Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.028975
Article

Tech Science Press

An Enhanced Graphical Authentication Scheme Using Multiple-Image Steganography

Khalil Hamdi Ateyeh Al-Shqeerat*

Department of Computer Science, College of Computer, Qassim University, Saudi Arabia
*Corresponding Author: Khalil Hamdi Ateyeh Al-Shqeerat. Email: kh.alshqeerat@qu.edu.sa
Received: 22 February 2022; Accepted: 25 March 2022

Abstract: Most remote systems require user authentication to access resources. Text-based passwords are still widely used as a standard method of user authentication. Although conventional text-based passwords are rather hard to remember, users often write their passwords down in order to compromise security. One of the most complex challenges users may face is posting sensitive data on external data centers that are accessible to others and do not be controlled directly by users. Graphical user authentication methods have recently been proposed to verify the user identity. However, the fundamental limitation of a graphical password is that it must have a colorful and rich image to provide an adequate password space to maintain security, and when the user clicks and inputs a password between two possible grids, the fault tolerance is adjusted to avoid this situation. This paper proposes an enhanced graphical authentication scheme, which comprises benefits over both recognition and recall-based graphical techniques besides image steganography. The combination of graphical authentication and steganography technologies reduces the amount of sensitive data shared between users and service providers and improves the security of user accounts. To evaluate the effectiveness of the proposed scheme, peak signal-to-noise ratio and mean squared error parameters have been used.

Keywords: Security; graphical authentication; steganography; peak signal to noise ratio; mean squared error

1 Introduction

An authentication process is a vital security requirement for any remote system as it determines whether or not the user can access the services. Despite the urgent need to increase the security layer of the authentication system, most systems still rely on textual passwords to authenticate the identity of users due to reliability flaws or the high costs of sophisticated authentication techniques [1]. However, conventional passwords have significant security and usability shortcomings. A variety of methods are available to hackers to use in order to guess or crack the weak or short-length password, including brute-force, dictionary attacks, and other common password-cracking techniques [2]. To avoid guessing attacks, users can pick a long, complicated password, which is hard to remember. The use of graphical passwords

has been proposed to overcome text-based problems as a human can easily remember visual information than text strings [3]. Graphical authentication solutions provide security but need to address usability and increase security by securing the confidentiality of the key used.

In general, recognition and recall-based techniques are the main types used in graphical user authentication [4,5]. The recognition-based approach presents a set of images to the user in which the authentication process is performed by detecting and identifying the elected images in the registration stage. In comparison to alphanumeric passwords, recognition-based passwords have smaller password spaces that make them susceptible to brute-force attacks.

In contrast, recall-based passwords require users to resubmit something they selected during the registration process such as drawing a line over an image or clicking on a specific location. In this type, security can be improved by more clicks, but it becomes more complicated. Whereas, the number of clicks required to authenticate users may vary according to system requirements.

Implementation of graphical authentication on remote systems has been plagued with many security flaws due to a series of weaknesses in a web-based environment [6]. Servers connected via the web can be secured, but client machines may contain vulnerabilities that could compromise the graphical authentication scheme. In addition, attackers may be able to intercept the sensitive data as it travels over the Internet to the remote server [7]. In order to create a convenient and secure authentication system, it is necessary to combine a graphical password, cryptography, and steganography. As the name implies, steganography refers to hiding information within various types of objects, including images, audio, video, and even text to create a stego-object [8]. Various spatial or transform domain steganography techniques can be used, such as least significant bit (LSB), discrete wavelet transform (DWT), or discrete cosine transform (DCT) [9]. Steganography and cryptography are often used together to improve the security of communication processes since it is more complicated for a third party to discern a randomly generated pattern of encrypted data in a stego-object [10].

An enhanced graphical user authentication scheme is presented in this paper, which integrates both recognition and recall-based approaches besides the Least Significant Bit (LSB) steganography technique. Integration of LSB into graphical password scheme increases the security level of access control systems for a more secure and convenient environment. An experimental study has been included in this paper to evaluate user perceptions of and behaviors related to integrated graphical schemes.

This paper is structured as follows. Section 2 reviews some recent research literature regarding the proposed scheme. The design of the proposed work is described in detail in Section 3. Section 4 discusses the security and usability features of the proposed graphical scheme. Finally, Section 5 provides the implementation of the proposed authentication scheme and illustrates the obtained results.

2 Literature Review

Recently, several proposals for graphical authentication schemes have been made. In this section, we will discuss some research that used steganography in graphical authentication. Most of the literature reviewed used steganography techniques to hide confidential text-based information into the graphical passwords to authenticate users. In [11], Soon-Nyean et al. have presented an Encrypted Steganography Graphical Password (ESGP)-based to secure NFC-smartphone access control system. In order to address the security constraints of current NFC access systems, the proposed method deploys a secure two-factor authentication system using security primitives (steganography, cryptography, and graphical password). Integrating both steganography and a graphical password scheme makes access control systems more secure. The proposed system has a limitation in which the user should remember the graphic password and steganography key for access. The authentication system in [12] used a combination of cued click

point method with steganography to encourage users to choose more random click points that make the graphical password harder to guess. In order to improve the security of the authentication process, the art of steganography is used to hide textual passwords within an image. Tsung-Hung et al. have improved the efficiency of the graphical password by developing and redesigning the Passpoint scheme [13]. The user graphical password points are hidden using steganography, and the encryption key is then sent to a server to be stored in a database. This secret key can be used to decrypt graphical passwords from images that are stored on the server. The use of tabular steganography enhances the security of a database as well as reduces the amount of storage required. A secure authentication approach using visual cryptography and stenography has been proposed in [14]. In the registration process, the user will have to choose one secret cover image and then creates a secret question and answer. A steganography technique hides the answer in the cover image. Then, two shares of the cover image are generated at the server using visual cryptography, one share is sent to the user and the other is stored on the server. In the login phase, the user has to provide the username, password, and own share. Superimposing user and server shares reveals the cover image (secret image) and extracts the secret answer. The user is then asked to answer the secret question. If both answers match, one provided by the user and the other extracted from the cover image, access to the system will be granted. In [15], Alotaibi et al. proposed a modulation to improve the security of authentication systems in portable devices. The enhanced mechanism involves combining hash, cryptography, and steganography mechanisms to secure data transmission over the internet in a trusted manner. AES encryption is used to encrypt the hashed password, and then hide it inside a cover image to be retrieved for authentication when needed. This combination of mechanisms provides authentication, confidentiality, and integrity. A study in [16] has presented an image and area selection scheme. In this scheme, the image magnification factor is used as a novel security key by comparing the pixel values of specific areas in an enlarged image for user authentication. To achieve high levels of security on embedded platforms, the proposed scheme combines image authentication and area authentication. This scheme can also be used for low-resource embedded devices for one-to-one authentication with little memory usage, by using the keypad and graphical LCD screen for password selection.

A remote user authentication system for the Internet of Things (IoT) devices has been presented in [17]. It protects IoT networks from unauthorized access. In order to provide user authentication and secure original data, authors have proposed a cancelable iris- and steganography-based user authentication system. Most existing cancelable iris biometric systems require a key-dependent transformation to guide feature transformation. If this user-specific key is compromised, useful data can be exposed and exploited by adversaries to retrieve data. The proposed scheme improves system security by using the steganography technique to conceal the user-specific key and to mitigate the threat of key exposure-related attacks. A secure online transaction method using visual cryptography and discrete wavelet transform steganography was proposed in [18]. The use of these technologies reduces the amount of data that is shared between consumers and online merchants, making online transactions more secure, and increasing customer confidence by reducing the risk of identity theft and phishing. The test results indicate that the PSNR value is appreciably higher as well as the MSE significantly reduced when compared to conventional techniques that hide secrets with discrete cosine transforms applied to cover images. The PSNR could be enhanced with 16-bit coding because more information could be represented in a pixel.

Venkataramana et al. [19] have developed a specialized steganographic image authentication (SSIA) algorithm for clustered cloud environments. Hybrid steganography in the private cloud is dynamically used to ensure security in hybrid cluster environments. In the proposed system, dual-type encryption is used to protect images in cloud systems. By combining a hybrid blowfish and genetic operator model, this model performs fast and provides the highest level of security. Chromosome selection is a crucial part of the process, which is optimized when performed over a cloud environment as opposed to other

cryptographic algorithms. Security over dynamic cluster-based private environments is managed carefully with better operation, which does not significantly increase the complexity of cloud systems.

A system for secure, reliable, scalable, elastic, and trustworthy IoT authentication was proposed in [20]. A crypto hash function based on discrete wavelet transforms (DWTs) is applied to messages sent or received by users. Multiple security features are included in this scheme, such as a one-time message code, message integrity, message anonymity, and session key agreement. Results showed that the proposed scheme offers hidden invisibility to secure against MAC attacks. Stego-objects were used as a two-factor authentication token by [21] to create seamless management of user passwords using information hiding techniques. In the proposed steganographic password management system, account information is embedded into a cover image after it has been encrypted with the user's master key. This solution has limitations in portability, as well as the possibility of losing all account information if the stego-image is lost.

XML-based authentication schema was proposed in [22] to present the graphical password. When a graphical password with a pattern is loaded, the server processes it and verifies that the pattern is valid based on stroke length and drift. Numerous transformations are applied to the input graphical pattern to obtain various graphical patterns. These pixel values are stored in an XML pattern database. The server then updates the pattern bits in the input image using LSB steganography and then returns the result to the user as a password image. Each time a user enters a password image, patterns are extracted and mapped to an XML pattern database.

According to our best knowledge, there are no relevant works on the adoption of a question-based authentication system using cryptography and multiple image steganography in combination with graphical passwords to verify the identity of users.

3 Proposed System

The proposed system provides a workable and secure solution to overcome the insecure connection between the user and the remote server over Internet. It adds an extra security layer to graphical passwords by hiding passwords inside another image to protect it from being seen during the transmission process. Using this steganography-based authentication system, the user is required to bypass interdependent sequential challenges successfully within a short time interval. In the authentication process, the duration of the image display is crucial, as the long display period facilitates the authentication process for users. However, the long time may give password crackers a big chance to discover hidden passwords.

The authentication system is divided into registration and authentication phases. The registration process enables users to register to the system remotely, while the authentication procedures are used to verify the identity of users every time they attempt to access or obtain services.

3.1 Registration Phase

This section describes the registration steps that a user must follow to register on the remote authentication server. The user must first create an account by defining a new username for the desired system. A dynamic string (salt) is generated randomly in the user's profile for later hashing. Afterwards a list of questions is then displayed where the user must choose one as a secret question. A grid consisting of several randomly distributed small images associated with the selected secret question is displayed, for example, if the user's chosen question is "Which country would you like to travel frequently?", so the following image grid will be displayed as shown in Fig. 1. The user selects one secret image to be the answer to this question.

Figure 1: Grid of small images

After that, a large cover image with less weight is then displayed (the one that is least used among the set of images predefined for this purpose), and the user then chooses a starting point to hide the secret image inside the cover image. The cover image must be large enough to ensure security as the image is divided into many sufficient sub-blocks to meet the needs of the users in order to hide their graphic passwords. Implementation of the authentication system on a small smartphone screen makes it difficult to adequately provide enough space for passwords. Moreover, the starting point registered by the user is expanded to include nearby pixels to define a secret hotspot. In this case, defining a small hotspot area helps increase security but at the same time increases rejection rates. In contrast, specifying a large clickable area will enable attackers to guess which area can be clicked.

A cryptographic hash algorithm can be used to hash the coordinates of the secret hotspot to provide confidentiality for the selected area. The value of the hashed coordinates is then stored in the database server. Furthermore, the hidden image can be protected using any encryption algorithm like AES-256 to add a security layer to the secret image inside the cover image.

3.2 Authentication Phase

To verify the identity of the user, the same steps used to create the graphical password are performed. The user must complete all challenges properly in order to log on to the system. Each time a challenge in one of the specified steps is not met; the user is logged out and must try again. If the user fails to log in three times, the account is blocked. Initially, the user is required to type the username to get the list of random related questions. The user must choose a secret question from the list to show the stego image where the secret small image is hidden. This question enables the user to remember the hotspot area identified within the stego image. If the user chooses an incorrect question or clicks on the wrong place, a failed attempt is recorded and he is asked to try another attempt and then a third, after which his account is suspended with the registration request again. When the user clicks on the correct place in the image, the location coordinates are approximately calculated and then concatenated with the salt value stored in the user's account to compute a new hash code. This new hashed value is compared with the value stored in the database to verify the identity of the user. When the values match, a hidden image is displayed to the user to verify the identity of the server, where the user can either press OK to complete the authentication process or cancel it if a different image is displayed. Fig. 2 shows the flowchart of the sequential authentication steps of the graphical password in the proposed scheme.

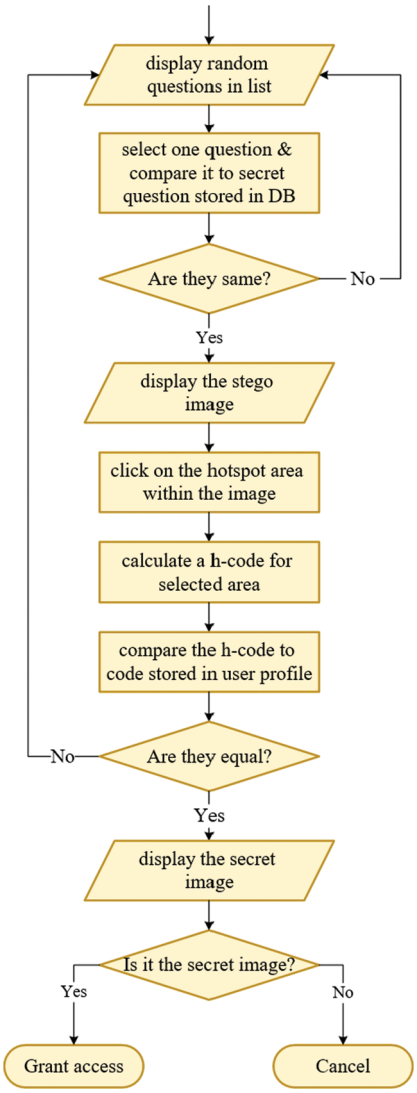

Figure 2: Flowchart of the authentication phase

4 Security and Usability Analysis

4.1 Security Analysis

The main three security features involved in the proposed graphical authentication scheme are a small hidden image, a stego image, and a pre-selected hotspot in the stego image. These security features can be analyzed in relation to password space and entropy challenges.

Password space contributes significantly to securing image-based password schemes. It is referred to as the size of composite keys applied to authentication systems so that users can choose one password from a range of possible passwords. The password space for given questions in the proposed scheme can be computed as follows.

$$Q_s = \sum_{i=1}^{q} T^q \tag{1}$$

where, q–the number of distributed questions in the list, T–the total number of secret questions in the system. Thereafter, the user has to pick up the correct hotspot area inside the stego image to reveal the hidden image. To calculate the password space (A_s) in this stage, the resolution of the stego image (R), as well as its size (S), were taken as follows, where n–the number of selected pixels.

$$A_s = \sum_{i=1}^{n} \left(\frac{R}{S}\right)^n \tag{2}$$

In most cases, password entropy measures the password strength and its resistance to guessing and brute-force attacks. It estimates the number of trails an attacker makes to guess the graphical password. To estimate how uncertain authentication choices can be, we used the entropy formula presented in [23]. In this case, the uncertainty of choice is the selection of the correct hotspot area within the stego image.

$$H(C) = -\sum_{i=1}^{n} p(c_i) log_2 p(c_i) \tag{3}$$

where, C–the total of clicks in the image, $p(c_i)$–the probability of finding the proper pixels. Having a high password entropy makes graphical passwords resistant to password attacks.

4.2 Usability Analysis

Usability is very important for evaluating the efficiency and effectiveness of the graphic password used and comparing it with other available methods.

This authentication scheme operates independently over any remote system that uses web-based resources. It is convenient for users who do not desire to share or store sensitive information on external devices or remote servers they do not control. Furthermore, it enables users from anywhere to access servers of service providers without worrying that their confidential data might be leaked if the device being used is compromised. In addition, the proposed scheme does not include any complex mechanism whereby users can remember their passwords due to the logical relationship between the suggested authentication steps.

5 Experimental Results

The graphical authentication scheme has been implemented in Python programming language using back-end tools like Flask web framework and SQLAlchemy toolkit. In addition, a set of front-end tools such as HTML, CSS, JavaScript, Bootstrap, jQuery have been used to build a web interface for accessing the remote Linux server. In the experiment, we have prepared 108 various small images classified into twelve various categories such as countries, cups, cars, pets, and others. Each class contains nine images distributed randomly over a 3 × 3 image grid. All images were cropped and adjusted using Adobe Photoshop to be the same dimension size of 100 × 100 pixels. After that, various cover images were gathered from the Internet and resized to 400 × 400 pixels. Both small and cover images have been uploaded to the MySQL database server. The small one is used as a secret image and will be hidden by the user into the cover image. Besides, 40 questions relevant to small images have been prepared. The use of questions helps the user to remember the chosen image hidden in the cover image.

In this study, we tested the effectiveness of the proposed graphical authentication system on 40 persons and measured their ability to remember their graphical passwords. Participants have connected to the system via the Internet using their smart phones, tablets or desktops. Participants were asked not to type any information about chosen passwords and to retry logging into the system after a week to test their ability to remember their passwords.

The use of an effectiveness metric helps to measure the usability of the system and therefore ease of use. During the experiment, we evaluated the effectiveness of the system by recording both the time that users need to register in the system and then the time to log in the first and second sessions. Tab. 1 shows the average of registration and login time, number of successful attempts in the second session and the success rate. The success rate shows the efficiency of the system by helping users to remember their graphic passwords.

Table 1: Average time and success rate of the experiments

Reg. time	Session (1)	Session (2)	Successes	Success rate
45 s	12.5 s	13.7 s	38	95%

As shown in Tab. 1, registration process takes longer than authentication since the user must first select the secret question, and then pick the appropriate image to answer it. In addition, a very slight difference is seen in how much time users spend in the first and second sessions, which indicates that how well users remember their passwords and can easily use the proposed system.

As part of experiment, several secret images were deliberately hidden within one cover image in order to examine the effectiveness of the proposed method and study how this affects image quality.

Fig. 3 shows the original and stego images of Petra when 16 different small images are hidden inside.

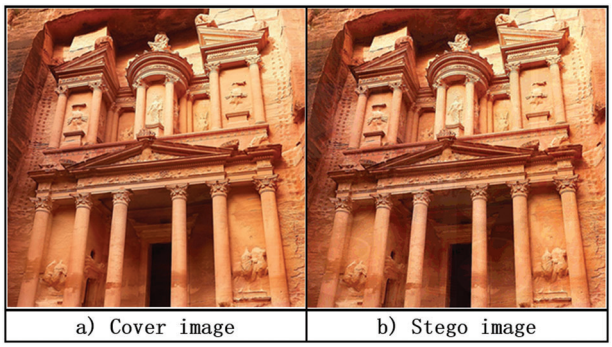

Figure 3: Original- and stego-images

In order to assess the effectiveness of this steganography-based scheme, the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR) parameters are used. Specifically, MSE measures the cumulative squared error between cover and stego images, whereas the PSNR represents the peak error.

MSE value has a direct relationship with error. The lower the MSE value, the lower the error. PSNR criterion is commonly used as a primary test to examine the image quality by measuring the difference between cover and stego images used. The PSNR value can be determined by first calculating the mean-squared error using eq. (4), where m represents the number of rows and n is the number of columns in the image.

$$MSE = \frac{1}{m.n} \sum_{x=0}^{m} \sum_{y=0}^{n} [I_1(x,y) - I_2(x,y)]^2 \tag{4}$$

Then, the PSNR value is calculated using eq. (5) as follows.

$$PSNR = 10\ log_{10}\left(\frac{r^2}{MSE}\right) \tag{5}$$

r-denotes the maximum pixel intensity between cover and stego images.

A steganographic methodology with a variety of embedding rates is applied to multiple images to estimate the quality of the stego image. Tab. 2 shows the PSNR and MSE results among the cover and stego images. The results show how much the image changes each time a new image is hidden within the same stego image.

Table 2: The comparison of cover and stego sequence images during 16 rounds

Images	PSNR	MSE
0 + 1	42.83043767	3.388727083
1 + 2	43.73892456	2.749083333
2 + 3	43.32009066	3.027410417
3 + 4	43.91525446	2.639702083
4 + 5	43.84061606	2.685460417
5 + 6	44.46889799	2.323756255
6 + 7	43.48425041	2.915112555
7 + 8	42.84482592	3.377518755
8 + 9	44.05660419	2.555170833
9 + 10	42.47404189	3.678545833
10 + 11	42.21323569	3.906220833
11 + 12	44.56861633	2.271008333
12 + 13	44.35099086	2.387708333
13 + 14	44.49828876	2.308083333
14 + 15	43.83807307	2.687033333
15 + 16	43.83807307	2.687033333

The results show that although a new image is added in each round to the previous stego image, the range of numbers in decibels remains within the acceptable range without affecting the quality of the original image significantly because only the least significant bits are changed in the cover image without affecting the most significant bits. Fig. 4 illustrates how the PSNR and MSE values change as new images are added and hidden. According to the inverse relation between MSE and PSNR, the lower values of MSE indicate the least amount of error in the cover and stego images, while PSNR value is high when the image reconstruction quality is better. To further improve the image quality, it is necessary to determine the optimum number of images that can be included within the image based on the properties of the image and the number of pixels that can be used in the steganography process.

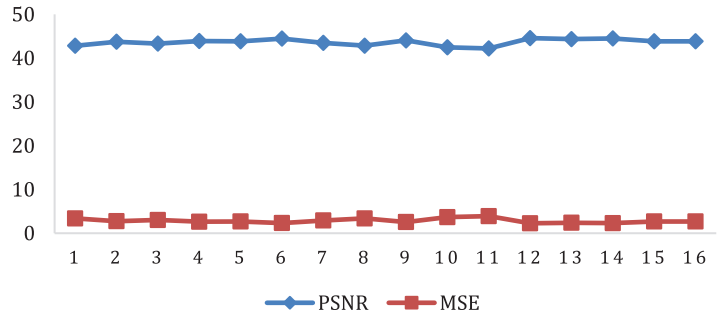

Figure 4: PSNR and MSE of the proposed scheme

Fig. 5 shows some samples of stego images and their histogram when hiding multiple images in different places. Tab. 3 demonstrates the PSNR test of the proposed scheme in comparison with other steganography methods. It shows that the proposed solution achieves better results than some existing methods such as adaptive LSB [24], multi-stage protection using Pixel Selection [25], and hybrid cluster-based steganographic authentication algorithm [19]. The reason behind this is that small changes occur in the discrete cosine transformation coefficients. It is seen that the proposed solution of steganography used to hide multiple images sequentially provides improved values over the other methods designed to hide a single object within a cover image.

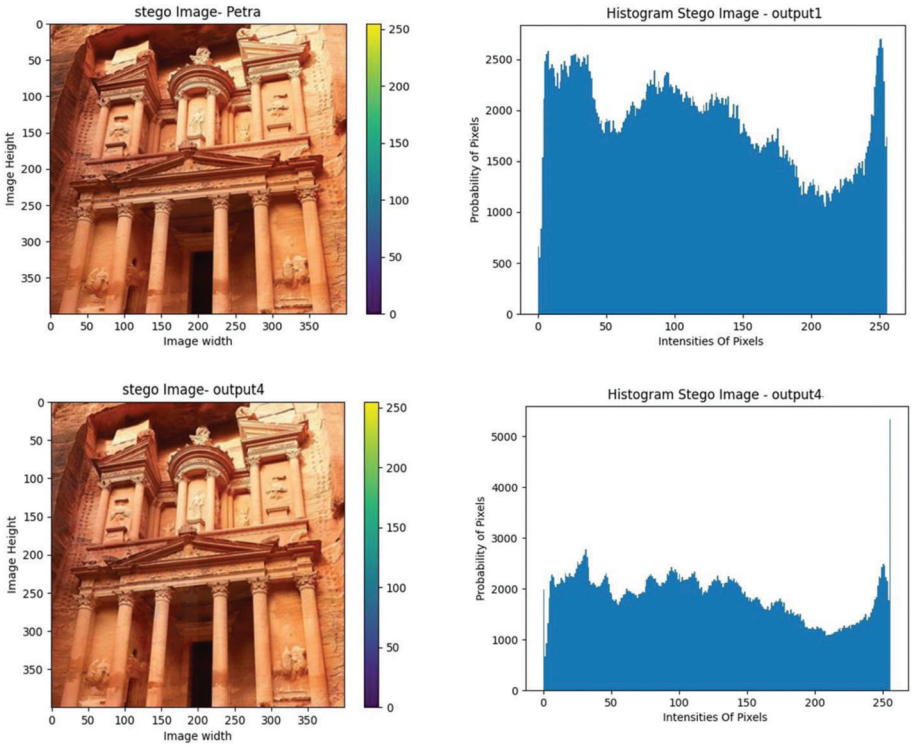

Figure 5: Continued

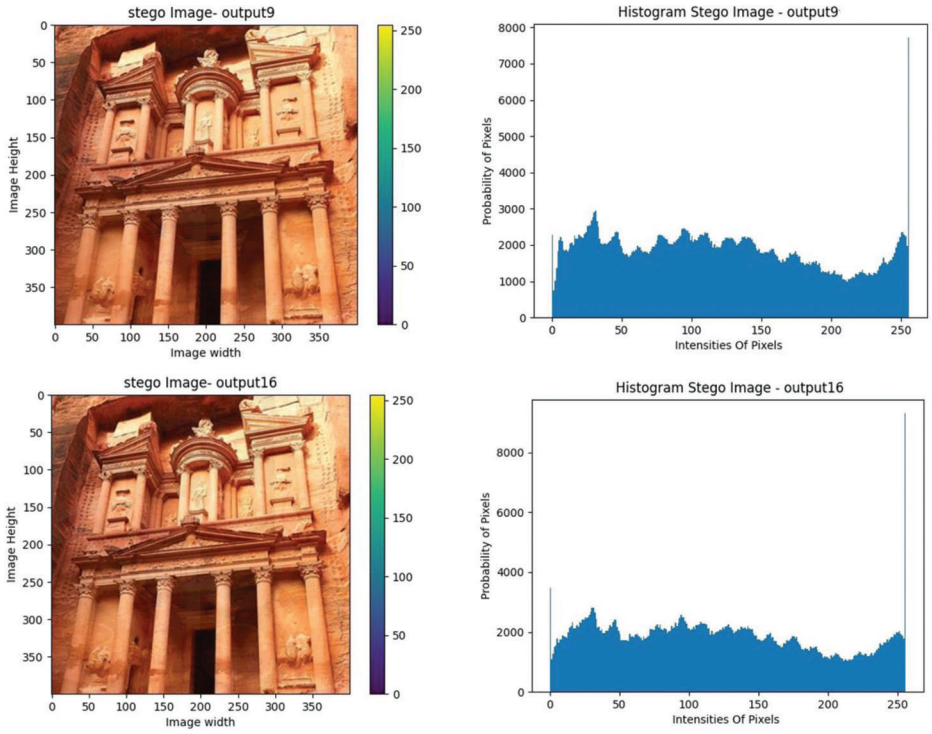

Figure 5: Histogram of multiple-image steganography

Table 3: A comparison between the proposed scheme and other steganography methods

Method	PSNR (dB)
Proposed scheme	52.31
Adaptive LSB [24]	48.21
Pixel selection technique [25]	47.53
Hybrid cluster-based [19]	45
Basic LSB	42.21

6 Conclusion

This paper presents a steganography-based graphical authentication solution that integrates both recognition and recall-based algorithms on the one hand and the LSB steganography technique on the other. The combination of LSB in graphical password scheme increases the security level of control systems in order to provide a more secure and convenient environment. This web-based authentication scheme is independent of a remote system used. It is useful for users who do not wish to store sensitive data on remote servers beyond their control. In the proposed system, users are easily able to memorize their passwords without sacrificing security. Security features have been analyzed with regard to various security aspects such as password space and entropy challenge. The effectiveness of the proposed scheme was evaluated using PSNR and MSE parameters. The experimental results showed that there is relative stability in the PSNR and MSE values despite the increase of hidden images within the stego image.

Funding Statement: The researcher would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Mihajlov and J. Borka, "On designing usable and secure recognition-based graphical authentication mechanisms," *Interacting with Computers*, vol. 23, no. 6, pp. 582–593, 2011.

[2] S. Varshney, M. S. Umar and A. Nazir, "A secure shoulder surfing resistant hybrid graphical user authentication scheme," in *Cybernetics, Cognition, and Machine Learning Applications. Algorithms for Intelligent Systems*. Singapore: Springer, pp. 79–87, 2020.

[3] S. Xiaoyuan, Z. Ying and G. Scott, "Graphical passwords: A survey," in *Proc. 21st Annual Computer Security Applications Conf. (ACSAC'05)*, Tucson, AZ, pp. 463–472, 2005.

[4] F. Towhidi and M. Masrom, "A survey on recognition-based graphical user authentication algorithms," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, pp. 119–127, 2009.

[5] G. Haichang, J. Wei, Y. Fei and M. Licheng, "A survey on the use of graphical passwords in security," *Journal of Software*, vol. 8, no. 7, pp. 1678–1698, 2013.

[6] K. Benzidane, S. Khoudali, L. Fetjah, S. J. Andaloussi and A. Sekkaki, "Application-based authentication on an inter-VM traffic in a cloud environment," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 148–166, 2019.

[7] Z. Zheng, X. Liu, L. Yin and Z. Liu, "A hybrid password authentication scheme based on shape and text," *Journal of Computers*, vol. 5, no. 5, pp. 765–772, 2010.

[8] S. Goel, A. Rana and M. Kaur, "Comparison of image steganography techniques," *International Journal of Computers and Distributed Systems*, vol. 3, no. 1, pp. 20–30, 2013.

[9] W. -J. Chen, C. -C. Chang and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3292–3301, 2010.

[10] S. Katzenbeisser and F. A. Petitcolas, "Information hiding techniques for steganography and digital watermarking," in Computer Security Series. Illustrated. ed., Norwood, Massachusetts, USA: Artech House, 2000.

[11] S. Cheong, H. -C. Ling and P. -L. Teh, "Secure encrypted steganography graphical password scheme for near field communication smartphone access control system," *Expert Systems with Applications*, vol. 41, no. 7, pp. 3561–3568, 2014.

[12] H. B. Anitha, R. Adithi, S. Irudaya and V. Vidya, "Graphical password based authentication system," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 2, pp. 169–171, 2016.

[13] T. H. Lin, C. -C. Lee, C. -S. Tsai and S. -D. Guo, "A tabular steganography scheme for graphical password authentication," *Computer Science and Information Systems*, vol. 7, no. 4, pp. 823–841, 2010.

[14] M. B. Goel, V. B. Bhagat and V. K. Katankar, "Authentication framework using visual cryptography," *International Journal of Research in Engineering and Technology*, vol. 2, no. 11, pp. 271–274, 2013.

[15] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi and A. Gutub, "Secure mobile computing authentication utilizing hash, cryptography and steganography combination," *Journal of Information Security & Cybercrimes Research*, vol. 2, no. 1, pp. 73–82, 2019.

[16] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan, "Graphical password authentication scheme for embedded platform," *Journal of Artificial Intelligence*, vol. 7, no. 4, pp. 161–171, 2014.

[17] W. Yang, S. Wang, J. Hu, A. Ibrahim, Z. Guanglou *et al.,* "A cancelable iris- and steganography-based user authentication system for the internet of things," *Sensors*, vol. 19, no. 13, pp. 2985, 2019.

[18] M. D. A. Devi and K. B. ShivaKumar, "A novel image steganography technique for secured online transaction using DWT and visual cryptography," in *Proc. IOP Conf. Series: Materials Science and Engineering*, Narsimha Reddy Engineering College, India, vol. 225, pp. 012070, 2017.

[19] K. Venkatraman and K. Geetha, "Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm," *Automatika*, vol. 60, no. 3, pp. 314–321, 2019.

[20] A. Yassin, A. Rashid, Z. Abduljabbar, H. Alasadi and A. Aldarwish, "Toward for strong authentication code in cloud of internet of things based on DWT and steganography," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 10, pp. 2922–2935, 2018.

[21] S. K. Omed, "Steganography-based password management: A conceptual model," *Zanco Journal of Pure and Applied Sciences*, vol. 31, no. 3, pp. 61–68, 2019.

[22] J. Kapil, "An XML transformed method to improve effectiveness of graphical password authentication," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, pp. 11–23, 2017.

[23] K. H. A. Al-Shqeerat and K. I. Abuzanouneh, "A hybrid graphical user authentication scheme in mobile cloud computing environments," *International Journal of Communication Networks and Information Security*, vol. 13, no. 1, pp. 68–75, 2021.

[24] M. Khan, M. Sajjad, M. Irfan, R. Seungmin and W. B. Sung, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," *Future Generation Computer Systems*, vol. 86, no. 4, pp. 951–960, 2018.

[25] K. Abuzanouneh and M. Hadwan, "Multi-stage protection using pixel selection technique for enhancing steganography," *International Journal of Communication Networks and Information Security*, vol. 13, no. 1, pp. 55–61, 2021.