, users run the risk of having them

stolen. By watching the user's authentication process on camera or by direct observation, an intrusive party can learn the password. This sport is known as shoulder surfing.[2]

Passwords are a major component of computer security that are utilized to confirm human clients. Clients have inconvenience recollecting passwords over time, indeed on the off chance that they utilize solid passwords—long, arbitrary passwords—that are secure. As a result, they habitually select frail passwords that are brief. Making secure and vital passwords can be a challenge. Graphical passwords, which require clicking on pictures instead of writing alphanumeric groupings, maybe the arrangement. In this think about, PassPoints are portrayed.[3]

Passwords and usernames are the most common methods of computer confirmation. Basic downsides have been shown with this methodology. Passwords that are easy to guess are what clients tend to choose. It is troublesome to be beyond any doubt if a mystery word is troublesome to figure. Some investigators have made procedures that use pictures as passwords to address this issue. We think about the graphical mystery word techniques in this paper. We classify these methodologies into two categories: recognition-based and recall-based approaches. The long-run explore headings in this locale show the qualities and obstacles of each strategy. We as well endeavor to answer two basic questions: "Are graphical passwords as secure as text-based passwords? What are the major problems with graphical passwords? This diagram will be important for information security investigators and experts who are inquisitive about finding an elective to text-based confirmation techniques.[4]

Potential certificates of identity can be identified by a wide range of human memory phenomena. The capacity for complex experiences that can be recognized and transferred to others is what these imprinting behaviors are characterized by. They are suitable for use in near-zero-knowledge protocols, which minimize the amount of secret information exposed to prying eyes while identifying an individual. We apply the examples to the protocols. This provides a novel approach to human-computer interfaces and raises new questions in several classic areas of psychology.[5]

The internet plays a crucial role in today's life, which is why the usage of online social networks is increasing. Online social network allows people to communicate with their friends. It is a big challenge to keep online social networks safe. We use a text-based password. Text-based passwords are hard to remember and vulnerable to attacks. Text passwords are not all that good. There is a way to remember passwords. Humans are less vulnerable to attacks because they can easily remember pictures. Text passwords are just as bad as graphical passwords. Users share their images.[6]

The development of the smartphone has changed the lifestyles of users. Integration of Near Field Communication into the phone has opened up new applications and business models. The graphical password scheme and near-field communication are two important technologies that can be used to achieve a secure and convenient access control system. One of the potential uses of such technologies is the integration of a steganography graphical password scheme into NFC-enabled smartphones to transcend conventional digital key/tokens access control systems into a more secure and convenient environment. The free hand to exchange surety and how they interact with the passage would be delivered to smartphone users. As such, this paper presents a secure two-factor authentication NFC smartphone access control system using a digital key and the proposed Encrypted Steganography Graphical Password (ESGP).The paper shows that the user perception and intent to use the phone access control system are valid through an experiment and user evaluation survey.[7]

The use of smart systems has introduced a threat to data security and privacy. Most of the applications are built-in unsecured operating systems, and so there is a growing threat to information cloning, forging tampering counterfeiting, etc. This will lead to an un-compensatory loss for end-users, particularly in banking applications and personal data in social media. The shoulder surfing touch can be polished with the aid of the adversary to accumulate the individual's watchword by searching over the client's shove. However, most of the current graphical password schemes are liable to shoulder-browsing a recounted hazard wherein an attacker can seize a password by means of way of a direct statement or by recording the authentication consultation. Because of the visual interface, shoulder-browsing becomes an exacerbated problem in graphical passwords. A graphical password is easier than a textual content-based password for the majority to undergo in thought. Suppose an eight-man or woman password is critical to benefit access into a specific computer network. Passwords that are strong are proof of their validity.[8]

III. EXISTING SYSTEM

To ensure the safe and accurate transmission of sensitive information, the framework proposed in this paper should include as many of the necessary components as possible.

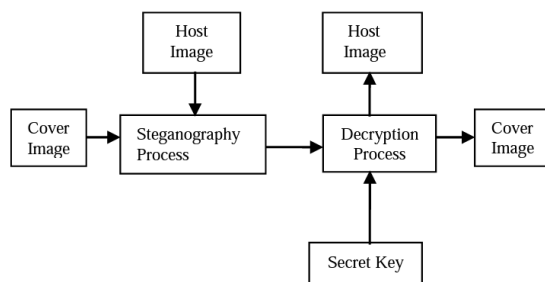


Fig.1: Block Diagram

Several modules are included in our framework. The host image will be standardized in the first module. The cover image will include the host image. The stego key will be used in the later modules. The receiver will decipher the secret image. The secret image is retrieved again. The proposed method has a detailed description.

a. Standardizing The Image

One of the needed images is a cover image, while the other is a hidden image, which we are entering or viewing. The photos should be as small as possible. The cover image in this case is 480 x 60 pixels in size. This significant size disparity serves as a reminder of the method's primary tenet—namely, that the total number of bits in the secret image should be smaller than those in the cover image in order for the image to retain its previous appearance. There is a conversion of the secret image to greyscale.'

b. Embedding process

Bit Plane Slicing is the first step of the process. The secret image was divided into individual bits. Now, related bit planes make up the secret picture plane. We thus have 8-bit planes that correspond to each and every pixel in the hidden image. LSB substitution steganography is proposed as an embedded technique. A secret image is used in place of the cover image's LSB. The following steps are used for Embedding.

STEP 1: With the necessary bit position, the bit plane slicing can be implemented.

STEP 2: We process the cover image. We want secret data to take the place of the LSBs.

STEP 3: The existing one should be empty if we wish to alter the data there. The LSBs must be vacant In order to replace the cover image and the host bit. From the cover image, the LSB bit is subtracted.

STEP 4: Just put the cover image piece to the LSB location of the cover image to replace the host bits. equivalent bit planes.

STEP 5: The secret image that is encoded in the stego image is transmitted in accordance with the requests of the users. Its host the cover image below, which can be embedded, is displayed.

1. Start
2. The input of a cover image and a secret image.
3. The image should be standardized.
4. There is a bit of plane slicing of a secret image.
5. The cover image has bits in it.
6. The Stego image was output.
7. End.

c. Security implementation

A double-level security system has been implemented at the receiver. A security password is required at the first level. We can proceed to the second level if the security password is acceptable. There is a banned image at this level. The decoding process begins if the key image matches. There is a chance that the secret image could be retrieved by the invaders.

d. Decoding

Decoding is the process of using an embedded technology in reverse. The following steps are used to complete this.

STEP 1: To form the corresponding bit planes, the LSBs of the cover image have to be collected.

STEP 2: The original secret image has the same number of bits as the original.

STEP 3: In order to maintain image clarity, scale the decoded image back to its original size.

The technique for decoding is shown in the algorithm below.

1. start
2. The inputs are the stego picture, secret image, and key image.
3. In comparison to the hidden key.
4. The picture was obtained.
5. contrasting the two images, you'll see the key image.
6. The secret image can be coded.
7. The secret image was output.
8. End

IV. MATERIALS AND METHODS

a. Cued click points

Cued Click Points are an alternative to PassPoints. Users click on one point on each of the five images rather than five points on one image. If a user makes a mistake when entering their most recent click-point, they can next image attempt and restart from the beginning. Because of this, attacks based on hotspot analysis are more difficult. As shown in the diagram. When users click on the next image, they are taken down a path as they click on their sequence of points. A misclick takes you down the wrong path, with an explicit indication of authentication failure only after the last click. The suggested system is an If they use a single or double click on the image, it is much more secure and effective. If the user makes a mistake while logging in, the reset button will allow them to make the correct click. Images of specific sizes and resolutions will be available in our system.

There are 16 grids on the image, and each one has an address that, when clicked, displays the associated image. What will happen, Four graphics with tolerance squares and sixteen grids. The first step in the procedure is user registration, when the user enters their name, which is then confirmed and put in the database. The user can pick an image from a database. The user will be presented with a tolerance square and asked to choose a point. A message box will be presented asking the user if they want to keep using the image or not and asking if they want to continue using it. To proceed, the user must choose another spot on the opposite image. If the associated image appears, the user must enter a password that is by the database, verified. The following image will be shown if the clicked location in the tolerance square is deemed to be erroneous. In the event that the user clicks on the incorrect point by accident, a reset option is available. The user is aware of the path they have taken after making the last click.

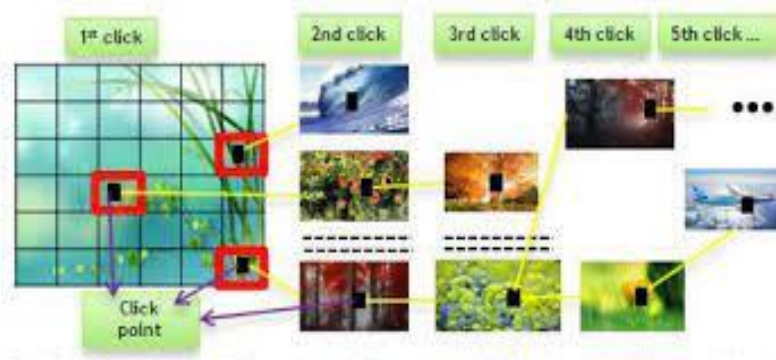


Fig.2: Graphical password authentication using Cued Click Points (Reddy et al.,2013)

b. Image steganography

Communication has been made more secure since the rise of the internet. The field of cryptanalysis deals with hiding the meaning of a message. It is very difficult to get the true meaning of a message when it is sent to the wrong people. Steganography is a field that deals with hiding the meaning of a message but also hiding its existence. The information is protected in its own way, but neither is perfect and can be compromised. In a hybrid approach, we hide the message and make it harder to see it. Digital data, like images, Audio, Video Network packets, etc, are used as the carriers in today's steganography. There are a lot of techniques for each of them, but this article aims to provide an overview of image stripping. There are lots of bits that are there to provide accuracy far greater than necessary for the object's use, which is why images are an excellent medium for concealing information. Steganography techniques alter redundant bits in such a way that they can't be seen by humans or computers.

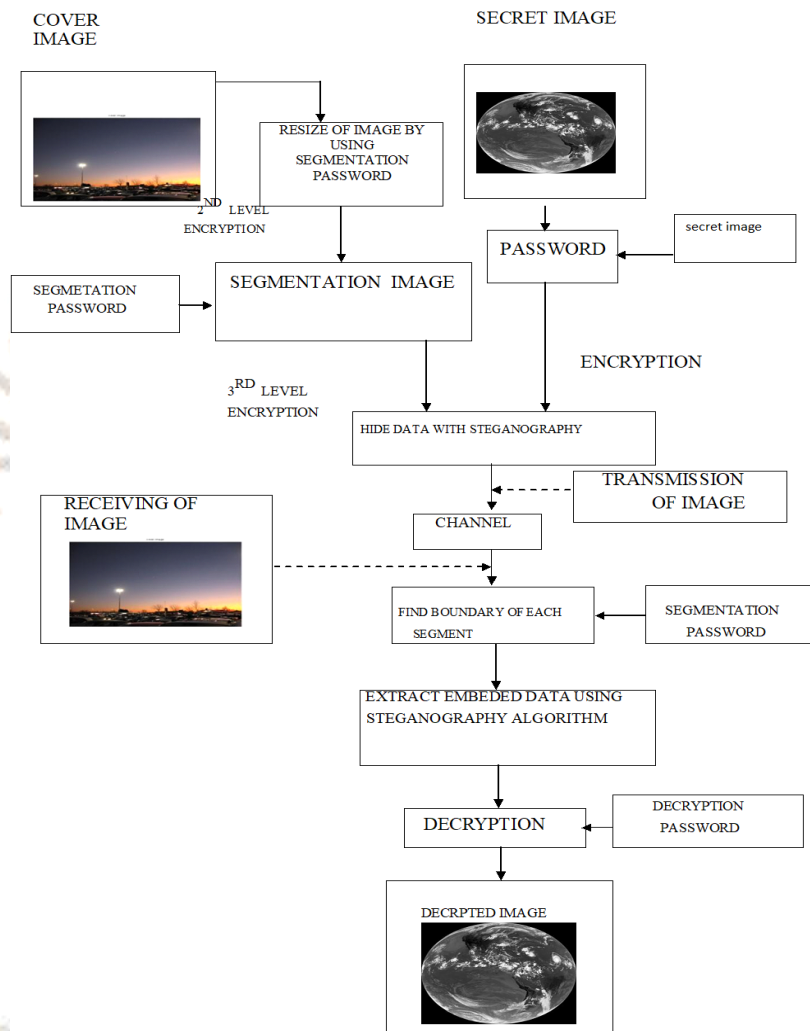


Fig.3: image steganography flowchart

V. EXPERIMENTAL RESULT

The outcome is satisfactory when the concealed image is twice as large as the cover image. In this case the cover image is a color image with many colors and the hidden image is a black-and-white image the result is accurate and The Stefano image is the same as before. If the hidden image is very much smaller than the cover image then also, we have a very good output. In this case, the cover image is having three colors and the hidden image is having multi colors then the result is accurate. In this instance, the cover image is a black-and-white photograph, while the hidden image is a color photograph with a white border. Although a yellow strip can be seen, the background of the stegno image is unchanged. In this instance, a cover image measuring 150 x 150 pixels and a hidden image measuring 300x300(i.e., the cover image is smaller than the hidden image) are taken there is an error in the output result. The hidden image was erased. In this instance, the cover image is assumed to be a black-and-white photograph, however, it is actually a color photograph without any white. background, the stegno picture has altered and the outcome is accurate. Black and white photos are used in this instance for both the cover image and the secret image. The hidden image has a white background so the output image contains a yellow and red strip.

















S.NO	ORIGINAL IMAGE	SIZE	INPUT IMAGE	SIZE	EMBEDDED IMAGE	OUTPUT IMAGE
1		1600×1200		437×437		
2		2048×1536		350×350		
3		640×480		150×150		
4		2592×1944		250×250		

Fig.4: results for hiding an image in an image

VI. CONCLUSION

Early this decade, graphical passwords gained popularity as a replacement for text-based passwords. We have outlined a new implicit password authentication method in this research, where the authentication data is implicit. The user is shown. The suggested protocol not only enhances user experience but also withstands testing. threats like malware and key logger attacks. Here, passwords are stored using image steganography technology. Steganography is a technique for delivering secret information while concealing it in images. hidden from view inside a cover picture that resembles. This work has outlined the method for image steganography that has recently been employed. To log in to a system with a graphical password, there is a screen with pictures on it. After clicking on the picture, the screen shows the picture that the user has set as their password, and then the user has to click on the spot in the picture where the password was set. The system will automatically log in if he clicks the password spot. There are many kinds of dedicated software applications available to facilitate steganography. An application called Steg hides may conceal data in a variety of picture files, including JPG, BMP, AU, and WAV.

a. An application used in the picture password system:

- Hard disk locking
- System login and logout process
- Folder locking
- Web log-in application

b. Technique proposed

- Blonder, passlogix, wiedenbeck
- **Authentication process** – click on several pre-registered locations of a picture in the right sequence.
- **Memorability** – can be hard to remember
- **Password space** – N^K (N is the number of pixels or smallest units of a picture, K is the number of locations to be clicked on)
- **Possible attack methods** – Guess, shoulder surfing.

REFERENCES

- [1]. Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle Computer Department, K. J. Somaiya College of Engine Comparison of Graphical Password Authentication Techniques International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015
- [2]. Arash Habibi Lashkari, Samaneh Farmand, Dr. Omar Bin Zakaria, Dr. Rosli Saleh Shoulder Surfing attack ingraphical password authentication [Submitted on 4 Dec 2009]
- [3]. Wiedenbeck Susan, Waters Jim, Birget Jean-Camille, Brodskiy Alex and Memon Nasir, "Passpoints: design and longitudinalevaluation of a graphical password system", *International Journal of Human-Computer Studies*, vol. 63, pp. 102-127, July 2005.
- [4]. Xiaoyuan Suo, Ying Zhu and G. Scott Owen, "Graphical passwords: A survey", *Proceedings of Annual Computer Security Applications Conference*, pp. 463-472, 2005.
- [5]. D.Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
- [6]. Jina Marin Bijoy; V. K. Kavitha; B. Radhakrishnan; L. Padma SureshA Graphical Password Authentication for analyzing legitimate user in online social network and secure social image repository with metadata 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)
- [7]. Soon-Nyeon Cheong a, Huo-Chong Ling a Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system Volume 41, Issue 7, 1 June 2014
- [8]. Prof. P. S. Gayke¹, Shraddha Thorat², Gayatri Nagarkar³, Priyanka Kusalkar⁴, Priyanka Waditake Secure Data Access using Steganography and Image Based Password volume 9, Issue 3 May-June-2022
- [9]. M. Sumithra and Dr. S. Malathi, "A Novel Distributed Matching Global and Local Fuzzy Clustering (DMGLFC) FOR 3D Brain Image Segmentation for Tumor Detection", IETE Journal of Research, doi.org/10.1080/03772063.2022.2027284, 2021
- [10]. B.Buvanswari and T.Kalpalatha Reddy, "A Review of EEG Based Human Facial Expression Recognition Systems in Cognitive Sciences" International Conference on Energy, Communication, Data analytics and Soft Computing (ICECDS), CFP17M55-PRJ:978-1-5386-1886-8", August 2017.
- [11]. M. Sumithra and Dr. S. Malathi, "Modified Global Flower Pollination Algorithm-based image fusion for medical diagnosis using computed tomography and magnetic resonance imaging", International Journal of Imaging Systems and Technology, Vol. 31, Issue No.1, pp. 223-235, 2021
- [12]. K. Sridharan , and Dr. M. Chitra "SBPE: A paradigm Approach for proficient Information Retrieval , Jokull Journal" , Vol 63, No. 7; Jul 2013
- [13]. M. Sumithra and Dr. S. Malathi, "3D Denselex NET Model with Back Propagation for Brain Tumor Segmentation", International Journal Of Curent Research and Review, Vol. 13, Issue 12, 2021.
- [14]. B.Buvaneswari and Dr.T. Kalpalatha Reddy, "EEG signal classification using soft computing techniques for brain disease diagnosis", Journal of International Pharmaceutical Research ,ISSN : 1674-0440, Vol.46, No.1, Pp.525-528, 2019.
- [15]. K. Sridharan , and Dr. M. Chitra "Web Based Agent And Assertion Passive Grading For Information Retervial", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 16, September 2015 pp:7043-7048
- [16]. M. Sumithra and Dr. S. Malathi, "Segmentation Of Different Modalities Using Fuzzy K-Means And Wavelet ROI", International Journal Of Scientific & Technology Research, Vol. 8, Issue 11, pp. 996-1002, November 2019.
- [17]. M. Sumithra and S. Malathi, " A Survey of Brain Tumor Segmentation Methods with Different Image Modalities", International Journal of Computer Science Trends and Technology (IJCTST) – Vol. 5 Issue 2, Mar – Apr 2017
- [18]. B.Buvaneswari and Dr.T. Kalpalatha Reddy, "High Performance Hybrid Cognitive Framework for Bio-Facial Signal Fusion Processing for the Disease Diagnosis", Measurement, ISSN: 0263-2241, Vol. 140, Pp.89-99, 2019.
- [19]. M. Sumithra and Dr. S. Malathi, "A Brief Survey on Multi Modalities Fusion", Lecture Notes on Data Engineering and Communications Technologies, Springer, 35, pp. 1031-1041, 2020.
- [20]. M. Sumithra and S. Malathi, "A survey on Medical Image Segmentation Methods with Different Modalities", International Journal of Engineering Research and Technology (IJERT) – Vol. 6 Issue 2, Mar 2018.
- [21]. B.Buvaneswari and Dr.T. Kalpalatha Reddy, "ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial", International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091, Vol.8, No.1, Pp. 12-17, 2019
- [22]. K. Sridharan , and Dr. M. Chitra , Proficient Information Retrieval Using Trust Based Search On Expert And Knowledge Users Query Formulation System, Australian Journal of Basic and Applied Sciences, 9(23) July 2015, Pages: 755-765.
- [23]. B.Buvaneswari and Dr.T. Kalpalatha Reddy, "ACPT- An Intelligent Methodology for Disease Diagnosis", Journal of Advanced Research in Dynamical and Control Systems, ISSN : 0974-5572, Vol.11, No.4, Pp.2187-2194, 2019.
- [24]. Sumithra, M., Shruthi, S., Ram, S., Swathi, S., Deepika, T., "MRI image classification of brain tumor using deep neural network and deployment using web framework", Advances in Parallel Computing, 2021, 38, pp. 614–617.
- [25]. K. Sridharan , and Dr. M. Chitra "RSSE: A Paradigm for Proficient Information Retrieval using Semantic Web" , Life Science Journal 2013;10(7s), pp: 418-425