*Dr. Barkha Bahl, **Ms.Harneet Kaur, ***Mr. Gagandeep Singh Matharu

PREVENTION OF SQL INJECTION ATTACKS USING COLOR PASSWORDS

*Dr. Barkha Bahl, Professor & HOD, DIAS, India
**Ms. Harneet Kaur, Indus Valley Partners, India
***Mr. Gagandeep Singh Matharu, Knownymous, India

ABSTRACT

The biggest challenge nowadays is to secure the website against cyber-attacks. Structured Query Language Injection Attack(SQLIA) is one of the most critical cyber-attack. As a result of SQLIA an attacker can have the access control on the database of an application and accordingly can make changes in the critical data stored on the database server of the website. Authentication plays an important role in securing critical data. Generally, alphanumeric passwords are most commonly used for authenticating users in computer systems but they are highly prone to cyber-attacks. However, graphical authentication systems have been proposed as a relevant and possible alternative solution to the traditionally used text-based (alphanumeric) authentication and the idea is motivated particularly by the fact that human brain has the ability to remember images better than text. Graphical passwords are mainly created by clicking or dragging activities on the pictures or certain parts of a picture rather than conventional typing of textual characters. The main objective of the paper is to highlight the various SQL injection attacks and SQL injection vulnerabilities on website databases, to study and analyse existing authentication systems and to propose a secure mechanism of authentication through colour code graphical passwords.

To enhance the security of colour passwords, an encryption algorithm has been proposed keeping in mind the vulnerabilities that existed in earlier techniques. The proposed encryption algorithm is called "Colour Matrix Map" algorithm. This algorithm provides a method to protect against SQLIA. The proposed algorithm has been tested for its efficiency and security by rigorous testing on various applications.

Keywords: *SQLIA - SQL Injection Attacks, User Authentication, Vulnerability, Graphical Passwords, Color code passwords, Web Security, Encryption, Color Matrix Map Algorithm, Website Databases.*

INTRODUCTION

Web applications have become one of the most important communication channels between service providers and clients but these web application databases are easy targets of sophisticated hackers. The increasing frequency and complexity of web based attacks has raised awareness among web application administrators of the need to effectively protect their web applications from such attacks (Gandhi et al., 2013). Every web application has an authentication mechanism. A system verifies the identity of the user during the authentication process. It is through this process that the user is allowed to either access a system or an application or an object running in a device.

In simple terms, authentication mainly provides security to the system by allowing only the authenticated user to use the system. Also, adequate authentication provided initially while logging into the system, protects the system from the malicious users. Various user authentication mechanisms are prevalent these days; however, most out of them are vulnerable to SQLIA in some form or the other. The SQL Injection Attacks and their concepts are discussed in detail in section 1.1.

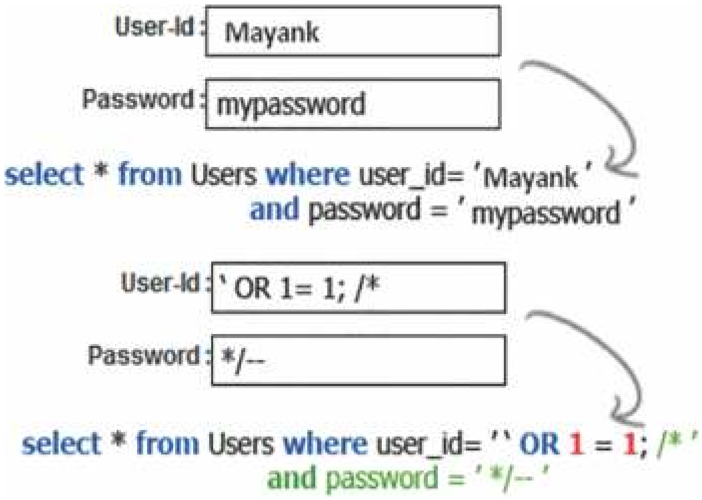
1. Sql Injection Attacks

SQL injection is a technique where malicious users can inject SQL commands into SQL statements intentionally of web page inputs. Injected SQL commands via user inputs can make changes in the SQL statement and hence compromise the security of any vulnerable web application by giving unauthorized access to website databases. SQL injection must exploit some security vulnerability in the application software, for example, if user input is either incorrectly filtered or string literal escape characters are deliberately embedded in SQL statements or user input is not strongly typed and that input gets unexpectedly executed.A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.SQL injection is most commonly known as an attack vector for websites' databases but it can easily be used to attack any type of SQL database systems(Gandhi et al., 2013).

Key Concepts Of Sql Injection

SQL injection is a type of software vulnerability that generally occurs when data entered by users are sent to the SQL interpreter as a part of a SQL query. For example, by entering an expression such as 'or 1=1' appended to the input string of username will always execute to value 'true' and hence in most cases will trigger the backend operation of the databases and user will be able to bypass the authentication without entering a valid user id and password as shown in fig. 1.

Attackers deliberately provide specially crafted, malicious input data to the SQL interpreter and exploit the interpreter to execute malicious commands in such a way that the interpreter is not able to differentiate between the actual commands and the attacker's specially crafted data. The interpreter then executes the SQL injection and exploits the security vulnerabilities at the database layer of a system (Gandhi et al., 2013).



User-Id : Mayank

Password : mypassword

```
select * from Users where user_id= 'Mayank '
                 and password = ' mypassword '
```

User-Id : ' OR 1= 1; /*

Password : */--

```
select * from Users where user_id= '' OR 1 = 1; /* '
                 and password = ' */-- '
```

Fig. 1 Example of SQL injection using query string

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. By exploiting the system's vulnerability, attackers can bypass authentication and then create, read, modify, or delete sensitive data. These types of attacks were found easier to trigger for systems which use textual passwords. Hence to overcome this, Graphical passwords were proposed as one of the solution for preventing the SQLIA. The brief idea about graphical passwords is given under section 2.

2. GRAPHICAL PASSWORDS

A graphical password is an authentication system that works by allowing the user to select from a given set of images, patterns, etc. in some specific order, present in front of the user in a graphical user interface (GUI). For this reason, this approach is sometimes also called as graphical user authentication (GUA). A graphical password is easier to remember for most of the people than a text-based password. Graphical passwords may provide better security when compared to text-based passwords because many people, in order to easily memorize text-based passwords, use easy, plain words (rather than the recommended jumbled up combination of characters) which is always easier to interpret (Fulkar et al. 2012).

3. LITERATURE REVIEW

There exist various techniques under SQLIA which can be used to get unauthorized access to any database system.An attacker can get access to confidential information available on the website's database server and can exploit the database. This is generally caused due to vulnerability of SQL in Relational Database Management System which results from

Table 1: Various SQLIA, Their Impacts and Risk

S.NO.	SQLIA	IMPACT	IMPACT OF ATTACK ON WEB APPLICATIONS
1.	Generate errors to display database table fields.	Enumeration of backend database table fields which assist in building further attacks	Medium Risk
2.	Login without authentication.	By pass authentication, unauthorized access to the application.	High Risk
3.	Bypass authentication.	Unauthorized access.	High Risk
4.	Bypass authentication using numeric input fields.	Bypass authentication, unauthorized access.	High Risk
5.	Create users on the database machine using stored procedure insertion description.	Unauthorized execution of arbitrary commands	Medium Risk
6.	Second-order SQL Injection.	Changing of the administrator password.	High Risk
7.	Insertion when input data length is fixed.	Execution of user specified commands.	Medium Risk.
8.	Evade logging in SQL.	Bypassing logging mechanism resulting to undetected SQLIA.	Medium Risk
9.	Insert injection.	Retrieval of unauthorized data from the database.	Medium Risk

inappropriate programming practices (Singh et al., 2012). The various types of SQL Injection Attacks are discussed in section 3.1.

SQLIA Approaches & Their Impacts on Web Applications (Singh et al., 2012):

A SQLIA takes place when an attacker endeavours to change the logic, semantic or syntax of a legitimate SQL statement. This is done by inserting new SQL keyword or operators into the SQL query through a web application interface that are accomplished in a back-end database of a web application. An application is said to have SQLIVs (SQL Injection Vulnerabilities), when SQL queries are generated by using some implementation language (e.g., Java Server Pages or JSP) and the incorrect inputs supplied by the user become part of the query generation process without proper validation checks of the input data. These vulnerabilities can be exploited through SQLIAs, which might cause unexpected results of authentication by-passing which can give any malicious user the unauthorized access and information leakage where sensitive information may be misused(Singh et al., 2012) .

Various different SQLIA along with their impacts and degree of risk on web applications has been summarized in the following table(Orso et al., 2006):

The above discussed advanced SQLIAs are few identified attacks which need to be prevented from all web based databases. One

such prevention measure being suggested is to implement graphical passwords for user authentication. There are majorly two classified password techniques, one is recall-based and the other is recognition-based. The legacy textual passwords are mainly recall-based techniques where the user has to remember the alphanumeric password string. Recognition-based techniques were later on proposed as a better alternative(Tajpour et al.,2010). Majorly, all graphical password techniques are recognition based where the user has to recognise the password from a given set of images. Under this study, it was found that graphical passwords can play an important role in minimizing the vulnerability of databases. Few of these techniques are discussed in section 3.2.

Graphical Password techniques

A graphical password is a technique that requires users to select a predetermined image or set of images on the visual display presented in a Graphical User Interface. A user is authenticated if the user enters some images only in a particular sequence. This feature is based on easy recognition of pictures by humans and can be effectively used for authentication. Users can select elements appearing on a screen as part of their graphical password (Kimwele et al., 2010).

Various different graphical authentication password techniques are available. They are discussed under section 3.3. Various weaknesses were observed in the stated techniques and hence to overcome those weaknesses, a new technique of COLOUR MATRIX MAP has been proposed.

Types of Graphical Passwords

Various techniques were well studied and analysed as below:

Déjà vu Authentication Technique

Déjà vu Authentication Technique is a recognition based authentication technique(Sonkar et al. 2012), which authenticates a user through their ability to recognize images that were previously shown to them. Deja Vu is based on the observation that humans have an excellent memory for images. Using Deja Vu, users first create an image portfolio for themselves, by selecting a subset of images out of a given set of sample images. Then to authenticate the user, the system presents a challenge set, consisting of 'n' images. This challenge contains 'm' images of the portfolio and the remaining 'n-m' images are decoy images. To get authenticated, the user must correctly identify the images which are part of the portfolio. Deja Vu technique is carried out in three phases: portfolio creation, training, and authentication. A trusted server stores all portfolio images of each user. Since each image is derived directly from the seed, the server only needs to store the seed and not the entire image.

The weakness observed in this system was that there is a considerable server memory overhead since it has to store different set of images for each user, also a larger image set may not be easy to remember for the user. Memory overhead is a major concern and it was much needed to be handled efficiently.

Colour Image Gallery

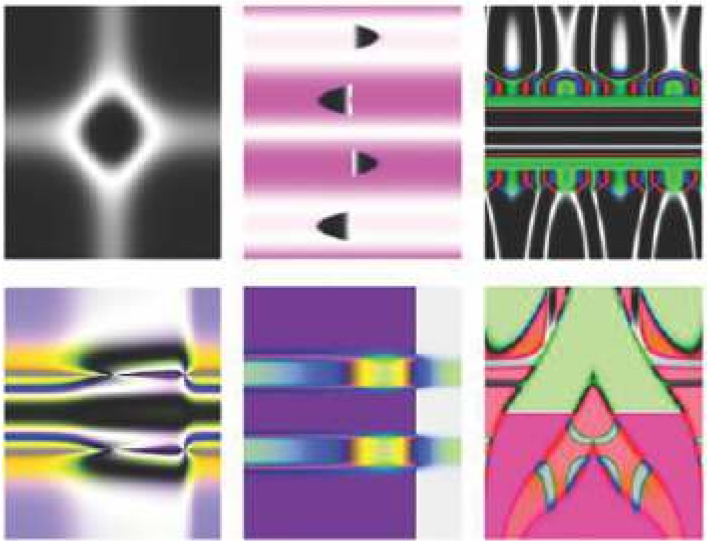


Fig 2: Sample set of image portfolio

Another recognition-based technique under study was Color Image Gallery. This technique is previously prevalent among web systems. In this technique, the user is required to select random image colour blocks at the time of registration/sign-up(Sonkar et al. 2012). It means suppose that user has selected first colour image block as Red, Second colour image block as Black and Third colour image block as Yellow. This sequence on colour blocks selected by the user gets stored in the database as that user's password and the user then must remember it to login each time into the system. But certain shortcomings were noticed in this system as this system stores the exact color images, it is still vulnerable to SQLIA to some extent that if this database gets hacked, the colour passwords can still be retrieved. This system lacks encryption of passwords.

Pass doodle

Pass doodle (Fulkar et al. 2012)is a recall-based technique. It is a technique that has handwritten drawing or text, which is normally sketched with a stylus over a touch sensitive screen as shown in Fig. 3 below. It shows that users can easily recognize a complete doodle password as accurately as they would have recognised any of the text-based passwords. After in-depth study of this technique it was found that this mechanism has certain weaknesses in a way that it is vulnerable to attacks such as key-logger, shoulder surfing, guessing, spyware, etc. and can also be a little difficult to reproduce the exact drawing/sketch each time.

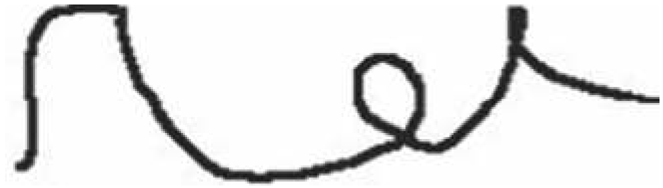


Fig 3: Example of Pass doodle

Picture Password

This technique of picture passwords(Jansen et al., 2003) was designed especially for handheld mobile devices such as PDAs, etc. In this technique the user is first asked to select the theme (e.g. sea shore, cat and dog, etc.) which consists of a set of small thumbnail photos. Then the user selects and registers a sequence of the selected thumbnail photos to form the password. The user needs to recognize and identify the previously seen photos and either click it or touch on it in the correct sequence using a stylus in order to be authenticated.

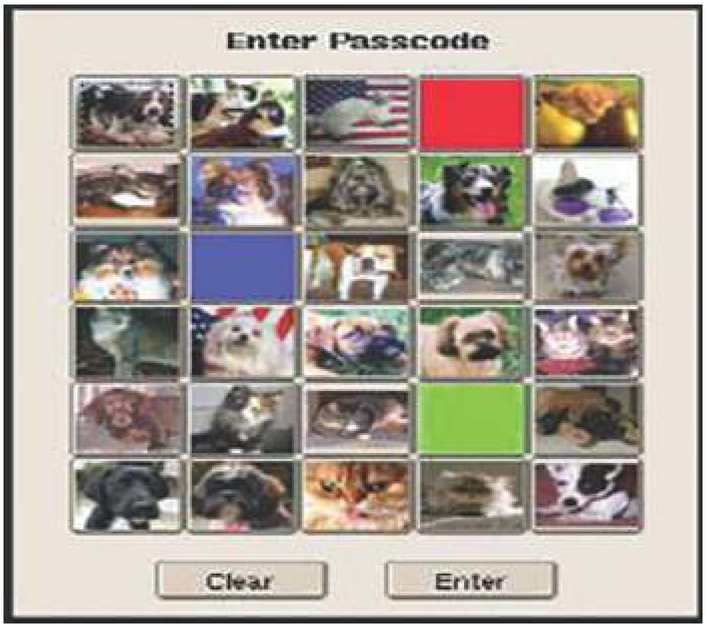


Fig 4. Cats and dog theme for picture password scheme

The major drawback of this scheme is, as the number of thumbnail photos in this technique is limited only to 30, the number of possible password combinations is considerably small. A numerical value is assigned for each thumbnail photo and the sequence of selection of these thumbnails will produce a numerical password. This numerical password is generally shorter than the length of textual password. To overcome this problem a user can select more than one thumbnail photo as one single combined action or as one composite password in order to create and increase the size of the password length. However, this makes it a complex password which becomes difficult to remember for the human brain and also there is some extra memory overhead as it needs to store thumbnails based on various different themes.

Passfaces

An interesting technique that used human face images as passwords had been previously existing is named as Passfaces. Based on the assumption that humans can recall human faces easier than other pictures, Real User Corporation has developed their own commercial product named Passfaces TM (Fulkar et al. 2012). Basically, Passfaces works as follows:

Users are required to select the previously seen human face from a grid of nine faces one of which is known while the rest are just decoys. This step is continuously repeated until all the four faces are successfully identified.

Fig. 5 – Passfaces TM

A comparative study was carried out by Real User Corporation as proof of concept in which 34 people were involved in the test and it was shown that, it was easier to remember Passfaces password as compared to textual passwords for human beings. But the results also showed that Passfaces took a much longer login time in most cases than textual passwords (Sonkar et al., 2012).

Passlogix

Passlogix Inc. is a commercial security company located in New York City, USA. The scheme proposed by them is called Passlogix v-Go (Fulkar et al. 2012) which uses a technique known as “Repeating a sequence of actions” which means creating a password by a sequence. In this scheme, users can select background images of their choice based on the environment or scenarios, for example image of the kitchen, bathroom, bedroom, etc. then to enter a password, user can click and/or drag on a series of items within that image. For example in the kitchen scene, user can prepare a meal by selection of certain cooking ingredients, then the click action of taking out food from refrigerator and putting it in the microwave oven, selection of some fruits and washing them in washbasin and then putting it in a clean bowl. The sequence of these actions together may form a person's password.

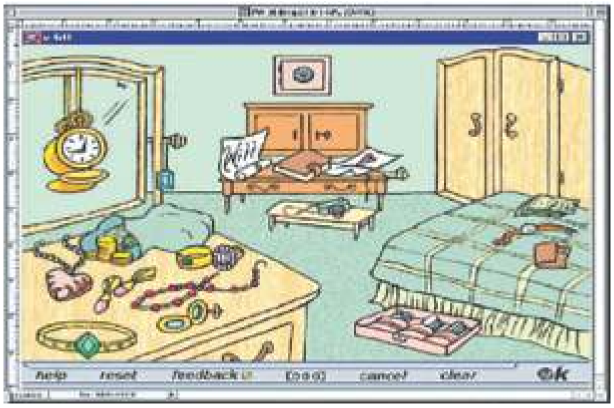


Fig. 6 - Passlogix scheme

This technique of Passlogix authentication system is easy to remember for the user since it is very logical. But, on the other hand, there are some disadvantages of this scheme i.e. the number of possible passwords are small. There are limited places that one can take vegetables, fruits or food from and put into, therefore, these results in making the passwords to be somewhat guessable or predictable.

Pass-Go

Last but not the least, another technique taken under study wasPass-Go(TAO, 2006) that can be considered as an improvement of DAS (draw – a – secret technique, as it keeps most of the advantages of DAS and provides stronger security and better usability. These improvements are believed to arise from the innovative design.

A simple teaching management system was developed on an Internet website, through which students could access their grades and study materials by logging in with Pass-Go

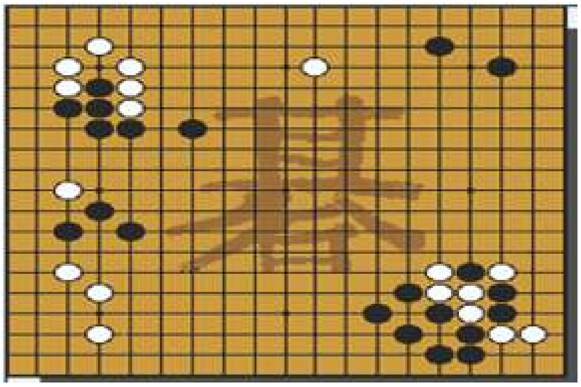


Fig. 7 Pass-Go

passwords. This was a system where Pass-Go technique was applied and tested previously. Major concern with this type of graphical passwords is that the registration process and log-in process which take longer time than in text-based passwords. During the registration process, the user picks image portions of different colours from a set of selections to make a colour graphical password. During authentication, the user has to identify the images and this process can be tedious and take long. The need for higher security can override the long and tedious process of registration in graphical passwords. Graphical passwords because of their sizes require more space than text based passwords. The pictures also have to be maintained in a centralized database which implies that network transfer is an area of concern for graphical passwords. However, with the high computer storage space and increased bandwidths, this concern about graphical passwords is no longer a serious issue (Kimwele et al., 2010).

After studying the above discussed techniques, identifying their weaknesses and in order to make further developments on Graphical Passwords, a new authentication technique called Colour Matrix Map to provide a better mechanism of protecting web application databases from the severity of SQL Injection Attacks has been proposed.

The problem of memory overhead identified in Déjà vu technique (Sonkar et al., 2012) has been overcome in the proposed system of COLOUR MATRIX MAP, which uses considerably less space to store the user passwords as it stores a commonly shared grid structure for all users. The Colour Image Gallery (Sonkar et al., 2012) technique lacked the encryption of password. This shortcoming has been overcome in the COLOR MATRIX MAP algorithm as the proposed algorithm comes with an encryption technique. The proposed technique also caters to the problem that was faced in Pass-doodle technique of authentication. Pass-doodle was prone to certain attacks like key-logger, shoulder surfing, guessing, spyware, etc.(Fulkar et al. 2012). The proposed COLOUR MATRIX MAP algorithm can prove to be a better alternative technique than techniques like Pass-faces and Passlogix since it makes the login process much faster when compared to other techniques.

The following table highlights and summarizes the weaknesses of each of the previously proposed techniques and how this new proposed system "Colour password technique and its security through Colour Matrix Map" provides counter measures for each of the weaknesses:

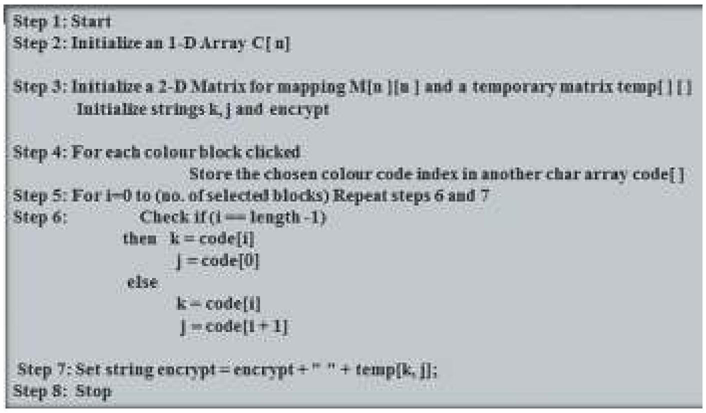
Table 2: Weaknesses of previously proposed techniques and their counter measures in the proposed scheme

S.NO.	Previously Proposed Technique	Weaknesses	Counter measures by the proposed Technique
1.	Prevention of SQLIA through Hashing Techniques	-Uses textual passwords only -Vulnerable to various different attacks like dictionary attacks, key logs, spyware, etc. -Hash functions are difficult to implement	Colour password proposed Easy to remember Safeguards from dictionary attacks , brute force, SQLIA Easy to implement algorithm
2.	Authentication using Images - Déjà vu technique (Sonkar et al., 2012)	-Uses image portfolios -Server memory overhead as it has to store different set of images for each user -Not easy to remember	Uses same colour set for each user Minimum memory requirements
3.	Graphical password authentication scheme based on colour image gallery	-Can be still vulnerable to SQLIA -Database can be hacked and colour passwords can be retrieved	Encryption of colour passwords.
4.	Pass-doodle (Fulkar et al. 2012)	-Vulnerable to attacks such as key-logger, shoulder surfing, guessing, spyware, etc. -Difficult to remember	Easy to remember -Safeguards from key-logger attacks
5.	"Picture password"- Passcode (TAO, 2006)	-thumbnail photos are limited only to 30 -thumbnails converted to numerical passwords, shorter in length -memory overhead as it needs to store thumbnails based on themes. - it often becomes difficult to memorize the complex password.	Colour block set can be increased as required No conversion into numerical
6.	PassFace Technique(Fulkar et al. 2012)	Takes much longer login time	No extra login time
7.	PassLogix V	Easy to guess logical sequence of events size of password space is small	No easy guessing
8.	PassGo (TAO, 2006)	Difficult to implement Pixel calculations involved	Easy implementation

Proposed Authentication Technique – COLOR MATRIX MAP:

A new password technique of Colour Codes along with its encryption algorithm has been proposed. When the user selects the colour password while registering to any web application, the colour password gets encrypted using colour matrix map algorithm and gets stored in the database. The encryption algorithm that has been designed is simple to implement yet difficult to break using attacks like eavesdropping, dictionary attacks, social engineering, etc. The proposed encryption algorithm is called "Colour Matrix Map" algorithm. The user must remember the colour code in order to login into the system. The introduced system has been tested for its efficiency and security by rigorous testing on various applications. The proposed algorithm is given in section 4.1 followed by its flowchart and algorithm design.

4. Proposed Algorithm:



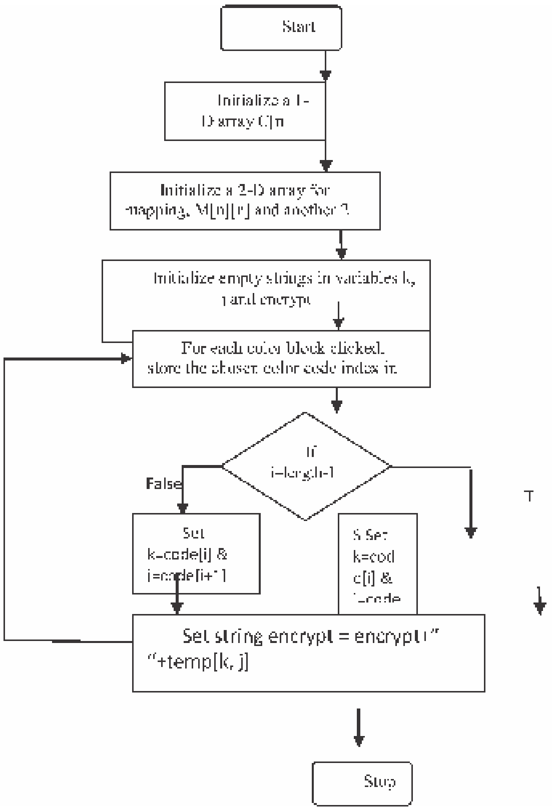
```
Step 1: Start
Step 2: Initialize an 1-D Array C[ n]

Step 3: Initialize a 2-D Matrix for mapping M[n ][n ] and a temporary matrix temp[ ] [ ]
        Initialize strings k, j and encrypt

Step 4: For each colour block clicked
                    Store the chosen colour code index in another char array code[ ]
Step 5: For i=0 to (no. of selected blocks) Repeat steps 6 and 7
Step 6:          Check if (i == length -1)
              then   k = code[i]
                     j = code[0]
              else
                     k = code[i]
                     j = code[i + 1]

 Step 7: Set string encrypt = encrypt + " " + temp[k, j];
Step 8:  Stop
```

Flowchart 1. Algorithm:


Start
Initialize a 1-D array C[]n
Initialize a 2-D array for mapping, M[n][n] and another 2
Initialize empty strings in variables k, j and encrypt
For each color block clicked, store the chosen color code index in
If i=length-1
False
T
Set k=code[i] & j=code[i+1]
S Set k=code[i] & j=code
Set string encrypt = encrypt+" "+temp[k, j]
Stop

Algorithm Design:

The algorithm proposed is an easy-to-implement algorithm. The algorithm aims at encrypting the colour code chosen by the user at the time of registration. The process of choosing the colour password in the system is that at the time of registration the user has to enter the User ID and for the password, there is a set of colour blocks provided to the user. For example: the colour blocks are provided to the user in the following sequence as shown in Fig. 8, the colours are stored in a 1-Dimensional array named C in the algorithm, with the array indices as inscribed on them.

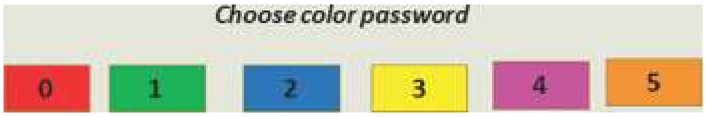
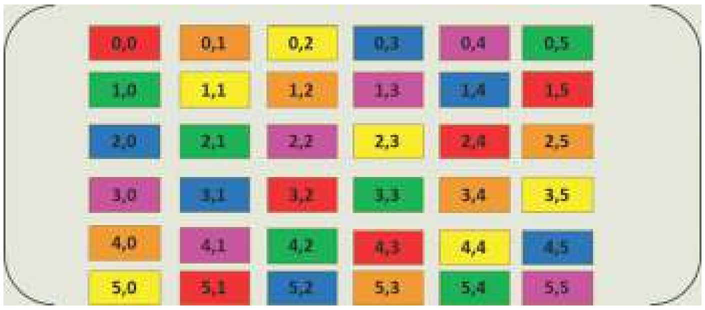


Fig. 8 Array C

The user has to choose randomly the colour blocks in any sequence. The user has to remember the entered colour password. The colour blocks selected are stored as string of colour names in the database. The encryption algorithm is applied at the server code. For simplicity of explanation, six different colour blocks have been considered at present. The number can be increased as per the requirement. At the backend, a 2-Dimensional COLOUR MATRIXof 6*6 colour blocks named M has been created as shown in Fig. 9.



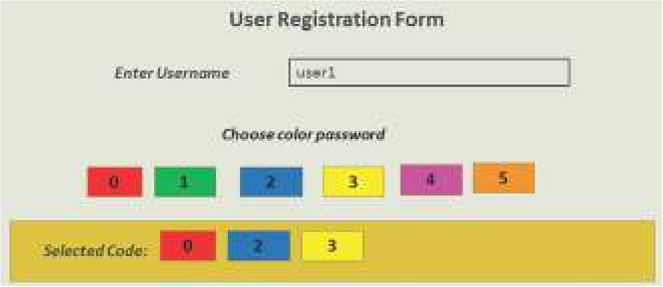
0,0	0,1	0,2	0,3	0,4	0,5
1,0	1,1	1,2	1,3	1,4	1,5
2,0	2,1	2,2	2,3	2,4	2,5
3,0	3,1	3,2	3,3	3,4	3,5
4,0	4,1	4,2	4,3	4,4	4,5
5,0	5,1	5,2	5,3	5,4	5,5

Fig. 9 COLOUR MATRIX M[ ] [ ]

The colours in the matrix are so arranged that each colour appears once in each row and once in each column. Each colour block shows the index value (i, j) of that array element inscribed on the block. This algorithm manipulates the above 2D matrix to encrypt the colours chosen.

Working of the Algorithm: The detailed working of the above mentioned algorithm is explained below:

Considering the sample registration form of a web application below in Fig. 10



User Registration Form

Enter Username: user1

Choose color password

0 1 2 3 4 5

Selected Code: 0 2 3

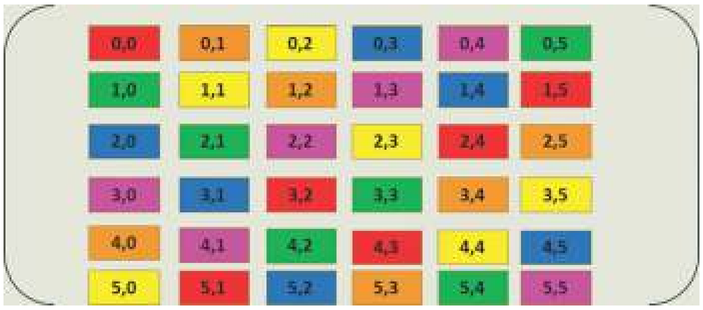
Fig. 10. Sample User Registration Form from Sample Web- Application

Considering the above example, suppose the user has selected the 1st colour as Red which is at the array index 0, 2nd colour as Blue with array index 2 and then the user selects the 3rd colour to be Yellow with the array index 3.

Now the colours selected are first translated into an array of characters named C[ ] which represent the index of each of the selected colour block i.e "023", C=[023] in this example.

Applying Encryption:

To apply encryption, 6*6 colour matrix M[ ][ ] has been considered,

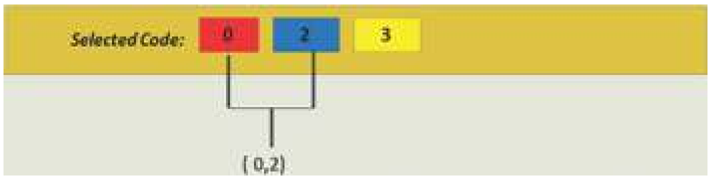


🟥 0,0	🟧 0,1	🟨 0,2	🟦 0,3	🟪 0,4	🟩 0,5
🟩 1,0	🟨 1,1	🟧 1,2	🟪 1,3	🟦 1,4	🟥 1,5
🟦 2,0	🟩 2,1	🟪 2,2	🟨 2,3	🟥 2,4	🟧 2,5
🟪 3,0	🟦 3,1	🟥 3,2	🟩 3,3	🟧 3,4	🟨 3,5
🟧 4,0	🟪 4,1	🟩 4,2	🟥 4,3	🟨 4,4	🟦 4,5
🟨 5,0	🟥 5,1	🟦 5,2	🟧 5,3	🟩 5,4	🟪 5,5

Fig. 11 Color Matrix M[] []

STEP 1:

To encrypt the first colour block, we have used the index value of first and the second colour as in the 1D array C shown in Fig. 12.

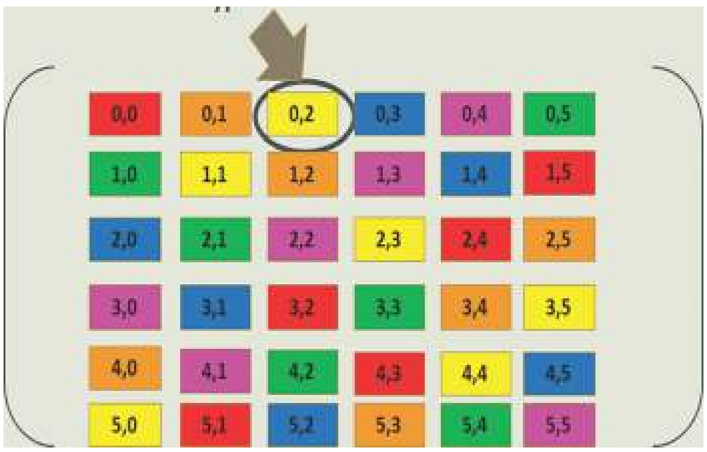


Selected Code: 0 2 3

(0,2)

Fig. 12 Encryption Step 1

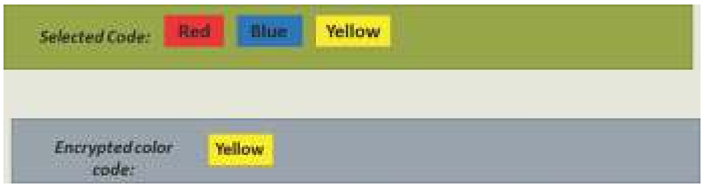
The first colour block index in array C forms the i, and the second colour code index in array C forms j. This (i, j) is then mapped to the (i, j) Th element in the 6*6 matrix M.



🟥 0,0	🟧 0,1	🟨 0,2	🟦 0,3	🟪 0,4	🟩 0,5
🟩 1,0	🟨 1,1	🟧 1,2	🟪 1,3	🟦 1,4	🟥 1,5
🟦 2,0	🟩 2,1	🟪 2,2	🟨 2,3	🟥 2,4	🟧 2,5
🟪 3,0	🟦 3,1	🟥 3,2	🟩 3,3	🟧 3,4	🟨 3,5
🟧 4,0	🟪 4,1	🟩 4,2	🟥 4,3	🟨 4,4	🟦 4,5
🟨 5,0	🟥 5,1	🟦 5,2	🟧 5,3	🟩 5,4	🟪 5,5

Fig. 13 Encryption mapping in Step1

Encrypted colour pattern at the end of step1 is shown in Fig. 14.



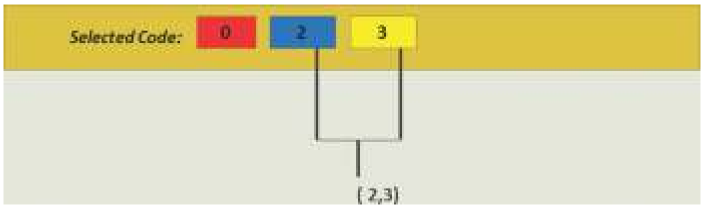
Selected Code: Red Blue Yellow

Encrypted color code: Yellow

Fig. 14 Pattern at the end of step1

STEP 2:

To encrypt the second colour block, we have used the index value of second and the third colour as in the 1-D array C shown in Fig. 15.

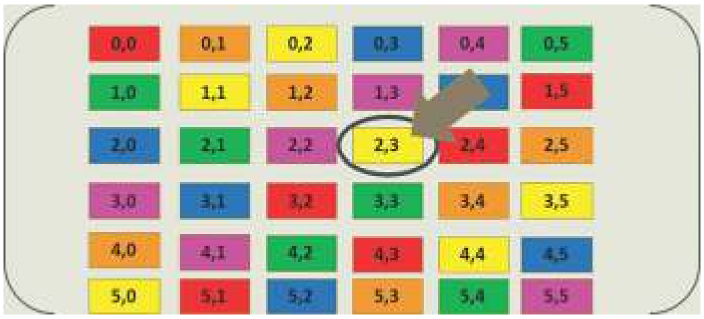


Selected Code: 0 2 3

(2,3)

Fig. 15 Encryption Step 2

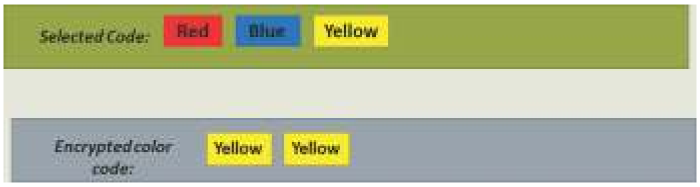
The second colour block index in array C forms the i, and the third colour code index in array C forms j. This (i,j) is then mapped to the (i,j)th element in the 6*6 matrix M.



🟥 0,0	🟧 0,1	🟨 0,2	🟦 0,3	🟪 0,4	🟩 0,5
🟩 1,0	🟨 1,1	🟧 1,2	🟪 1,3	🟦	🟥 1,5
🟦 2,0	🟩 2,1	🟪 2,2	🟨 2,3	🟥 2,4	🟧 2,5
🟪 3,0	🟦 3,1	🟥 3,2	🟩 3,3	🟧 3,4	🟨 3,5
🟧 4,0	🟪 4,1	🟩 4,2	🟥 4,3	🟨 4,4	🟦 4,5
🟨 5,0	🟥 5,1	🟦 5,2	🟧 5,3	🟩 5,4	🟪 5,5

Fig. 16 Encryption mapping in Step2

Encrypted colour pattern at the end of step 2:



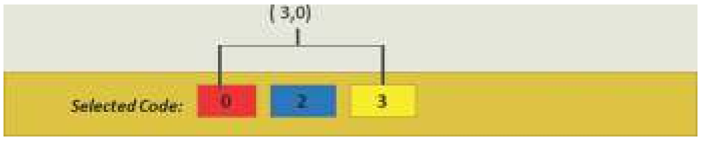
Selected Code: Red Blue Yellow

Encrypted color code: Yellow Yellow

Fig. 17 Pattern at the end of step 2

STEP 3:

To encrypt the third colour block, we have used the index value of third and the first colour as in the 1-D array C shown in Fig. 18:

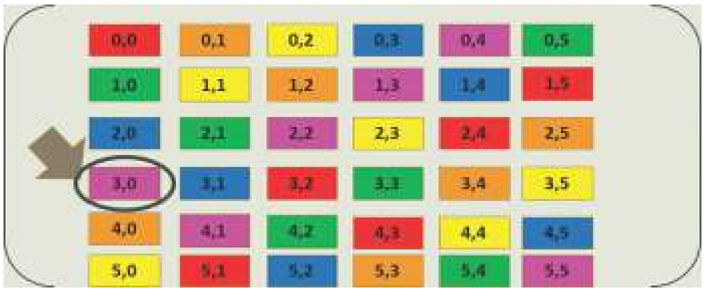


(3,0)

Selected Code: 0 2 3

Fig. 18 Encryption Step 3

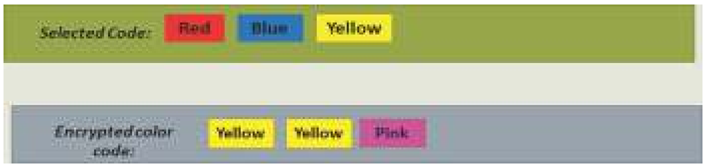
The third colour block index in array C forms the i, and the first colour code index in array C forms j. This (i,j) is then mapped to the (i,j)th element in the 6*6 matrix M.



0,0	0,1	0,2	0,3	0,4	0,5
1,0	1,1	1,2	1,3	1,4	1,5
2,0	2,1	2,2	2,3	2,4	2,5
3,0	3,1	3,2	3,3	3,4	3,5
4,0	4,1	4,2	4,3	4,4	4,5
5,0	5,1	5,2	5,3	5,4	5,5

Fig. 19 Encryption mapping in Step 3

Encrypted colour pattern at the end of step 3 is shown in Fig. 20.:



Selected Code: Red Blue Yellow

Encrypted color code: Yellow Yellow Pink

Fig. 20 Pattern at the end of Step 3

Hence, after encryption the colour password that goes into the database is:

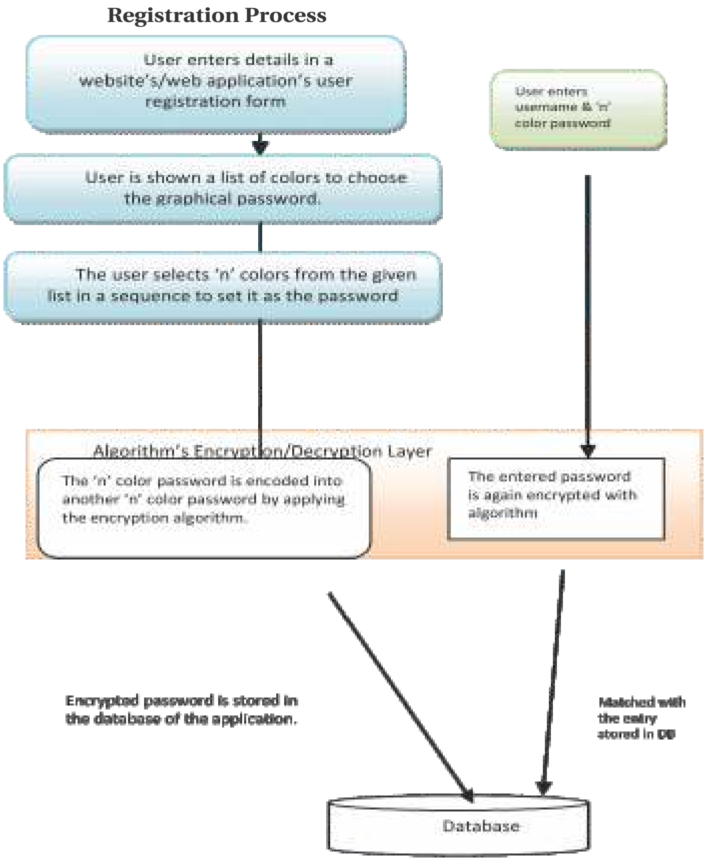
YELLOW YELLOW PINK

Note: The number of steps for the algorithm depends on the number of colour blocks chosen by the user. And the number of encrypted colours will be same as the number of chosen colours.

It is advisable to choose maximum number of colour blocks (in this example it is 6) for creating a secured password

Application of Algorithm:

The algorithm of COLOR MATRIX MAP technique when applied to any application can be better understood through the following flow chart for web application:


Registration Process
User enters details in a website's/web application's user registration form
User is shown a list of colors to choose the graphical password.
The user selects 'n' colors from the given list in a sequence to set it as the password
User enters username & 'n' color password
Algorithm's Encryption/Decryption Layer
The 'n' color password is encoded into another 'n' color password by applying the encryption algorithm.
The entered password is again encrypted with algorithm
Encrypted password is stored in the database of the application.
Matched with the entry stored in DB
Database

Flow-chart II: Web Application

The above flow-chart explains the simple application of the algorithm and the interaction with the database through the encryption layer.

The process explains the flow right from the time when the user registers for the first time with the web application and when the user comes back to login into the system each time.

The application of the proposed algorithm has been shown with relational database for simplicity but this can be efficiently applied on other types of databases such as object oriented databases, etc. as well.

TESTING METHODOLOGY

The proposed algorithm was implemented and tested on a simple web application, which was created on .NET platform that supported 50-100 users. While testing, the algorithm was applied using six color combinations in the selection grid of COLOR MATRIX. Around thirty five dummy user accounts were created for the application and the user details where stored in the underlying database that was SQL server. The application's login screen provided the option to enter the color password. The sample application was rigorously tested by hitting various SQL Injection queries through the Login screen. But it was seen that due to the absence of textbox to enter string based literals as password the SQL Injection attacks were unsuccessful on the application. To test it to the next level, the application's database was then exposed to a tester. Getting access to the database which contained the encrypted passwords, the tester was unable to decrypt the color coded passwords into actual user passwords. Hence this very easily proved that the COLOR MATRIX MAP algorithm was a secure graphical password technique that can replace legacy string based passwords.

CONCLUSION:

After the in-depth analysis of various SQLIA and existing graphical password techniques, the identified weaknesses have been overcome in the proposed technique of colour passwords along with its secure encryption mechanism.

The proposed system has the advantage that even if somehow the hacker gets access to the database entries. The hacker can see the colour passwords in their encrypted forms and the hacker might get fooled by this trick and try the retrieved combination, but his attempts would fail. It is observed that this type of graphical password is easy to memorize. Since colour passwords do not require providing text fields to enter passwords, the chances of SQLIA and the loop holes get eliminated to great extent. This encryption algorithm provided counter measures to weaknesses of previous techniques like avoiding memory overheads, increased number of possible combinations of passwords, etc. The "Colour Matrix Map" is simple to understand and implement hence even a beginner programmer can implement the algorithm code.

Analysis of the Proposed algorithm

The strength of the proposed algorithm lies in the fact that it can easily withstand various common attacks like dictionary attacks, brute force attacks, key logger attacks, etc.

The following calculations to analyse the proposed scheme were done: Since we have taken only 6 colour options for creating the password, and we have applied the restriction that the user can at most choose 6 colours. Colours can be repeated. User can choose single colour password, 2 colour passwords, and 3 colour passwords and so on till 6 colour passwords. So it has been analysed that the total number of passwords options can be:

(6^6)+(6^5)+(6^4)+(6^3)+(6^2)+(6^1) = 55986

So, we can conclude that it is difficult to apply brute force attacks, guessing attacks as the hacker will need to try 55986 combinations of colour passwords which are not easy to do.

Hence, we can say that this algorithm is quite efficient and could not be broken easily.

FUTURE SCOPE

The efficiency of the proposed system has been well analysed and tested on a dummy web application with few hundred users and this algorithm is found to work very well for small and medium sized web applications since these kind of web applications have around few hundreds to few thousands of users. The database retrievals are efficient for such small scale applications. Future work can be done in this area for using advanced colour schemes for generating colour codes. These techniques canbe applied to large sized web applications with millions of users like mailing services, social network sites, etc. For that purpose, bigger colour pellets can be used to give a bigger range of choice. This will result in increasing the matrix dimensions as well. But this can provide further enhanced security features.

REFERENCES

Dhameja Rachna, Perrig Adrian " Deja Vu: A User Study Using Images for Authentication " https://sparrow.ece.cmu.edu/group/pub/old pubs/usenix.pdf

Eljetlawi A. M., & Ithnin N.,"Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods", 2008, pp.1137-1143

Eljetlawi A. M., Ithnin N., "Graphical Password: Prototype Usability Survey", International Conference on Advanced Computer Theory and Engineering (ICACTE) 2008, pp. 351-355

Fulkar Ashwini , Sawla Suchita, Khan Zubin and Solanki Sarang, "A study of graphical passwords and various graphical password authentication schemes", *World Research Journal of Human Computer Interaction Vol. 1,2012, pp.04-08*

Gandhi Mihir Gandhi, Baria Jwalant, "SQL INJECTION Attacks in Web Application", *International Journal of Soft Computing and Engineering,* Vol. 2, Issue 6, 2013, pp.189.

Haichang G., Xuewu G., Xiaoping C., Liming W. & Xiyang L.,Yagp: , "Yet Another Graphical Password Strategy", Annual Computer Security Applications Conference, 2008, pp. 988-999.

Jansen, Gavrila W., Korolev S., Ayers V., Swanstrom R., "Picture Password: A Visual Login Technique for Mobile Devices", NISTt NISTIR 7030, 2003, pp. 1 – 16.

Kimwele Michael Kimwele, Mwangi Waweru, Kimani Stephen, "Strengths of aColored Graphical Password Scheme", *International Journal of Reviews in Computing,* 2010 IJRIC&LLS, pp.66-67.

LIN P. L. , WENG L. T., & HUANG P. W.,"Graphical Passwords Using Images with Random Tracks of Geometric Shapes", *Congress on Image and Signal Processing (CISP),* 2008, pp.27-31.

Mcdonald Stuart, "SQL Injection: Modes of Attack, Defence, and Why It Matters", *SANS Institute, Global Information Assurance Certification Paper Directory,* 2002, pp. 1-32.

Morgan D., "Web application security - SQL injection attacks," *Network Security,* vol. 2, April 2006, pp. 4-5.

Singh Nanhay, Singh Khushal, Raw Shringar Ram, "Analysis of Detection and Prevention of Various SQL Injection Attacks on Web Applications", International Journal of Applied Information Systems 2(7):20-26, Foundation of Computer Science, New York, USA, May 2012, pp.22-25

Sonkar S. K., Paikrao R. L. , Kumar Awadesh, "Graphical Password Authentication Scheme Based on Color Image Gallery", *International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4,* October 2012. pp. 13-16.

Tajpour A., Masrom M., Heydari M. Z., Ibrahim S., "SQL injection detection and prevention tools assessment" *Proc. of ICCSIT,* vol.9, no.,2010, pp.518-522, 9-11.

Tao Hai,"Pass-Go, a New Graphical Password Scheme", *Master Thesis,* University of Ottawa Canada, June 2006, pp.3-38.

Thomas Stephen , Williams Laurie, Xie Tao, "On automated prepared statement generation to remove SQL Injection vulnerabilities ", *Information and Software Technology 51,* 2009, pp. 590.

Wei Ke, Muthuprasanna M., Kothari S., "Eliminating SQL Injection Attacks in Stored Procedures", *IEEE ASWEC,* 2006, pp. 191-198.

William G.J., Halfond, Viegas Jeremy , Orso Alessandro, "A Classification of SQL Injection Attacks and Countermeasures", *Proceedings of International Symposium on Secure Software Engineering (ISSSE),* 2006, pp.1-10.

YAMPOLSKIY, R. V., "User Authentication via Behaviour Based Passwords", *IEEE Long Island Systems, Applications and Technology Conference (LISAT),* 2007., pp. 195-204.