International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 12, No. 1, February, 2022, pp. 21-29
Journal homepage: http://iieta.org/journals/ijsse

Passnumbers: An Approach of Graphical Password Authentication Based on Grid Selection

Seerwan Waleed Jirjees[*], Ali Majeed Mahmood, Ahmed Raoof Nasser

Control and Systems Engineering Department, University of Technology, Baghdad 10066, Iraq

Corresponding Author Email: seerwan.w.jirjees@uotechnology.edu.iq

https://doi.org/10.18280/ijsse.120103

Received: 1 January 2022
Accepted: 12 February 2022

Keywords:
graphical password, authentication, shoulder surfing, cryptanalysis, grid selection

ABSTRACT

The authentication textual passwords are the most widely used technique. However, this type of legacy authentication is vulnerable to various attacks, such as shoulder-surfing attacks. Hence, graphical password authentication is one of these approaches which has been suggested to overcome the issues related to textual passwords. Nevertheless, the hackers have also developed new techniques that can be finally broken the graphical password, for instance, listening to the transmitted information between the client and the server. In this paper, Passnumbers graphical authentication password is proposed. Passnumbers approach involves two new stages, which are first, using the coordinates of a graphical grid cells-based numbers for entering the password. The second stage is represented by deploying a new technique to encrypt the password based on the image pixels. The performance evaluation reveals that the proposed Passnumbers can provide high resistance against several graphical password attacks including shoulder surfing and eavesdropping attacks. Passnumbers is evaluated using several metrics including security and usability.

1. INTRODUCTION

Authentication is the process by which a person's identity is verified in a large number of applications including websites and mobile computing environments. It is also a way to establish the truth whether the data feature claimed by an entity is valid or not. The authentication system stores identity provided in the user information database within the computing system user information database [1, 2]. During verification, if the credentials entered match with this information stored in the database, the verification process is completed, and the user gets permission to access the system. Throughout this process, hackers have many ways to break the user password to access private information [3]. Therefore, several challenges may confront the design of authentication systems. One of these challenges is how to maintain high security, but also convenient or simple to use [3]. In the classical textual passwords, using a string of characters may be vulnerable to what is so-called the ‘Dictionary Attack’ [4], which relies on frequent passwords that could be used by users. In other words, there is a trade-off between the ease of passwords that can be simply guessed and its difficulty which is often difficult to remember. To overcome the problem of low security, one of the possible alternative solutions is graphical authentication that uses images, shapes, or patterns as a password easier to remember or recognize than text.

Graphical password has been proposed as a possible alternative to text-based schemes, which adds more difficulty against some of the common attacks. For instance, the dictionary attack, brute force, replay attack, eavesdropping and spyware attacks [5, 6]. There are several advantages for using graphical password authentication technology which are i), the dictionary attacks and brute forces search are infeasible; ii) graphical password provides a way of making more human-friendly passwords with high security; iii) reduces the burden of human memory as in the classical text-based password However, the graphical password is also exposed to several new attacks such as shoulder-surfing attacks [6, 7]. which requires more complected authentication approaches to maintain high level of security.

In this paper, a new graphical password authentication called Passnumbers is proposed to enhance the legacy graphical password approach. Passnumbers uses numbers in the range from 0 to 99 for entering the password based on the index of both rows and columns locations on the grid cells. Additionally, a new method is used to encrypt the password over the transmission medium via encoding the password using the image pixels. The proposed method is resistant to shoulder attacks where it is very difficult for the attacker to monitor the entry because the password locations on the grid are constantly changing due to the changing of the location numbering of rows and column. To the best of author’s knowledge, no research study has been followed similar the procedure of the proposed Passnumbers approach. The rest of the paper is structured as follows. In section 2, a concise literature review of the previous work is presented. Section 3 presents the proposed Passnumbers method. Section 4 includes the analysis and the experimental results. In section 5, some conclusions with key future ideas are provided.

2. RELATED WORK

Regarding the prior works, several research studies have been conducted to focus on the problem of information security and authentication. Some of these contributions that have been commonly used are summarized as follows. Sadasivam et al. [7] has proposed the Blonder authentication approach in which the user can click on different positions of the image that are already clicked on the password creation phase. The advantage of this approach is to provide a hint for the user to recall the password. However, the main drawback is the password space is very little and also users cannot arbitrarily click on the background. Likewise, Syukri et al. [8] have developed the so-called Syukri authentication method where the users can draw their signatures using the mouse. Goldberg et al. [9] have proposed the Passdoodle authentication or (hand-drawn) method, which allows the user to draw on the touch-sensitive screen using a stylus. This enables the user to remember whole doodle images accurately like the alphanumeric passwords. Zhao and Li [10] propose an authentication approach called the Textual-Graphical password authentication approach. In this method, a combination of graphics and texts is used to avoid different types of attacks such as shoulder surfing, brute force attack, hidden cameras, and spyware attacks.

Tao et al. [11, 12] have developed a Pass-Go graphical password method. In this method entering the password is achieved by choosing the intersections on the generated grid. which was inspired by the Chines game “GO”. This method can offer 256 bits as password space and can be applied to a large number of applications. However, this scheme has a significant drawback which is that the user can easily forget their stoke sequence. This causes the user to often set simple passwords which will reduce security and increase vulnerability to graphical dictionary attacks. Zangooei et al. [13] develop the Passpoint authentication method which is inspired by the idea of Blunder’s method by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, the user can click on any place on an image (as opposed to some pre-defined areas) to create a password. Chiang and Chiasson [14] have focused on the challenge of typing text passwords in touchscreens mobile devices, so a touchscreen multi-layered drawing approach has been proposed as a graphical password to be used in touchscreens devices. The proposal tries to maintain the input accuracy issues while keeping a secure password.

Different other research studies have been proposed for graphical password technology. A hybrid pin keypad has been used with the graphical password authentication which can be deployed in banking applications [15]. The shoulder surfing attack is one of the main purposes of developing this method. Yao et al. [16] have tried to connect between the text-based and topological graphic passwords to improve the security of the authentication process. This has been applied by using some graph labeling that is related to some mathematical conjectures. The focus was on the representation of text-based passwords in form of topological graphic passwords.

Likewise, pattern-based password authentication has been developed in the studies of Sinha et al. and Hemamalini and Saranya [17, 18]. In these studies, the user has to select the pattern type throughout the registration. In the process of login, the password is represented in form of a textual password that must be entered in order like the patterns that have been selected in the registration phase. Here, the style of text password grid is presented randomly with objects such as images, numbers, or characters which is more difficult against the shoulder surfing attack.

All of the mentioned studies have compared different mechanisms of password entry that combine graphics and text in the authentication process and shoulder surfing attacks resistance. However, the password entry is rarely encrypted or encoded in a new way. Furthermore, to best our knowledge, no studies have used numbers to enter the password directly on the graphical grid cells as shown in the proposed method.

3. THE PROPOSED PASSNUMBERS APPROACH

The proposed Passnumbers is designed to be resistant to shoulder attacks where it is very difficult for the attacker to monitor the method of entry because the password locations on the gird are constantly changed, which results from changing the numbering of rows and columns. The Passnumbers is also considered a new way to encrypt the password based on the image data sent by the server during the authentication phase. In other words, the password does not send directly or encrypted by traditional methods, but it will be encoded using data from the image sent by the server. The detail of the Passnumbers structure approach is depicted in Figure 1, which consists of two main stages. The first stage involves entering the password. In the next stage, the image is sent by the server to be encrypted to encode the password.

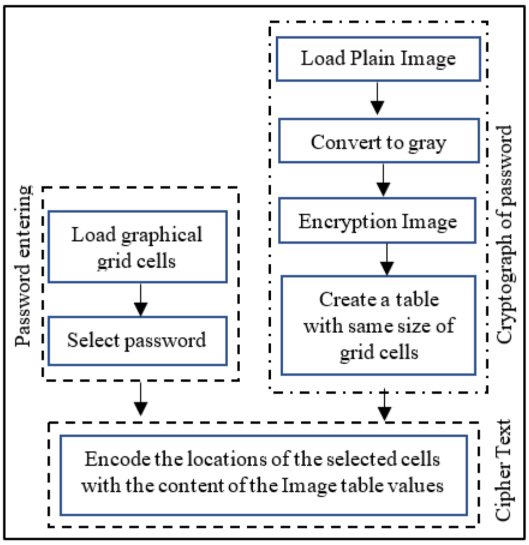

Load Plain Image
Convert to gray
Encryption Image
Create a table with same size of grid cells
Cryptograph of password
Password entering
Load graphical grid cells
Select password
Encode the locations of the selected cells with the content of the Image table values
Cipher Text

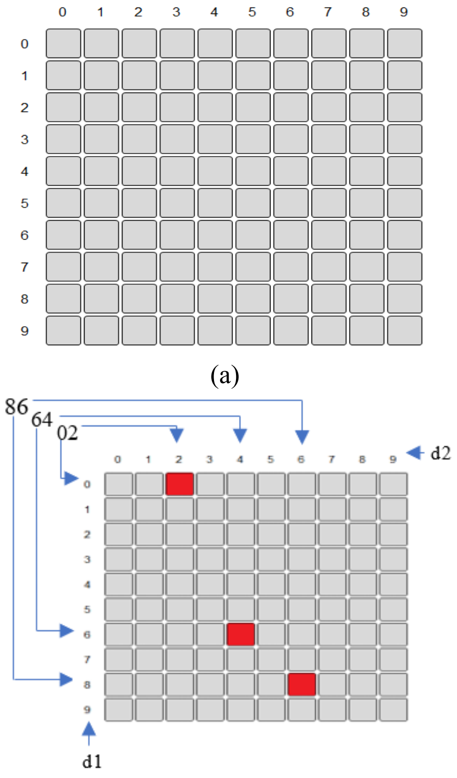
Figure 1. Structure of the proposed Passnumbers authentication approach

3.1 Password entering technique

There are two main parts included in the process of password entering in the proposed approach as follows.

3.1.1 Grid-based password system

The designed grid size is 10 x 10 which consists of square-shaped cells as shown in Figure 2 (a). Numbers of rows and columns locations will be displayed in grid cells to enable the user for choosing the cells corresponding to the password. The selection is made by clicking on the required cell independently. In other words, each button will be represented by a pair of coordinates resulting from the intersection of the row and the column. Hence, the cells grid is represented by two-dimensional coordinate pairs as shown in Figure 2(b). The cell in the grid is represented by two indexes which are the row index (R) and the column index (C). Columns and rows of the grid are numbered from (0 to 99), and the arrangement of numbers is varying dynamically at each login process to strengthen the resistance to shoulder surfing attacks. The applied grid size is relatively large, so it is very difficult to guess the password by the attackers and makes it resistant to guess attacks also.



(a)

(b)

Figure 2. Graphical password grid: (a) Blank grid cell (b) Example of selecting a password on grid cell

3.1.2 Password selection

In the Passnumbers approach, the user can choose a set of numbers that depend on the size of the grid cells, which will be located on the intersections of the grid cells between the row and the column represented in the two dimensional coordinate pair. The point of interest in the proposed system is that how to locate the password in (m * n) grid cells by crossing the row and the column in which their locations are changeable in every login session to avoid the shoulder surfing attack. The password consists of a set of numbers chosen by the user in a range between (0 to 99), each value includes two digits which are illustrated by Figure 2-b and Eq. (1). The first digit in the pair is used to select the row and the second digit is used to select the column. This formulation is easy to use since it depends on numbers, which have to be entered graphically by clicking cells on the grid.

$$P = V_1, V_2, V_3, \dots V_r \qquad (1)$$

where, P is the position of the cell on the grid, r is the length of the password and V refers to values of password containing two digits, which are selected as in Eq. (2).

$$V = d_1 * 10^1 + d_2 * 10^0 \qquad (2)$$

where, d1 represents the selection of rows (m), d2 represents the selection of columns (n).

The applied policy for creating a strong and dynamic password has followed a set of rules that are designed to increase the security of passwords as follows:
i) Minimum length of numbers (r) is 8.
ii) Maximum length of numbers (r) is 20.
iii) At least four of the numbers (V) are different in d1.
vi) At least four of the numbers (V) are different in d2.
vii) Repeating similar numbers is unacceptable.

3.1.3 The authentication of the proposed system

In authentication connection, the proposed framework includes two phases: the registration phase and the authentication phase as shown in Figure 3.

A. Registration phase

The registration phase involves the process of requesting the login to the server, which is divided into six steps.

Step 1. *User*: Send his/her ID to the server.

Step 2. *Server*: Check the availability of user ID, if the received ID exists in the database, then go to step 1 and ask the user for another ID, else go to step 3.

Step 3. *Server*: Select a random image, then choose the encryption algorithm, and prepare a grid cell.

Step 4. *User*: Select the password (numbers selection from grid cells)

Step 5. *User*: Password is used as a key for an encryption algorithm to encrypt the image then execute the passnumbers approach to encode the password and send it to the server using Algorithm2.

Step 6. *Server*: Decoding the ciphertext using Algorithm 3

Step 7. *Server*: Store password to the respective user ID, then the server informs the user that the process is successful.

B. Authentication phase

The process of authentication has to implement on both the user and server sides.

- *Authentication at the user side*

Step 1. The user inserts his/her ID and password by clicking cells for the grid shown in Figure 2.

Step 2. The image is encrypted after the user enters his/her password, where the password is a key for the encryption algorithm.

Step 3. The password is ciphering by applying the passnumbers approach depending on step (demonstrate in Algorithm2)

Step 4. Submit ID and graphical password, then wait for the response from the server.

- *Authentication at the Server-side*

Step 1. Select a random image and the encryption algorithm.

Step 2. Prepare a grid cell and arrange random rows and columns.

Step 3. The server verifies the user ID, if it exists in the user database table, go to step 4, otherwise, exit from the authentication phase.

Step 4. Use a password as a key to encrypt the image.

Step 5. Apply the decoding algorithm as shown in Algorithm 3 to get a plain password, then make a comparison with the value that has been saved in the database table, if there is a difference, the server will reject the login request, otherwise, the server has accepted the authentication request.

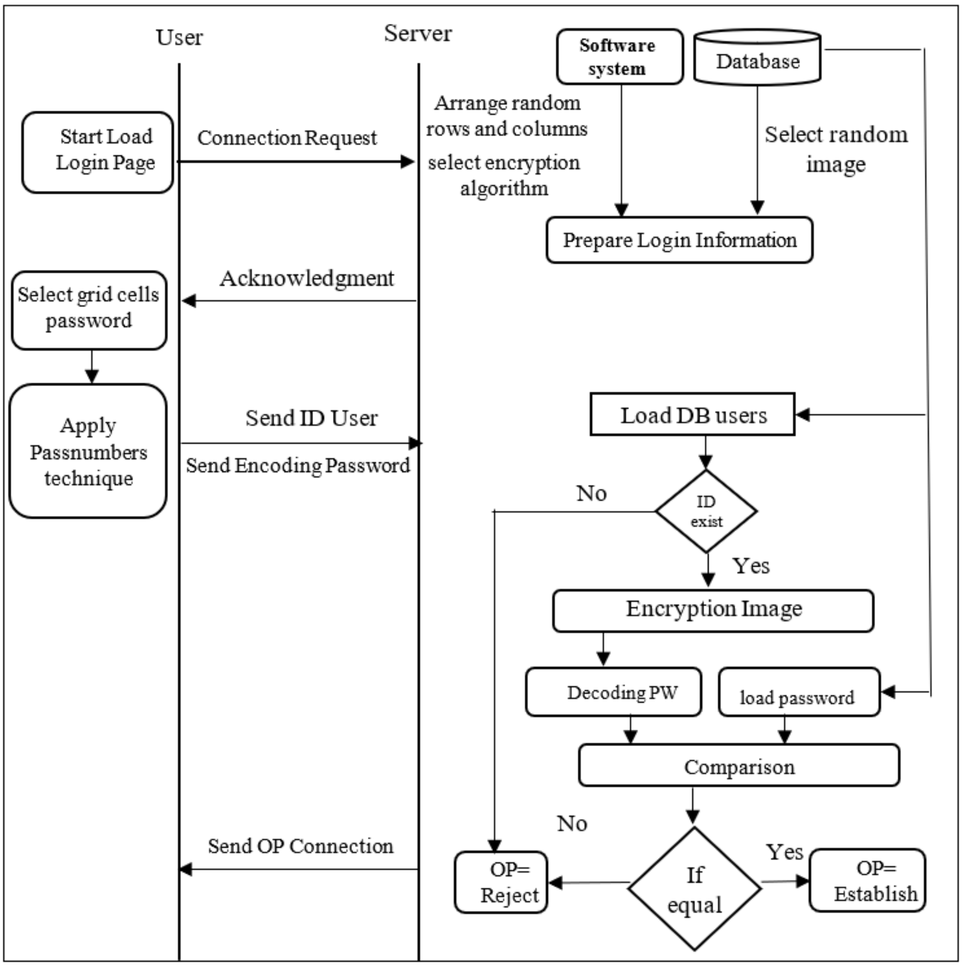
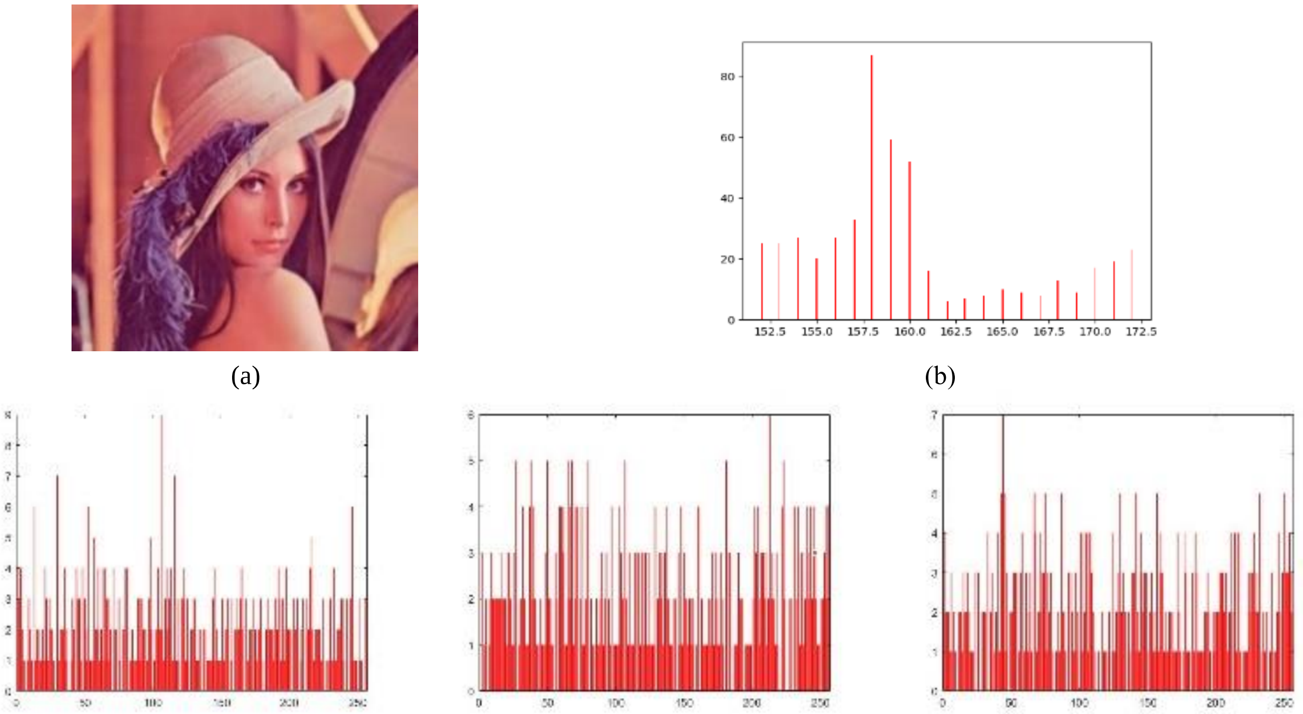


Figure 3. The authentication phase of proposed system



(a)

(b)

(c)

(d)

(e)

Figure 4. The histogram analysis results. (a) Original test image, (b) histogram of original image, (c) histogram of encryption image by DES, (d) histogram of encryption image by AES, (e) histogram of encryption image by Blowfish

3.2 The proposed cryptography technique

In fact, in each request for authentication, an image that is randomly chosen from many images in the server's database is to be sent to the client side. The random selection of the image does not affect the efficiency of data encryption, since the proposed system depends on the strength of the algorithm which generates random numbers in each process. Using different images will confuse the attacker and the data analysis process will be highly complicated since the analyses of the encrypted text depended on the previous image that has been sent. The most important characteristic of the proposed method is that the data encryption process will depend on image data will be encrypted to obtain random values. Hence, any algorithm or method can be used to obtain random values and the entered password will be a key to encrypt the image.

A set of encryption algorithms (AES, DES, and Blowfish) were used, which were applied to the image of Lena. Figure 4 shows an approximate number of pixels for colorimetric values. Thus, all values between (0-255) will be represented, and this provides all possibilities in the password character encoding process to resist an eavesdropping attack. The randomness in password encryption depends on the entropy criterion of the encrypted image, where the entropy is a measure of the degree of randomness in the image [19-21]. The entropy of information for our original test images is listed in Table 1, along with the entropy of the encoded information. The absolute entropy of the entropy values of the AES, DES, and Blowfish encryption algorithms are 7.6064, 7.5789, and 7.5828 respectively, which are close to the ideal number 8. According to the entropy statistics, the ciphertexts have a high level of randomness among the pixel values.

Table 1. Entropy of original images and other encryption algorithm

Original image	DES	AES	Blowfish
3.9877	7.6064	7.5789	7.5828

3.3 Encryption and decryption methods

After the image encryption process, a table will be selected from the middle of the image to ensure using randomly distributed numbers. The columns of the selected table will be (10 x N) and the rows will be 10, N is the number of bytes representing each letter in the password. In our proposed system we assumed N equals 5 so each digit/character from the password will be encoded with a 5-digits value that changes in each new connection process as shown in Figure 5, where these values are taken from the table created from the encrypted image data.

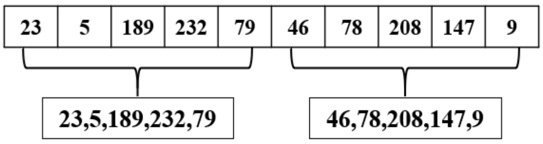


Figure 5. Encoding encryption image pixels technique

Algorithm 1: Function: Encoding Image Matrix ()

```
Input:
  EG(r,c)          // Encryption image where r,c Rows
and columns of image
Output:
 P(10,10)          // encoding table
    create a temporary variable c=0
    create a temporary array h=[]
    For i=0  to 10 // loop for rows
       For j=0  to 50 step 5 //loop for columns
          For k=j to j+5 //loop to select 5 values
             h=h& EG[i,k]//append 5 values
          End for k
          p[i,c]= h
          c+=1
       End for j
       c=0
       h=[]
    End for i
    Return (P)
    End function
```

- Client Side

After entering the password by the user, the password will be encrypted before the transmission as shown in Algorithm 2.

Algorithm 2: Image encryption

```
Input:
   G(r,c)   //Grid Cells where r,c rows and columns
   S (n,m)  // Image  where n,m rows and columns
    V       // password values V=(r1,r2,…., s) where
r=0,.., r*c and s=length of  V
Output:
     T        // Cipher text
convert Image S to gray scale G
Encryption image G(r,c) to EG(r,c)
Create array P(n,m) // call  Algorithm 1
Entering password by clicking on grid cells G
//where V1=$G_1$(n,m) , V2=$G_2$(n,m) ,… $V_s$ =$G_s$(n,m)
T= [ ]  //create empty array
For i=1 to s //loop to length of password
   z =int (Vi/10) //read second digit
   x =Vi%10 //read first digit
   T[i]=Pi[z,x] //read the location of encoding
function array
End for
```

- Server Side

The password sent will be verified by applying the decryption process shown in Algorithm 3. Upon receiving the encrypted text, the server will perform the encryption process for the same image, depending on the password stored in the database. Afterward, when the password is correct, the user will have access to the system, or the process will be canceled in case of the wrong input password.

Algorithm 3: Image decryption

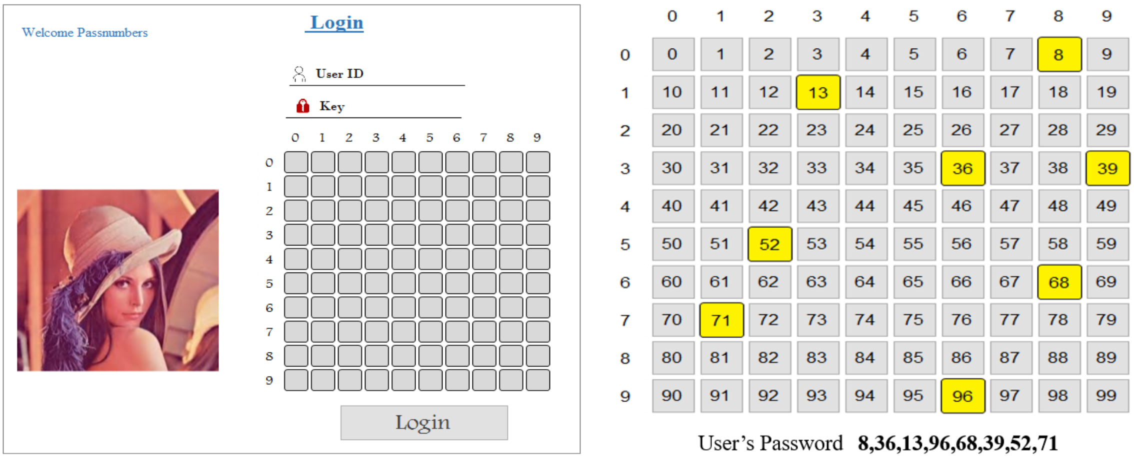
```
Input:
S (n,m)  //Image  where n,m rows and columns
V          // original password that saved in the
database,V=(r1,r2,…., s) where r=0,.., r*c and s=length of
V
C         // Cipher text C=($r_1$,$r_2$,…., s) where r=0,1.., 255
and s=length of  C
```

Output:

```
D          //statues of connection
Convert Image S to grayscale G
Encryption image G(r,c) to EG(r,c)
Create array P(n,m) // call  Algorithm 1
T=[]
For i=1  to s
    z=int(Vi/10)
    x=Vi%10
    T[i]=P[n,m]
End for
For i=1  to s *5  \\compare cipher text of server and client
        If T[i]<>C[i]
                Break and exit ()     // send to client authentication rejected
        End if
End for
send to client Authentication successful
```

4. ANALYSIS AND EXPERIMENTAL RESULTS

The graphical user interface of Passnumbers system shown in Figure 6 involves important features which are the random changing of the image and grid indexing numbering at each login session to enable the authentication system to be more secure. Different types of possible attackers that may face the proposed algorithm will be explained as follows.

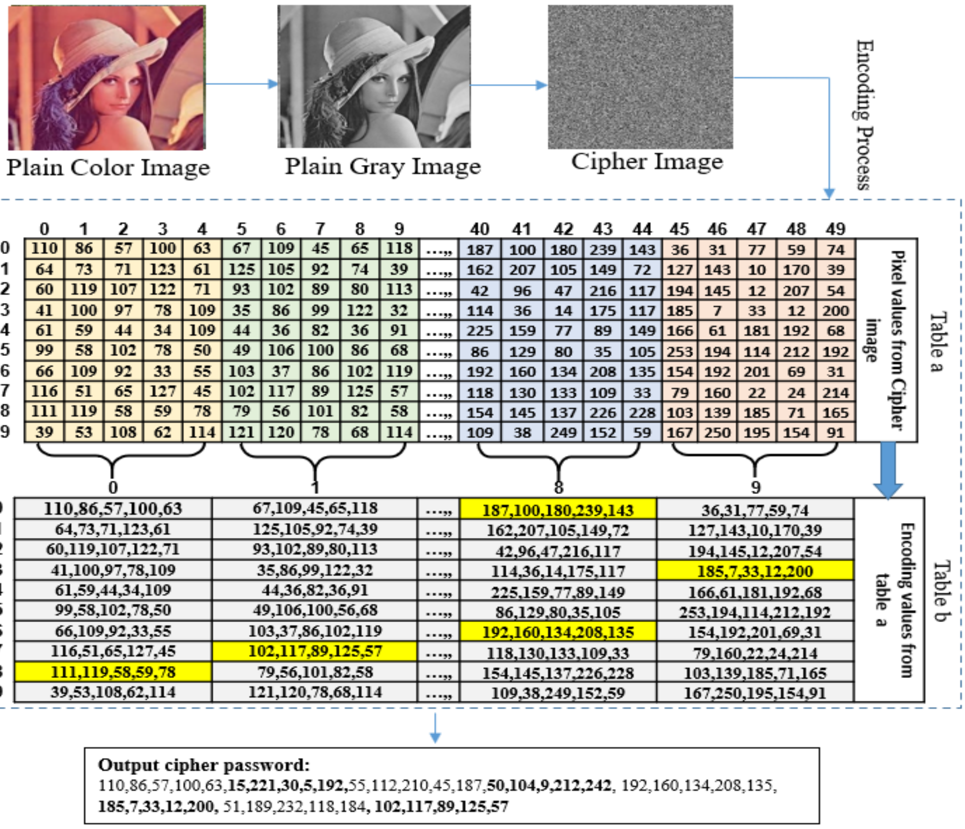


	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	10	11	12	13	14	15	16	17	18	19
2	20	21	22	23	24	25	26	27	28	29
3	30	31	32	33	34	35	36	37	38	39
4	40	41	42	43	44	45	46	47	48	49
5	50	51	52	53	54	55	56	57	58	59
6	60	61	62	63	64	65	66	67	68	69
7	70	71	72	73	74	75	76	77	78	79
8	80	81	82	83	84	85	86	87	88	89
9	90	91	92	93	94	95	96	97	98	99

User's Password **8,36,13,96,68,39,52,71**

(a) (b)

Figure 6. Graphical user interface



	0	1	2	3	4	5	6	7	8	9		40	41	42	43	44	45	46	47	48	49
0	110	86	57	100	63	67	109	45	65	118	…,,	187	100	180	239	143	36	31	77	59	74
1	64	73	71	123	61	125	105	92	74	39	…,,	162	207	105	149	72	127	143	10	170	39
2	60	119	107	122	71	93	102	89	80	113	…,,	42	96	47	216	117	194	145	12	207	54
3	41	100	97	78	109	35	86	99	122	32	…,,	114	36	14	175	117	185	7	33	12	200
4	61	59	44	34	109	44	36	82	36	91	…,,	225	159	77	89	149	166	61	181	192	68
5	99	58	102	78	50	49	106	100	86	68	…,,	86	129	80	35	105	253	194	114	212	192
6	66	109	92	33	55	103	37	86	102	119	…,,	192	160	134	208	135	154	192	201	69	31
7	116	51	65	127	45	102	117	89	125	57	…,,	118	130	133	109	33	79	160	22	24	214
8	111	119	58	59	78	79	56	101	82	58	…,,	154	145	137	226	228	103	139	185	71	165
9	39	53	108	62	114	121	120	78	68	114	…,,	109	38	249	152	59	167	250	195	154	91

	0	1		8	9
0	110,86,57,100,63	67,109,45,65,118	…,,	187,100,180,239,143	36,31,77,59,74
1	64,73,71,123,61	125,105,92,74,39	…,,	162,207,105,149,72	127,143,10,170,39
2	60,119,107,122,71	93,102,89,80,113	…,,	42,96,47,216,117	194,145,12,207,54
3	41,100,97,78,109	35,86,99,122,32	…,,	114,36,14,175,117	185,7,33,12,200
4	61,59,44,34,109	44,36,82,36,91	…,,	225,159,77,89,149	166,61,181,192,68
5	99,58,102,78,50	49,106,100,56,68	…,,	86,129,80,35,105	253,194,114,212,192
6	66,109,92,33,55	103,37,86,102,119	…,,	192,160,134,208,135	154,192,201,69,31
7	116,51,65,127,45	102,117,89,125,57	…,,	118,130,133,109,33	79,160,22,24,214
8	111,119,58,59,78	79,56,101,82,58	…,,	154,145,137,226,228	103,139,185,71,165
9	39,53,108,62,114	121,120,78,68,114	…,,	109,38,249,152,59	167,250,195,154,91

Output cipher password:
110,86,57,100,63,**15,221,30,5,192,**55,112,210,45,187,**50,104,9,212,242**, 192,160,134,208,135, **185,7,33,12,200**, 51,189,232,118,184**, 102,117,89,125,57**

Figure 7. Example of the Passnumbers approach

A practical example of the entire of Passnumbers approach is shown in Figure 6 and Figure 7. The example consists of the following steps.

Step 1: The first stage represents the password insertion. The selected password is (8,36,13,96,68,39,52,71) which generated as follows: the first value a “8” is inserted by clicking the cell that has row number 0 and column number 8, the second value is inserted by clicking the cell that has row number 3 and column number 6 and these steps are repeated for all password values.

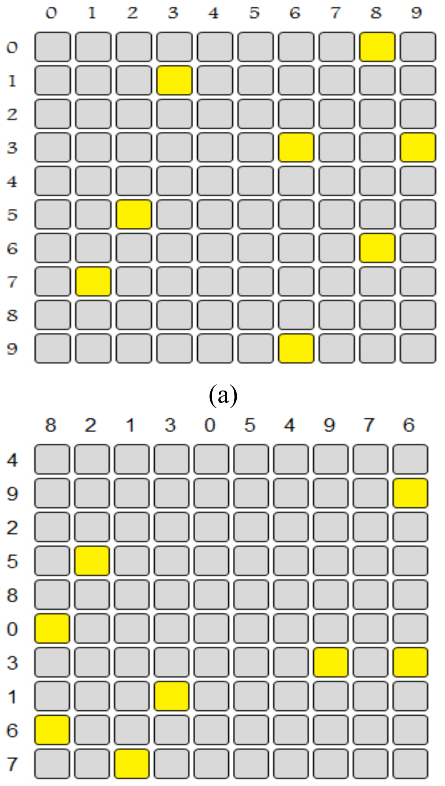
Step 2: The second stage is image encryption. A random image "Lena" has been selected from a server then converted to grayscale.

Step 3: start the encryption process by inserting a key from a client and selecting table 10 * 50 from the image. The proposed system creates table 10*10 similar to the size of graphical grid cells demonstrated in an Algorithm (2).

Step 4: After that, the password is encoded from the table for the encrypted image.

4.1 Shoulder surfing

Shoulder surfing is an attack on password authentication by direct observation or by registering individual authentication [22]. The proposed approach resistive this attack, since the order of numbering for columns and rows will be changed dynamically within an algorithm in each new process of communication. Figure 8 (a) illustrates the default arrangement is a sequence of columns and rows, while Figure 8 (b) it can be noticed a change in the numbering order. Therefore, when the attacker notices or records the entry process, the stolen number is useless since it cannot be used in the next time for entering the system.



(a)

(b)

Figure 8. Arranging numbers in different ways in grid cell: a) Default arrangement, b) Change in the numbering order

4.2 Replay attack

In these types of attacks, the stream of messages that has to be sent between two parties will be copied by the attacker to gain access via replying to the data stream maliciously to the server [2]. The proposed Passnumbers approach is preventing this type of attack since the encrypted text will be changed in every login by changing the image and even in the case of using the same image, the algorithm that is used in the encryption depends on the key with a random value. Hence, the attacker in the event of sending the stolen text from the eavesdropping operation cannot contact and signs of a retransmission attack.

4.3 Brute force attack

The brute force attacks are a search and comparison process for all probabilities in a hope of guessing the intended password correctly. It is worth stating that two important concepts have to be considered in this type of attack, which is password space [23].

4.4 Password space

The total number of all possible passwords of length (L) is 100^L. Therefore, the password space of the proposed Passnumbers scheme denoted by (P_s) can be calculated in the following expression.

$$P_s = \sum_{L=8}^{L=16} 100^L \tag{3}$$

For example, if L = 8, then $P_s=10^{16}$, Where the graphic input process will take, as the best time is five seconds, while the time required for the attacker to complete the process equals up to 578,703,703,703.7 days.

4.5 Eavesdropping attack

In this type of attack, attackers sniff on network communications by listening illegally to the confidentiality information between the client and the server [24]. In the proposed Passnumers, the password is encoded with the values taken from the encrypted image and these values change due to the change of the image on each login. Analyzing the encrypted text from the attacker is the closest to impossible because the password was not entered into the encryption algorithm and the encoding length of each number of the password varies according to the system designer. Eq. (4) is used to determine Eavesdropping attack E_d, where B is the number of bytes to encode each character and L as mentioned earlier is the length of the password.

$$\mathbf{E_d=2^{8*B*L}} \tag{4}$$

For example, suppose the size of an encoding character (B) is five bytes and password length (L) is 8 characters. The probability number of ciphertext analysis is:

$$\mathbf{E=2^{320}} \rightarrow 2.136 \text{ e+96}$$

4.6 Usability issue

The user interface of Passnumbers approach has a grid of cells on-screen that most users are familiar with. However, only the difference being in the number selection process, which is resulted from the intersection of the row and the column. Hence, the user can easily complete the login process . The time factor and cost of implementing the authentication system is one of the most important success points in adopting an authentication system. Hence, it can summarize the advantages of implementation and improvement in the procedures of the work when using the proposed authentication technique.

The input method through the numbers grid can be easily used on various authentication systems that use a mouse or touch screen (such as ATMs, smartphones, tablets, and computers) .The use of the proposed keyboard reduces the cost and time of designing, manufacturing and integrating the physical keyboard into some authentication systems such as ATMs.

5. CONCLUSION

Several attacks may face users while entering a password such as the shoulder surfing, replay attack and eavesdropping attack. Hence, the actual challenge is how can develop a high secure authentication technique for entering a password that is resistant to multi attacks for graphical password with low complexity of entering the password and low require time. The proposed Passnumbers is considered as a new way to encrypt the password based on the image data that should be sent by the server during the authentication phase. it is depended on numbers which are difficult in guessing. The result of the analysis shows that the Passnumbers is an effective approach since the user interaction is easy and simple because the user only searches on the cell from the grid and clicks on it. Furthermore, the proposed approach can be applied in several applications including desktop systems, smart phones and ATMs.

REFERENCES

[1] Binbeshr, F., Kiah, M.M., Por, L.Y., Zaidan, A.A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. Computers & Security, 101: 102116. https://doi.org/10.1016/j.cose.2020.102116

[2] Lee, K., Yim, K., (2020). Cybersecurity threats based on machine learning-based offensive technique for password authentication. Applied Sciences, 10(4): 1286. https://doi.org/10.3390/app10041286

[3] Kumar, B.P., Reddy, E.S. (2020). An efficient security model for password generation and time complexity analysis for cracking the password. International Journal of Safety and Security Engineering, 10(5): 713-720. https://doi.org/10.18280/ijsse.100517

[4] Luo, W., Hu, Y., Jiang, H., Wang, J. (2018). Authentication by encrypted negative password. IEEE Transactions on Information Forensics and Security, 14(1): 114-128. https://doi.org/10.1109/TIFS.2018.2844854

[5] Meng, W., Zhu, L., Li, W., Han, J., Li, Y. (2019). Enhancing the security of FinTech applications with map-based graphical password authentication. Future Generation Computer Systems, 101: 1018-1027. https://doi.org/10.1016/j.future.2019.07.038

[6] Singh, V., Pandey, S.K. (2019). Revisiting cloud security threat: Dictionary attack. In Proceedings of International Conference on Advancements in Computing & Management (ICACM). http://dx.doi.org/10.2139/ssrn.3444792

[7] Sadasivam, G.K., Hota, C., Anand, B. (2018). Honeynet data analysis and distributed SSH Brute-force attacks. In Towards Extensible and Adaptable Methods in Computing (pp. 107-118). Springer, Singapore. https://doi.org/10.1007/978-981-13-2348-5_9

[8] Syukri, A.F., Okamoto, E., Mambo, M. (1998). A user identification system using signature written with mouse. In Australasian conference on information security and privacy (pp. 403-414). Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0053751

[9] Goldberg, J., Hagman, J., Sazawal, V. (2002). Doodling our way to better authentication. In CHI'02 extended Abstracts on Human Factors in Computing Systems, pp. 868-869. https://doi.org/10.1145/506443.506639

[10] Zhao, H., Li, X. (2007). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), pp. 467-472. https://doi.org/10.1109/AINAW.2007.317

[11] Tao, H. (2006). Pass-Go, a new graphical password scheme. Doctoral dissertation, University of Ottawa (Canada). http://dx.doi.org/10.20381/ruor-18637

[12] Tao, H., Adams, C. (2008). Pass-go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, 7(2): 273-292. https://doi.org/10.6633/IJNS.200809.7(2).18

[13] Zangooei, T., Mansoori, M., Welch, I. (2012). A hybrid recognition and recall based approach in graphical passwords. In Proceedings of the 24th Australian Computer-Human Interaction Conference, pp. 665-673. https://doi.org/10.1145/2414536.2414637

[14] Chiang, H.Y., Chiasson, S. (2013). Improving user authentication on mobile devices: A touchscreen graphical password. In Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, pp. 251-260. https://doi.org/10.1145/2493190.2493213

[15] Awang, M.I., Mohamed, M.A., Mohamed, R.R., Ahmad, A., Rawi, N.A. (2017). A pattern-based password authentication scheme for minimizing shoulder surfing attack. International Journal on Advanced Science, Engineering and Information Technology, 7(3): 1049-1055. https://doi.org/10.18517/ijaseit.7.3.1517

[16] Yao, B., Mu, Y., Sun, H., Zhang, X., Wang, H., Su, J. (2018). Connection between text-based passwords and topological graphic passwords. 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), pp. 1090-1096. https://doi.org/10.1109/ITOEC.2018.8740702

[17] Sinha, A., Shrivastava, G., Kumar, P. (2019). A pattern-based multi-factor authentication system. Scalable Computing: Practice and Experience, 20(1): 101-112. https://doi.org/10.12694/scpe.v20i1.1460

[18] Hemamalini, M., Saranya, R. (2019). Graphical password authentication using hybrid pin keypad. Malaya Journal of Matematik (MJM), S(1): 554-559. https://doi.org/10.26637/MJM0S01/0100

[19] Li, C., Lin, D., Feng, B., Lü, J. and Hao, F., (2018). Cryptanalysis of a chaotic image encryption algorithm

based on information entropy. IEEE Access, 6: 75834-75842. https://doi.org/10.1109/ACCESS.2018.2883690

[20] Ye, G., Pan, C., Huang, X., Zhao, Z., He, J. (2018). A chaotic image encryption algorithm based on information entropy. International Journal of Bifurcation and Chaos, 28(1): 1850010. https://doi.org/10.1142/S0218127418500104

[21] Hashim, A.T., Jalil, B.D. (2020). Color image encryption based on chaotic shit keying with lossless compression. International Journal of Electrical & Computer Engineering, 10(6). https://doi.org/10.11591/ijece.v10i6.pp5736-5748

[22] Lai, J., Arko, E. (2021). A shoulder-surfing resistant scheme embedded in traditional passwords. Proceedings of the 54th Hawaii International Conference on System Sciences, p. 7144. https://doi.org/10.24251/HICSS.2021.860

[23] Bošnjak, L., Sreš, J., Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1161-1166. https://doi.org/10.23919/MIPRO.2018.8400211

[24] Yang, W., Zheng, Z., Chen, G., Tang, Y., Wang, X. (2019). Security analysis of a distributed networked system under eavesdropping attacks. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(7): 1254-1258. https://doi.org/10.1109/TCSII.2019.2928558