# One-Time Graphical Cube Authentication

Inventors: Simon Tansey
Applicant: Gridy Technology Ltd
Patent Filing No. GB2411070.2

## ABSTRACT

One-Time Graphical Cube Authentication is a security method that utilises a graphical cube interface enabling a user to authenticate themselves by creating and inputting a unique pattern onto one of six coloured grid-based cube faces.

## BACKGROUND

This invention relates generally to Authentication & specifically to a One-Time Graphical Cube Authentication method.

The present invention introduces a one-time cube authentication method that includes, receiving a request to authenticate from a user. The authentication request includes the user Id. The method includes verifying the user id. The method includes generating a request for a one-time graphical cube authentication challenge from the authentication service, receiving from the authentication service a one-time graphical cube authentication challenge. The method also includes securely transmitting the one-time graphical cube authentication challenge to the user and drawing each of graphical authentication challenge cube's six coloured cube faces onto the user's display screen. The method includes prompting the user to select one of the six coloured cube faces using the cube face selector and inputting their unique pattern by selecting cells in a specific sequence onto the selected cube face. The method includes receiving the inputted pattern from the user and determining whether the inputted pattern matches the one-time graphical cube challenge pattern transmitted. If the inputted pattern on the selected cube face matches the transmitted pattern the method will authenticate the user and can generate a one-time 6-digit authentication code .

For a more detailed understanding of the present invention reference is now made to the accompanying drawings and description.

Figure 1. - Illustrates a flow diagram of the method for using one-time graphical cube authentication.
Figure 2. - Illustrates a method for registering a graphical cube authentication pattern
Figure 3. - Illustrates a method for authenticating a one-time graphical cube authentication challenge.

## DETAILED DESCRIPTION

Authentication methods are critical for securing access to electronic devices and applications. Traditional methods, including passwords and PINs, are vulnerable to various attacks such as phishing, keylogging, and brute force attacks. Biometric systems, while more secure, often require expensive hardware and can be inconvenient for users. There is a need for an alternative authentication method that is both secure and user-friendly.

This method utilises a graphical cube interface where a user can create and input unique patterns by selecting cells in a specific sequence onto one of the six coloured grid-based cube faces. The pattern can be input through touch gestures, such as swiping or tapping, on a touchscreen device. The method captures the sequence of cell selections and compares it to a securely stored pattern for authentication. The method enhances security by leveraging the user's spatial memory, visual colour memory and unique interaction style, making it more challenging for unauthorized users to replicate the pattern.

All aspects of the present invention can be implemented entirely in hardware, entirely in software or a combination of both hardware and software. Furthermore, all aspects of the

present invention may take the form of a computer program written in any one or more programming languages. The program code can be executed entirely on a computer or mobile device, partly on a computer and partly on a remote computer or entirely on a remote computer, running in a cloud environment or offered as a Software as a Service (SaaS).

With reference to Figure 1. a flow diagram **100** of a method for using one-time graphical cube authentication outlined in the present invention, a user may access the authentication mechanism through, for example, a browser, a mobile device or any other type of computer device **110.** At **111** a user makes a request for an authentication challenge to the authentication service **120** with their user id. At **112** the authentication service **120** verifies the user id and on successful verification generates a one-time authentication challenge cube, and securely returns the one-time authentication challenge cube including the challenge id back to the user. At **113,114** the one-time authentication challenge cube and cube face selector is drawn on the device screen. At **115** the user selects their coloured cube face using the cube face selector and inputs their unique pattern by selecting cells in a specific sequence onto the selected cube face. At **116** the user inputted pattern and challenge id are securely sent back to the authentication service **120** for authentication. At **117** the authentication service **120** sends back an authentication response to the user.

With reference to Figure 2 a diagram of a method for using one-time graphical cube authentication outlined in the present invention, more detail is now given for challenge provisioning & credential enrolment. As previously detailed in Figure 1 **112** the authentication service generates a one-time authentication challenge cube. Figure 2. **200** shows an example of the one-time authentication challenge cube faces generated at this time, each of the six grid-based cube faces consist of a M x N grid array of cells containing randomly generated characters. In Figure 2. **200** each of the six authentication challenge cube faces consist of 5 x 5 grid array of cells containing alphanumeric characters - this can be configurable to any size grid arrays i.e 6 x 6, 7 x 7, M x N in the authentication service. At **220** the generated one-time authentication challenge grid-based cube faces that make up the one-time authentication challenge cube are securely transmitted to the user. At **230** the authentication challenge cube is drawn on the user's device screen. At **231** the one-time authentication challenge cube face is drawn with all randomly generated characters that make up the cube face masked with a circular dot – the masking & shape used to mask the grid character can be configured on the authentication server. At **230** only one two-dimensional cube face of the one-time authentication challenge cube will be displayed at a time to the user – this can also be configured to be displayed as a three-dimensional (3D) cube. At **232** the cube face selector arrows are drawn on the user's device screen positioned around the outside of the cube face, these allow the user to move the one-time authentication challenge cube to all six of the authentication challenge cube's faces. Each of the six cube faces of the one-time authentication cube are coloured one of six colours – Front/Green, Back/Orange, Right/Blue, Left/Red, Top/Yellow & Bottom/Purple – colour is known to stimulate visual memory, helping in the recall of a credential & thus reducing the need for constant resetting. At **240** during user registration & credential enrolment the user is prompted to select a preferred coloured cube face from the one-time authentication challenge cube, using the cube face selector arrows positioned around the outside of the displayed cube face. At **250,251** the preferred coloured cube face has been selected, the user then inputs their unique pattern by selecting cells in a specific sequence onto the selected cube face. At **260** the user selected cube face pattern characters & challenge id are securely transmitted to the authentication service for enrolment. At **261** the authentication service receives the challenge id and characters from the one-time authentication challenge cube's selected cube face pattern. The authentication service verifies the challenge id & cube face

pattern, then, on verification, proceeds with enrolling the user pattern by mapping each of the one-time authentication cube face pattern characters to a cube face grid cell array position. The authentication service then securely stores the user's pattern grid cell array position map .

With reference to Figure 3. a diagram of a method for using one-time graphical cube authentication outlined in the present invention, more detail is now given to authenticating a user's one-time graphical authentication challenge cube. Figure 3. 3**00** shows an example of the one-time authentication challenge cube generated for each authentication request. Each of the six grid-based cube faces consist of a M x N grid array of cells containing randomly generated characters. At **310** a new one-time authentication challenge cube request is received by the authentication service, the authentication service will verify the user's request, then, on verification, generate a one-time authentication challenge cube. At **320,321** the authentication service will retrieve the verified user's pattern cube face grid position map from secure storage. At **322** the authentication service will randomly generate alphanumeric characters for each position in the pattern position map retrieved at **320,321**. At **323** the authentication service will update the generated one-time authentication challenge cube **f**ace grid at **320** with the characters generated at **322,** at each position within the position map retrieved at **320,321**. At **324** the generated one-time authentication challenge cube is securely stored. At **325** the one-time authentication challenge cube is securely transmitted to the user. At **326** the one-time authentication challenge cube is verified & decrypted on the user device. At **327** the one-time authentication challenge cube is drawn on the user's device screen including the cube face selector arrows. At **328** the user is prompted to input their unique pattern onto their chosen cube face. At **329** the user moves the challenge cube to the face registered during enrolment using the cube face selector arrows positioned around the outside the cube. At **330,331** the user then inputs their unique pattern by selecting cells in a specific sequence onto the selected cube face. At **332** the one-time authentication challenge cube face pattern characters selected during **330,331** & challenge id are securely transmitted to the authentication service for authentication. At **333** the authentication service verifies & decrypts the one-time authentication challenge cube face pattern characters selected during **330,331.** At **334** the authentication service retrieves the user's authentication challenge from secure storage identified by the challenge id, determines whether the pattern transmitted at **332** matches the pattern generated at **323** and returns an authentication response to the user. If the authentication service is configured to return an authentication code to the user on successful authentication, at **335** the authentication service will generate a 6-digit authentication code and return this code as part of the authentication response.

Figure 1.

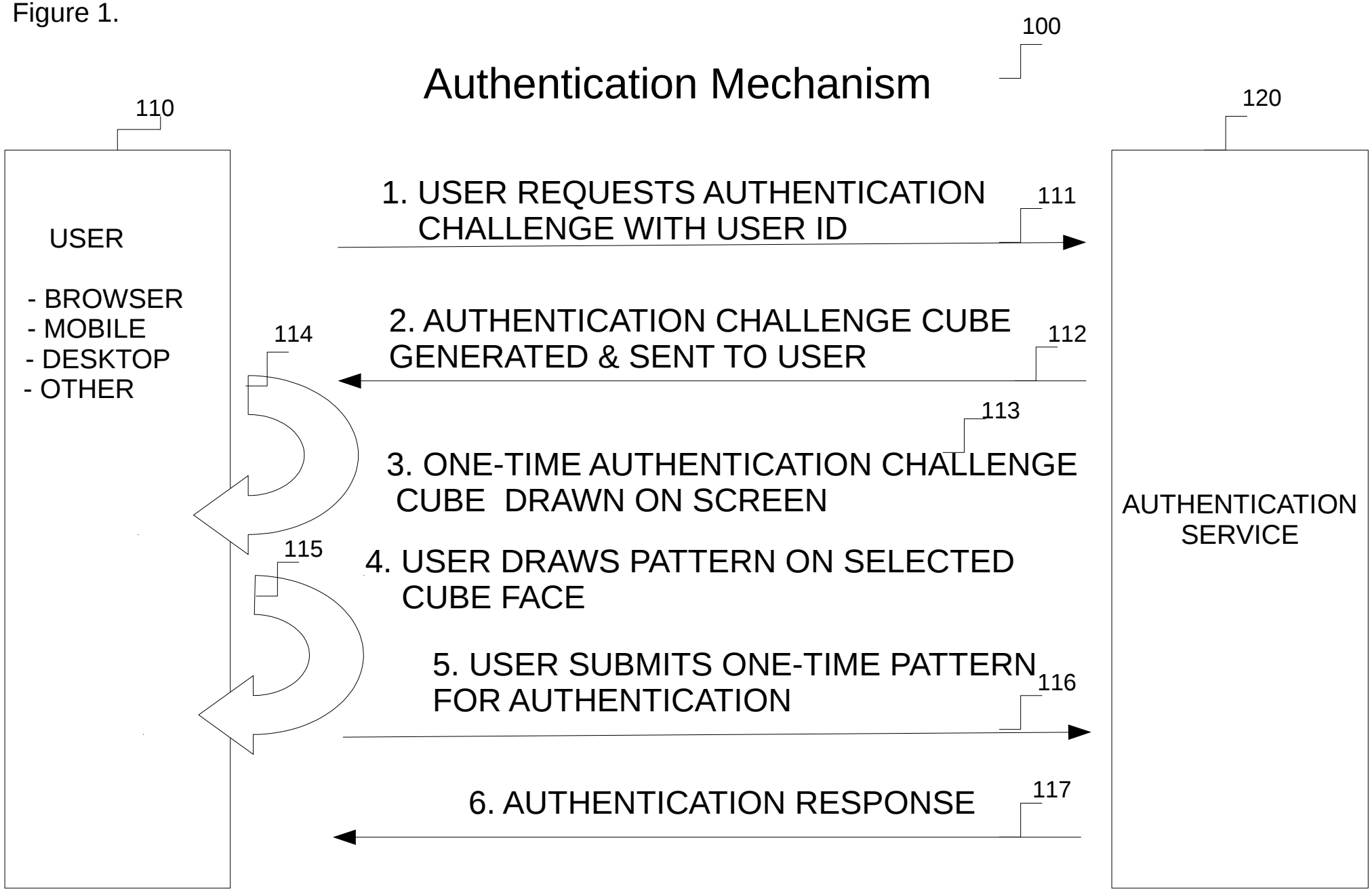

100
Authentication Mechanism
110
120
USER
- BROWSER
- MOBILE
- DESKTOP
- OTHER
1. USER REQUESTS AUTHENTICATION CHALLENGE WITH USER ID
111
2. AUTHENTICATION CHALLENGE CUBE GENERATED & SENT TO USER
112
114
113
3. ONE-TIME AUTHENTICATION CHALLENGE CUBE DRAWN ON SCREEN
115
4. USER DRAWS PATTERN ON SELECTED CUBE FACE
5. USER SUBMITS ONE-TIME PATTERN FOR AUTHENTICATION
116
6. AUTHENTICATION RESPONSE
117
AUTHENTICATION SERVICE

Figure 2.

# ONE-TIME GRAPHICAL CUBE AUTHENTICATION CHALLENGE PROVISIONING & CREDENTIAL ENROLMENT

200

| | | | | |
|---|---|---|---|---|
| J | 5 | M | L | 7 |
| K | D | Q | I | E |
| A | 3 | P | N | H |
| C | 1 | B | 6 | A |
| 2 | F | 9 | 8 | G |

| | | | | |
|---|---|---|---|---|
| 1 | J | K | N | L |
| B | 4 | P | M | A |
| 7 | F | 8 | C | 6 |
| I | D | 5 | H | G |
| Q | 9 | E | 2 | 3 |

| | | | | |
|---|---|---|---|---|
| J | D | 4 | 9 | E |
| N | 5 | 8 | B | P |
| 6 | A | K | 1 | M |
| H | 7 | 3 | 2 | I |
| C | Q | F | L | G |

| | | | | |
|---|---|---|---|---|
| G | 7 | I | 1 | M |
| J | 6 | 8 | K | 3 |
| C | P | D | 5 | L |
| B | A | H | Q | 9 |
| E | 2 | F | N | 4 |

| | | | | |
|---|---|---|---|---|
| 1 | F | D | 8 | P |
| K | B | 7 | H | M |
| 3 | A | I | 2 | C |
| Q | L | 5 | G | N |
| 4 | E | J | 6 | 9 |

| | | | | |
|---|---|---|---|---|
| M | E | L | C | J |
| N | 1 | 4 | 9 | K |
| 3 | B | 2 | G | Q |
| I | P | 8 | 5 | 7 |
| D | F | 6 | H | A |

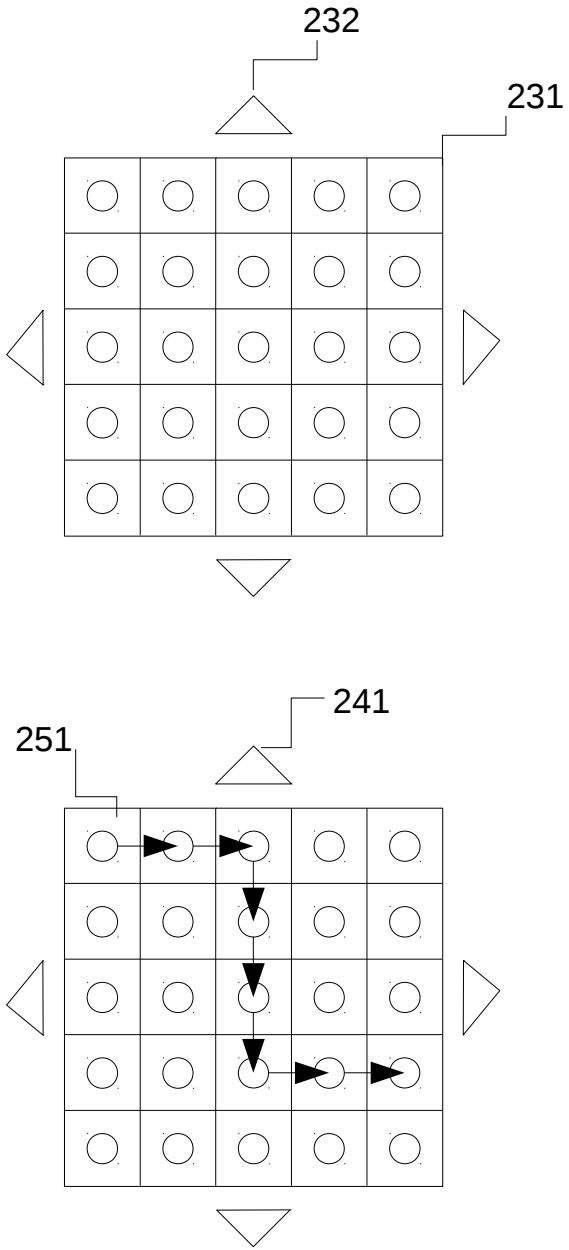
210

1. GENERATE SIX ONE-TIME AUTHENTICATION CHALLENGE CUBE FACE M x N GRIDS

220

2. SECURELY TRANSMIT ENROLMENT CHALLENGE GRIDS TO USER

Figure 2.




# ONE-TIME GRAPHICAL CUBE AUTHENTICATION CHALLENGE PROVISIONING & CREDENTIAL ENROLMENT

230

5. DRAW CHALLENGE CUBE FACES ON SCREEN WITH CUBE FACE SELECTOR ARROWS

240

6. USER ROTATES CUBE USING SELECTOR ARROWS TO PREFERRED COLOURED CUBE FACE

250

7. USER DRAWS PATTERN ON SELECTED CUBE FACE

260

8. PATTERN TRANSMITTED FOR ENROLMENT

261

9. USER PATTERN ENROLLED & SECURELY STORED

Figure 3.

# ONE-TIME GRAPHICAL CUBE AUTHENTICATION

300

Front / Green *

| | | | | |
|---|---|---|---|---|
| J | 5 | M | L | 7 |
| K | D | Q | I | E |
| A | 3 | P | N | H |
| C | 1 | B | 6 | A |
| 2 | F | 9 | 8 | G |

Back / Orange

| | | | | |
|---|---|---|---|---|
| 1 | J | K | N | L |
| B | 4 | P | M | A |
| 7 | F | 8 | C | 6 |
| I | D | 5 | H | G |
| Q | 9 | E | 2 | 3 |

320

Right / Blue

| | | | | |
|---|---|---|---|---|
| J | D | 4 | 9 | E |
| N | 5 | 8 | B | P |
| 6 | A | K | 1 | M |
| H | 7 | 3 | 2 | I |
| C | Q | F | L | G |

Left / Red

| | | | | |
|---|---|---|---|---|
| G | 7 | I | 1 | M |
| J | 6 | 8 | K | 3 |
| C | P | D | 5 | L |
| B | A | H | Q | 9 |
| E | 2 | F | N | 4 |

Top / Yellow

| | | | | |
|---|---|---|---|---|
| 1 | F | D | 8 | P |
| K | B | 7 | H | M |
| 3 | A | I | 2 | C |
| Q | L | 5 | G | N |
| 4 | E | J | 6 | 9 |

Bottom / Purple

| | | | | |
|---|---|---|---|---|
| M | E | L | C | J |
| N | 1 | 4 | 9 | K |
| 3 | B | 2 | G | Q |
| I | P | 8 | 5 | 7 |
| D | F | 6 | H | A |

310

1. GENERATE SIX ONE-TIME AUTHENTICATION CHALLENGE CUBE FACE M x N GRIDS

321

2. RETRIEVE USER REGISTERED CUBE FACE PATTERN GRID POSITIONS

322

Back / Orange

| | | | | |
|---|---|---|---|---|
| | | | N | L |
| B | 4 | | M | A |
| 7 | F | | C | 6 |
| I | D | | | |
| Q | 9 | E | 2 | 3 |

323

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 9 | V | F | N | L |
| 1 | B | 4 | F | M | A |
| 2 | 7 | F | 7 | C | 6 |
| 3 | I | D | A | N | 8 |
| 4 | Q | 9 | E | 2 | 3 |

324

3. ENCRYPT ONE-TIME AUTHENTICATION CHALLENGE CUBE FACE GRIDS AND SECURELY STORE

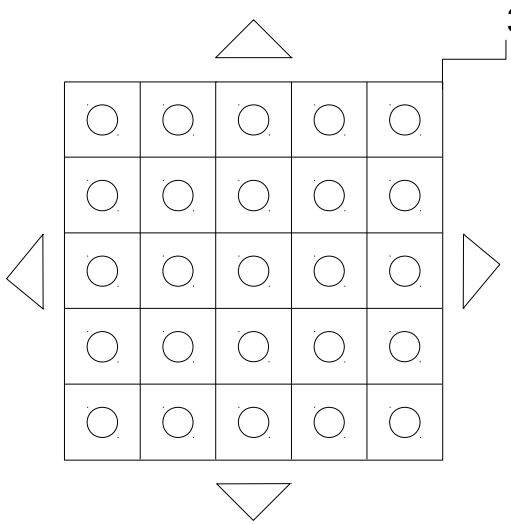
325

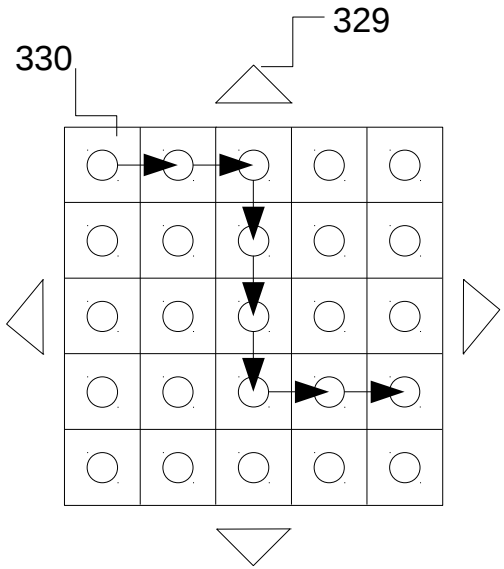
4. TRANSMIT ENCRYPTED CHALLENGE GRIDS TO USER

* CUBE FACE & COLOUR

Figure 3.

# ONE-TIME GRAPHICAL CUBE AUTHENTICATION




326

5. DECRYPT ONE-TIME CHALLENGE CUBE FACE GRIDS ON USER DEVICE

327

6. DRAW CHALLENGE CUBE ON SCREEN WITH CUBE FACE SELECTOR ARROWS

328

7. USER ROTATES CUBE TO COLOURED FACE SELECTED DURING CREDENTIAL ENROLMENT

331

8. USER DRAWS PATTERN ON SELECTED CUBE FACE

332

9. USER PATTERN ENCRYPTED AND SUBMITTED FOR AUTHENTICATION

333 - 335

10. AUTHENTICATION RESPONSE RECEIVED FROM AUTHENTICATION SERVICE