Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2018, 5(7): 474-480

Research Article ISSN: 2394 - 658X

Design and Implementation of Game Based Security Model to Secure the Information Contents

Bindu A N and Dr. Jalesh Kumar

Department of Computer Science and Engineering, JNNCE Shivamogga, shivamogga, India- 577201
binduan99@gmail.com, jalesh_k@yahoo.com

ABSTRACT

Cryptography is used to provide security for the data by using cipher text, plain text and secret key. But it has its own problems, even though the cipher text likes like meaningless information the attacker can interrupt the data while transmitting from sender to receiver. The sender must be careful while sending the information, otherwise the message will be known to the unauthorised users. Hence to overcome from these problems game based cryptography techniques is used to provide security for the sensitive information. In this work, security models based on rubic cube, Sudoku and ken ken puzzle games are designed and implemented. The performance analysis is carried out based on peak signal to noise ratio.

Key words: Cryptography, Rubic cube, Sudoku, Ken ken puzzle, Peak signal to noise ratio

---

1. INTRODUCTION

Nowadays providing security for the information or data becomes a big challenging task. Along with the protection of the data, maintaining the integrity and authentication of the data is also an important thing. As the technology improves the method of providing security is also difficult and it is tough task to safe guard the information from the unauthorised users. Most of the information's are conveyed through images. By using variety of techniques, data is protected from the unauthorised users. Image encryption plays an important role in the protection of the data. Byhiding the information in the images, authentication can be achieved. Hence the unauthorised users can't easily access the information from the images, even it is difficult to identify that the data is hidden in image. So, many algorithms are used to perform the image encryption and decryption process along with traditional cryptosystem.

2. LITERATURE SURVEY

Many efforts are identified for image encryption; most of the work is based on standard techniques or chaos method. Adrian-Viorel diaconu [1] introduces many algorithms for the image encryption such as novel chaotic, permutation-substitution and gray-scale image encryption algorithm. All these algorithms are used to reduce the redundancy of the Fridrich's structure based encryption algorithm. Rubik cube is the main principles used in the designing of the digital images and confusion, diffusion are the important properties included to provide the security. NPCR and UACI are the different tests used in the encryption algorithm.

Arnab k. maji, et al [2] discusses the image encryption technique based on Sudoku. Sudoku is "the digital must remain single". This game is based on numeric and problem solving. Minigrid based algorithms are used to develop the Sudoku. In this work 9*9 Sudoku puzzle is solved with 81 cells and backtracking is performed for each of the cell. Instead of performing operation on each of cells, backtracking is performed only on those minigrids and it also consumes less time to perform the operation. Here no guessing of the value is possible in the whole computation. This game is implemented in many applications and those applications found in the field of steganography, cryptography, image authentication, image encryption and so on. To solve Sudoku problem few logical techniques are required. Backtracking is one of the basic techniques used to solve this Sudoku problem.

John black, et al [3] discussed internet chess club which is an online game which is popular through the world with more than 30,000 users or members. This ICC ensures the security for the users between client and server. Earlier by using the time stamp, players are cheated by the name of awards and cash prize. Hence Sleator's introduces the encryption method in the chess game to present the time stamp tampering, so the data sent is encrypted between the client and ICC server.

Therefore the client can sent data to the server without worrying about the eavesdropper. It uses two distinct security models such as time stamp and communication model. The time stamp model controls the machine and the programs running on the client side. The main problem of this game is cheating. To overcome control of the time stamp process from the players are removed and encryption process is adopted, then key is generate by the process provides the security in both client and server side. Hence it provides authentication for the players.

Valeriu Mannuel Jonescee, et al [4] discusses about the improved encryption algorithm is simple but give the powerful solution and it uses the simple function using XOR operation. The implementation of image size & computational plat from encryption algorithms are compared with Rubik's cube principle. In the encryption algorithm first need to find out the direction of the circular shifts, so two random vectors are generated with the help of these vectors the number of circular shifts are computed. The security level was tested for different type of attacks and ensures the security level by implementing both algorithms. The difference of time also calculated. This encryption algorithm which is improved also tested on a mobile device to know the level of performance in the device. The main advantages of this method are, on server side computations are occurring at faster and the availability of the memory is large.

A. Iosup [5] describes about the puzzle which is a game it provides an entertainment for the players by solving logical challenges because it requires more time to solve the each instances of puzzle. The main aim of this approach is to generate the puzzle instances automatically by using the random walk and game solving methods. To overcome from this problem two types of metrics are considered and history based mechanisms were also used to find out the ability of solving the puzzle by the player. The number of the times played and the number of instances takes to solve the puzzle are stored in the database. With the help of this database it is easy to find out the level of difficulty for solving puzzle by the players.

Kiminori Matsuzaki [6] describes the puzzle game 2048 which is a single player game. In this game only four grids are used to play the game among N tuples. This game attracts the people because of its easy way learning and playing the game. Earlier systematic method was proposed to select the N tuples in the game and those tuples should be independent of each other. If the number of tuples are limited then the selection of tuples does not holds good. To overcome from this method another method is proposed, this method provides the successful result as designed by humans and this method can also be applied to other games. The temporal difference learning algorithm was introduced by the szubert and Jaskowskio and it discusses about how to apply the tuples network to the game. The time complexity is more for this game when the depth is more. By applying this method the time required to play is reduced to milliseconds.

Zhan-heou, et al [7] discusses steganography which is a method of hiding data using different cover media. To hide the data steganography method that to three phase embedded algorithm is proposed. The main intension of the steganography is that the data which is hidden in the stego image should not be detected by the hackers. The system will generate the random key when player start the game. Embedding system, extraction, scenarios are the parts of the system. For the secret message random seed will generate in a sequence. Once the random seed is generated, the meaningless tetromino starts generating the meaningless tetromino until the game is finished. In novel steganography method the data is hidden in the form of the tetromino sequence.

Braden Soper, et al [8] botnet is game which is based on model of local mean field. This method contains many features to deal with the complexities of this botnet game. It has a bot master, it take the control of each and every computers. This game is played between the bot master that is attacker and the owner of the computer that is defender. The botnet game can be extended to play with more number of players. When the number of players increased the security for game also became complicated. The bot master has centralised and decentralised agents. Decentralised agents has higher threshold compare to centralised agents, in this case botnet plays an higher aggressiveness over the central agents.

Andrew C. Gallagher [9] discussed about the tree types of puzzle. They proposed the tree based algorithm and it uses the merge components to solve the puzzle problem. Initially in the jigsaw puzzle, the image pieces have the unknown orientation and unknown location. To solve this, the puzzle dimension should know to the developers. When the location or dimension is known, it leads to the complexity of solving the puzzle. When the orientation is unknown and location is unknown, in this case it requires least time for the computation. By using tree based reassembly method type one and two puzzles are solved and it is able to solve the state of art even though without knowing the jigsaw orientation and remaining one type of puzzle is solved.

3. DESIGN METHODOLOGY

In this work, encryption model based on different types of games are proposed. Three different types of games are considered-

i. Rubik cube
ii. Ken Ken
iii. Sudoku

The following figures 1 and 2 shows the encryption and decryption process of the image. Input is the original image which is used to hide the information or data and undergoes many processes as input.

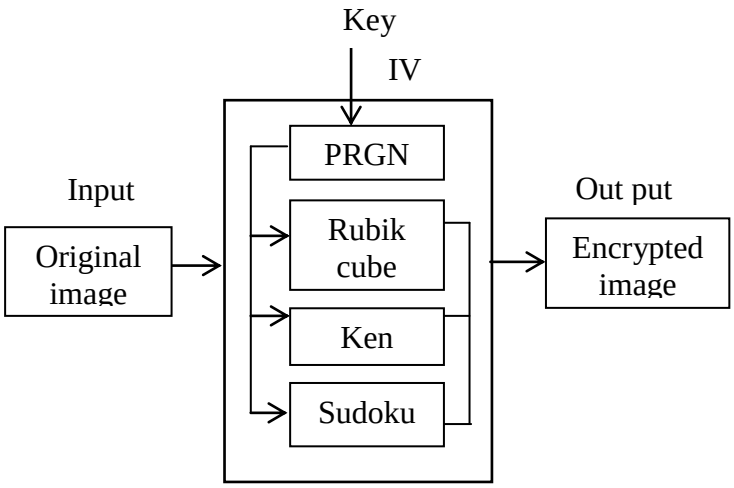


Fig. 1 Block diagram for image encryption

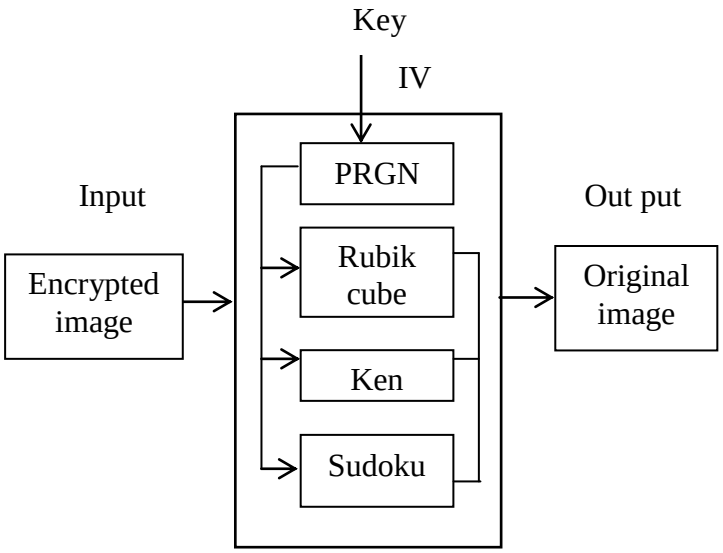


Fig. 2 Block diagram for image decryption

Initialization vector is used to indicate that the image has fixed size. Pseudorandom number generator is used to generate the sequence of random numbers. These sequences of random numbers are generated for each game process. So that with the help of random numbers secret key is generated. By performing various processes on the input image, secret key is generated. By using this secret key the data is hidden in the image and hence the image is encrypted.

Algorithm for Rubik cube:

Step 1: before solving the Rubik cube its necessary to know the different size of rubik cube. The first step is to identify the different types of pieces and colours present in the cube.

Step 2: in each face, the centre piece of the cube must contain any colour but it must be only one colour.

Step 3: initially make the centre piece as logo piece that is white. White is the only colour which is used as a logo piece of the cube.

Step 4: the next step is to identify the number of edge pieces present in the cube and two colours are present every edge piece and once the edge is obtained then identify the corner piece of the cube.

Step 5: next step is that make sure that the logo piece that is white colour is present in the top layer. Means it must face upwards.

Step 6: now make the white piece as cross on the top layer of the cube such that white must be remain same in the centre piece.

Step 7: now set the top corner piece as white so that the remaining piece must remain same as in the previous step and top face is arranged with white colour pieces.

Step 8: now solve to the middle layer hence move the solved top layer into bottom layer of the cube.

Step 9: in the middle layer first place the edge pieces to their position so that rest of the layers can be solved easily.
Step 10: once all the edge pieces are present in the correct position the middle layer is solved so that move to the last layer.
Step 11: move the solved yellow side to the upwards and then make yellow piece as cross as in the sixth step.
Step 12: in the last step place the yellow piece at the corner of the top face. Once the corner pieces are set with the yellow colour we will get the solved Rubik cube.

Algorithm for ken ken:
Step 1: before playing the ken ken game the players needs to identify the different sizes of puzzle and should select the size of the puzzle to be solved.
Step 2: once the size is selected it necessary to select the mathematical operation to be performed. It may be addition, subtraction, division and so on.
Step 3: fill the numbers in the cells and each number should present only once in each row and column. Example a 4*4 grid should contain only 1,2,3,4 numbers only once.
Step 4: next step is to reach the target number which is given in the cage by performing the mathematical operation mention in the cage itself.
Step 5: mathematical operation is not stick to particular one. More than one operation can be performed in the puzzle but only one operation in cage.
Step 6: the cage may contain the repeated numbers but same numbers should not present in row or column.
Step 7: in the last step each cells should contain the correct numbers and so that ken ken puzzle is completely solved.

Algorithm for Sudoku:
Step 1: initially select the puzzle with the 9*9 grid.
Step 2: divide the grid into subgroups which has 9 cells in each subgroups.
Step 3: each subgroups must contain all the numbers from one to nine and should not repeated.
Step 4: select the subgroup which contains only one empty cell or least numbers of empty cells.
Step 5: Then perform the hatching and counting operations.
Step 6: in the empty cell, make the temporary notes on the corner of the each cells.
Step 7: Apply the same method to the rows and columns and find the missing number in the rows and columns and make the temporary notes in them.
Step 8: select the proper temporary notes (marks up) as permanent numbers and filled in the cells.
Step 9: the same procedure is performed until the entire cell in subgroups that is in the puzzle contain unique numbers.
Step 10: once the cells are filled by the unique number without repeating in the subgroups, rows and columns it means that the Sudoku puzzle is completely solved.

4. RESULT ANALYSIS

In this dissertation, different game based encryption techniques are designed and implemented. Based on random selection, Rubik's cube, ken ken puzzle and Sudoku based encryption technique is applied. The results obtained in the different techniques are presented in this chapter. The result obtained are analysed with PSNR value.
The Fig. 3 (a)-(c)show the input images considered for the encryption process. Fig 4 shows the result obtained from the Rubik cube method. The result shows that encrypted images (Fig. 4(b1)-4(b3)) are completely different from the input images (Fig. 4(a1)-4(a3)) and not giving any clue about the original input image. According to the number of different rows and columns shuffling, the encrypted images are scrabbled. Scrambled rows and columns are given below.Fig 4 (c1)-4(c3) shows the result of decryption process.
Fig 5 show the results of the Sudoku puzzle. The result shows that the encrypted image (Fig. 5(b1)-5(b3)) and input images are not identical. Encrypted image is totally different from original image. Fig. 6(b1)-6(b3) describe the results obtained by ken ken puzzle. This result also explains that the original image is different from encrypted image. The encrypted image does not provide any formation about the original input image. Fig. 5 (c1)-5(c3) and Fig. 6(c1)-6(c3) show the result of decryption. From the decryption images it is evident that there is no loss of information in the decrypted images.

192	196	205	112
115	123	117	112
190	124	127	130
213	231	116	145

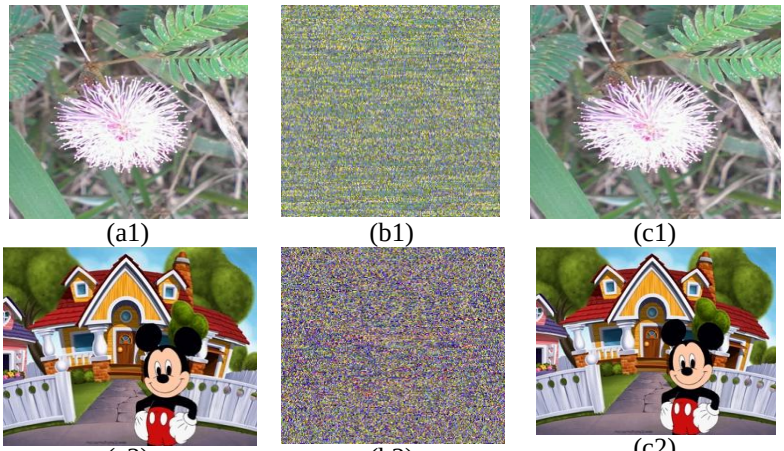
205	112	112	186
117	112	111	111
127	130	180	114
116	145	231	132

196	205	112	112
123	117	112	111
124	127	130	180
231	116	145	231

112	112	186	110
112	111	111	165
130	180	114	178
145	231	132	116

(a) (b) (c)

Fig. 3 Input images for image encryption

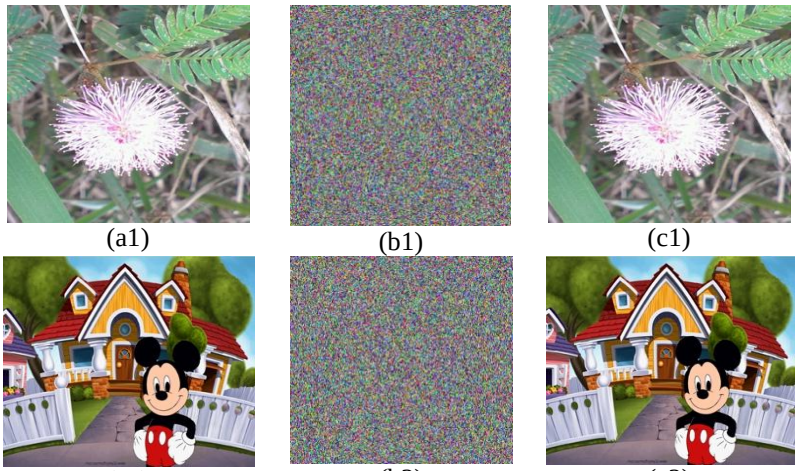


(a1) (b1) (c1)

(a2) (b2) (c2)

(a3) (b3) (c3)

Fig. 4 Encryption process using Rubik cube method (Method 1)



(a1) (b1) (c1)

(a2) (b2) (c2)

(a3) (b3) (c3)

Fig. 5 Encryption process using Sudoku (Method 2)

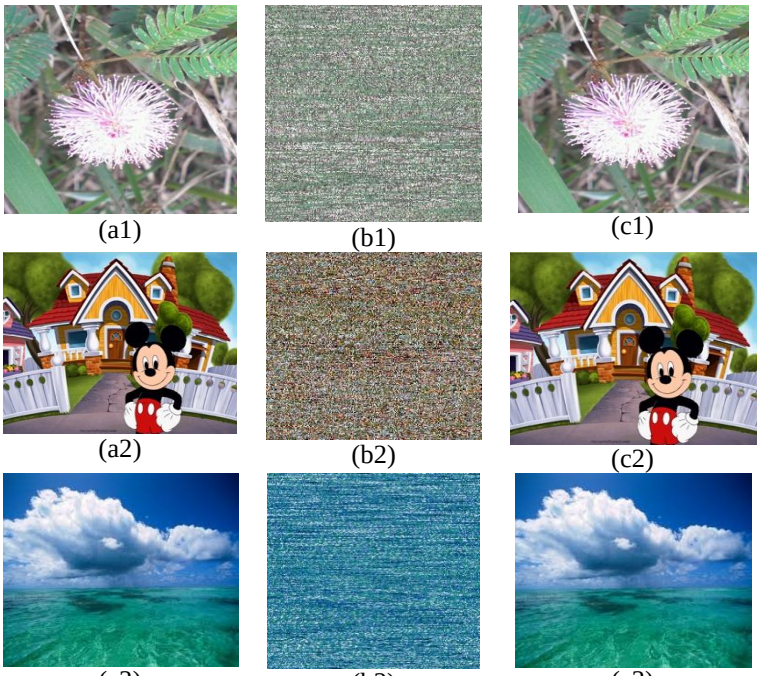


Fig. 6 Encryption process using ken ken puzzle (method 3)

PSNR Analysis:

The PSNR can be computed by

$$\text{PSNR} = 10log_{10}\ \frac{L^2}{MSE} \quad (1)$$

Where MSE (mean square error) is

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}(c_i - p_i)^2 \quad (2)$$

Table -1 PSNR Analysis

Input Images	Method 1	Method 2	Method 3
3 (a)	10.4	8.67	11.67
3 (b)	9.8	7.89	10.02
3 (c)	10.3	8.45	11.01

The analysis carried out for three different methods based on peak signal to noise ratio (PSNR). The PSNR values are computed between input images and corresponding encrypted images. The values are tabulated for three different methods. It is observed from the table that compared to method 1 and method 3, method 2 gives the efficient result. Low value in the PSNR indicates that it is not possible to identify the original input image on the basis of encrypted image and encrypted image is completely different. There will not be any clue in the encrypted image to guess the original input image.

5. CONCLUSION

Now a day's technology is developing very fast, as the technology developing maintaining our data securely from the unauthorised users is also big challenging task. Many technologies were developed to secure the sensitive information. In this work mainly described about the security of the data by using different games. The different methods are used to solve the Rubik cube, ken ken and Sudoku. By using the methods used in these games, the information is protected from the unauthorised users. These methods are successful in maintaining the sensitive information securely by using game based cryptography.

REFERENCES

[1]. Adrian-Viorel diaconu, "Kenken puzzle–based image encryption algorithm", The Publishing House of the Romanian Academy Volume 16, Special Issue, pp. 271-286, **2015**.

[2]. Arnab k. maji, "A Novel Algorithmic approach for solving Sudoku puzzle in Guessed Free Manner", European Academic Research, vol. I, issue 6/ September **2013**.

[3]. John black, Martin cochran, and Ryan gardner, "A Security Analysis of the Internet Chess Club", IEEE security & privacy.

[4]. Valeriu Mannuel Jonescee, Adrian – Viorel Diaconee, "Testing the performance of the improved Rubik's cube encryption algorithm on virtual system", IEEE computer society, **2015**.
[5]. A. Iosup, "Player-Customized Puzzle Instance Generation for Massively Multiplayer Online Games", 978-1-4244-5605-5/09, IEEE publication, **2009.**
[6]. Kiminori Matsuzaki," Systematic Selection of N-Tuple Networks with Consideration of Interinfluence for Game 2048", 978-1-5090-5732-0/16, IEEE publication, **2016**.
[7]. Zhan-heou, Ling-hwei chen, "hiding data in tetris", Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, **2011**
[8]. Braden Soper and John Musacchio, "A Botnet Detection Game", Fifty-second Annual Allerton Conference Allerton House, UIUC, Illinois, USA October 1 - 3, **2014**
[9]. Andrew C. Gallagher, "Jigsaw Puzzles with Pieces of Unknown Orientation", IEEE publication-**2012**.