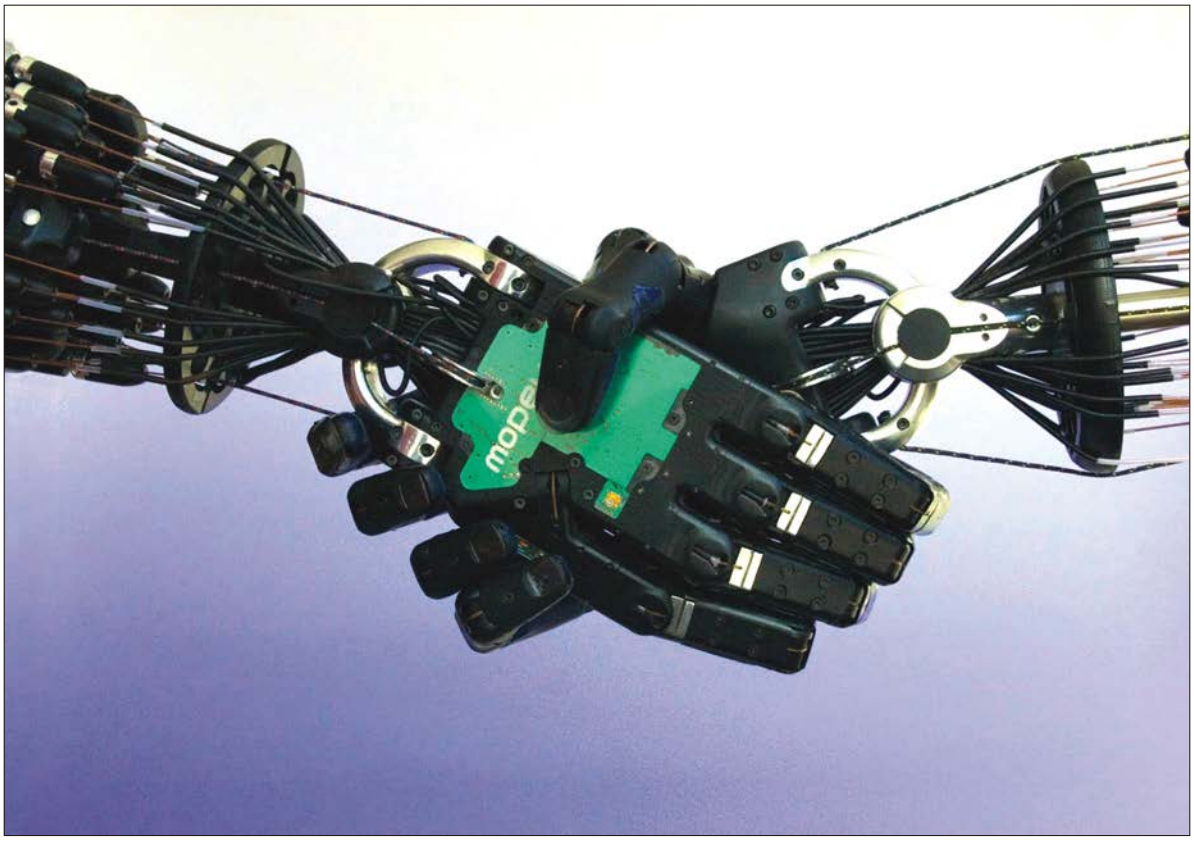

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 7 (4): 161-171, 2014
ISSN 1994-5450 / DOI: 10.3923/jai.2014.161.171

Graphical Password Authentication Scheme for Embedded Platform

Siva Janakiraman, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: Siva Janakiraman, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

Numerous existing graphical systems in the embedded world for password authentication use image, area or pattern selection process. This study presents a novel method that employ image selection at its first level and an isolated pattern selection process on a magnified image display at its next level to provide a well secured password authentication system. The firmware for the proposed authentication scheme was developed under Eclipse open source platform and tested on Cortex-A8 embedded device as a standalone system with the aid of a TFT based graphical LCD screen, a character LCD and a keypad.

Key words: Graphical password, pass points, authentication, ARM, embedded security, hardware security

INTRODUCTION

Data in digital form can be secured via scrambling process called cryptography or by means of hiding on other cover media known as steganography (Amirtharajan *et al*., 2012; Amirtharajan and Rayappan, 2013; Amirtharajan *et al*., 2013a-j; Chan and Cheng, 2004; Cheddad *et al*., 2010; Praveenkumar *et al*., 2012a, b, 2013a-d, 2014a-m; Thanikaiselvan *et al*., 2012a-c, 2013a, b). These security schemes made use of still images and randomness (Amirtharajan and Rayappan, 2012; Janakiraman *et al*., 2012b; Rajagopalan *et al*., 2014) as methods for securing the data. Embedded devices such as microcontrollers (Janakiraman *et al*., 2012a; Janakiraman *et al*., 2014) and Field Programmable Gate Arrays (FPGAs) (Janakiraman *et al*., 2013; Rajagopalan *et al*., 2012a, b) have been the choice of platform for the implementation of security in devices that requires portability. In the increasingly internet-dependent world of today, it is imperative to have sound security and password authentication schemes (Tazawa *et al*., 2010).

There are two important requirements for an effective password; it must be easy to remember and must be hard to crack. Thus the characteristics of a secure password are:

- Password must be long enough
- Should contain a blend of alphabets (upper case and lower case), numbers as well as special characters
- Should never contain any phrase book words or user's private information

Recent years have seen an exponential increase in the number of transactions being carried out online. Thus the users are required to manage different accounts for the various services that

they avail. These days, graphical password is being regarded as promising alternative to replace traditional text-based password in network security (Meng, 2012). Here, the users interact with images for authentication rather than input alpha-numeric strings. This is because image-based password provides a high level of security and is user friendly. The categories of graphical authentication schemes (Hashemi *et al.*, 2012) include image, area or pattern selection. The image schemes involve a click to select an image from the pool; area-based method needs sequence of image selection while pattern-based method relies on drawing some patterns.

People saw the importance of security on the internet and began incorporating techniques to build a stronger secure network. They began to realise the effectiveness of image-based password authentication schemes in providing secure systems. This gradual move towards image-based passwords is seen in the banking sector, e.g., the CUB online banking portal uses image-based password (i.e., where the user selects an image from a group of images displayed) as an entry level authentication and conventional text-based passwords as the second level of authentication. The pattern lock authentication scheme has been incorporated in devices where there is a touch panel interface e.g., smart phones and tablets.

This scheme involves the user drawing a specific continuous pattern i.e., a pattern which is drawn without the user taking his finger off the touch screen. But touch screens are not at everyone's disposal. Thus this study was aimed to design a system that has a wider reach among the customers. Here, we let the user to select an image from a small pool at the first stage. In the next stage it is then combined with pass point method (Wiedenbeck *et al.*, 2005) where, discrete point selection process (click area/click point) is carried out on the selected image. In between the image selection and area selection, the user can select a magnification factor before he starts picking his pass points (areas) on the selected image. The proposed scheme can be effectively put to use among many others, in the areas like banking, finance, online shopping, electronic mail, etc.

MATERIALS AND METHODS

Proposed password authentication scheme

Hardware implementation: The two stage graphical password authentication scheme is implemented on the application level embedded processor CORTEX-A8 where, a graphical TFT based colour graphical LCD (GLCD) screen of dimension 240×320 (Rows×Columns) is interfaced via Serial Peripheral Interface (SPI) to display the required images. A 16×2 character LCD (CLCD) interfaced via Inter Integrated Circuit (I^2C) is used to display the options to be selected by the user for the purpose of password creation, verification or to gain access to the login (authentication). The detailed guide lines for the user in selecting the options displayed in character LCD is provided through serial communication via the on-chip Universal Synchronous Asynchronous Receiver Transmitter (USART) of the embedded processor.

The layout map of GLCD with pixel numbers and row, column positions are given in Fig. 1a. Data is written to the colour GLCD screen by means of writing to the particular memory location using a pointer. The pixel values written to the memory locations contain four bytes of data. The MSB byte, a don't care value is usually kept as zero. The remaining three bytes of data correspond to Red, Green and Blue (RGB) colour components. Grey scale images can be displayed by writing the same eight bit pixel value of the image to all the three fields (RGB) of a particular address as shown in Fig. 1b.

The entire screen is made white (cleared), by writing the value 0xFFFFFFFF to the address corresponding to all pixels of the GLCD screen before the display of actual images. The general principle for the magnified display of 100×100 image as 200×200 image on the GLCD screen is to write the same pixel value in multiple locations in a proportionate manner so that the image

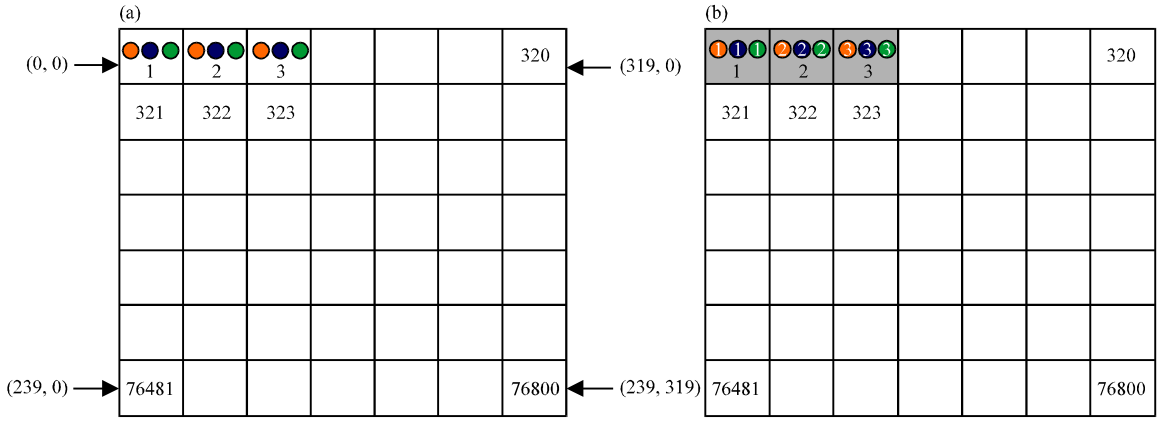

Fig. 1(a-b): (a) Layout of GLCD and (b) Grey image display using RGB components

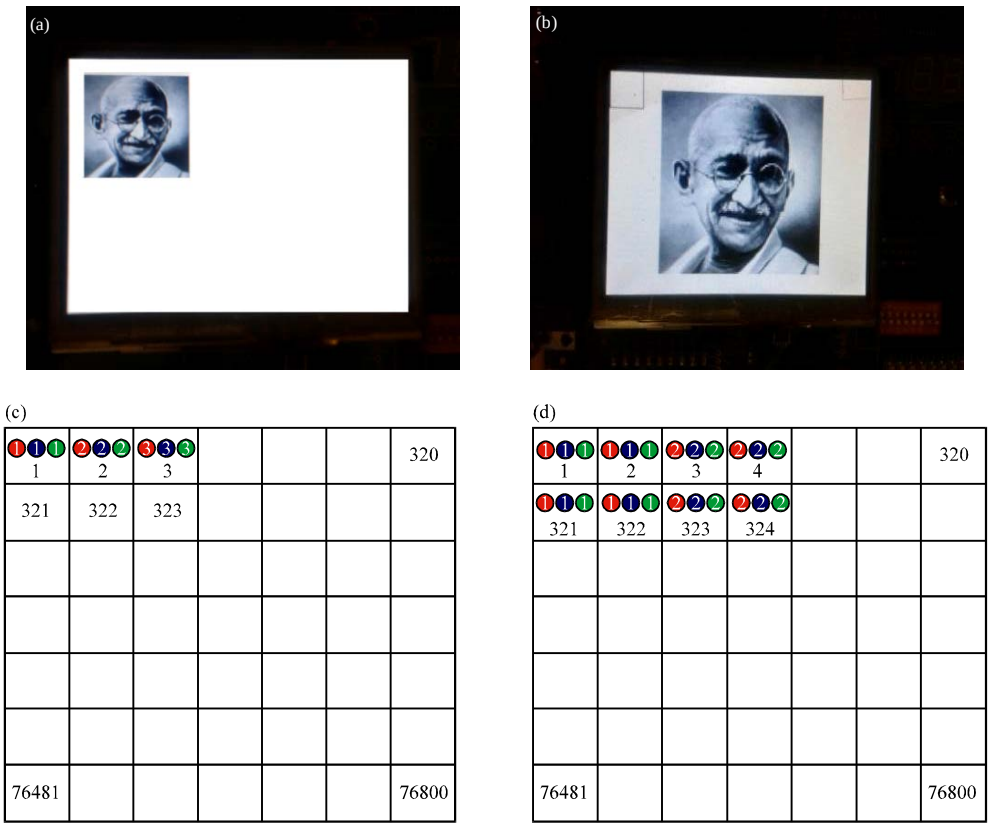

Fig. 2(a-d): (a) Original grey image 100×100, (b) Magnified grey image 200×200, (c) Pixel layout for original image display and (d) Pixel layout for magnified image display

appears magnified. The square image is made double of its size on both width and height by copying the original pixel values in its next column and row. For example, the first pixel value is written in (1, 1) (1, 2) (2, 1) (2, 2) locations so as to double the image size on both height and width. The grey image display in original and magnified size along with the pixel positions in the display layout to be written with the values of image pixel are shown in Fig. 2.

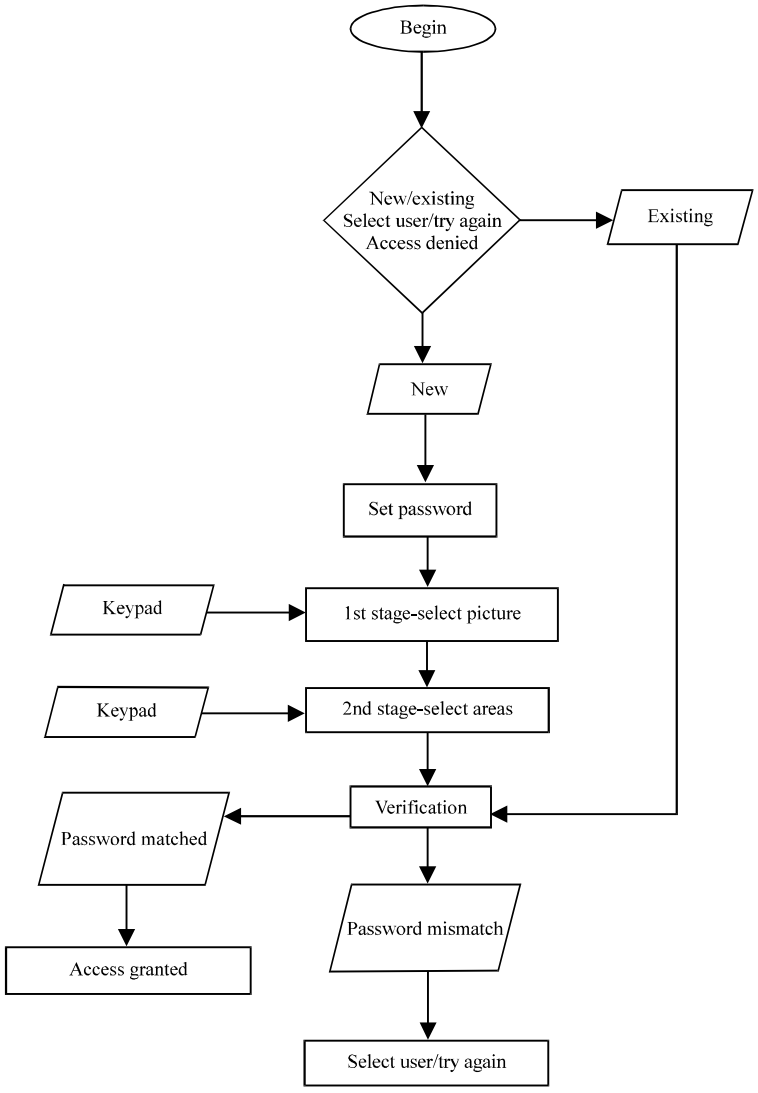

Fig. 3: Flowchart for overall authentication scheme

The flowchart of the overall authentication scheme is shown in Fig. 3. The various option selections can be done using the 6×6 keypad connected via a Power Management Integrated Chip (PMIC) with built-in scanning mechanism for the detection of hardware key press.

Password creation: Initially the users are asked to identify him as a new user or an existing user. A new user is asked to set a password while an existing user is directed to the verification stage. Every new user is first assigned with an account number that acts as user name. For the first stage of password setting, the new user has to select an image as password from the four 100×100 images displayed on the graphical LCD screen. Then, the selected image is magnified and displayed as a 200×200 image on the screen. There is also a 40×40 selection box appears on the top left corner of the screen for the user to select specific areas of the image.

The second stage of password setting involves the user moving the selection box across the magnified image and selecting portions of the image in any specific order as he desires. The

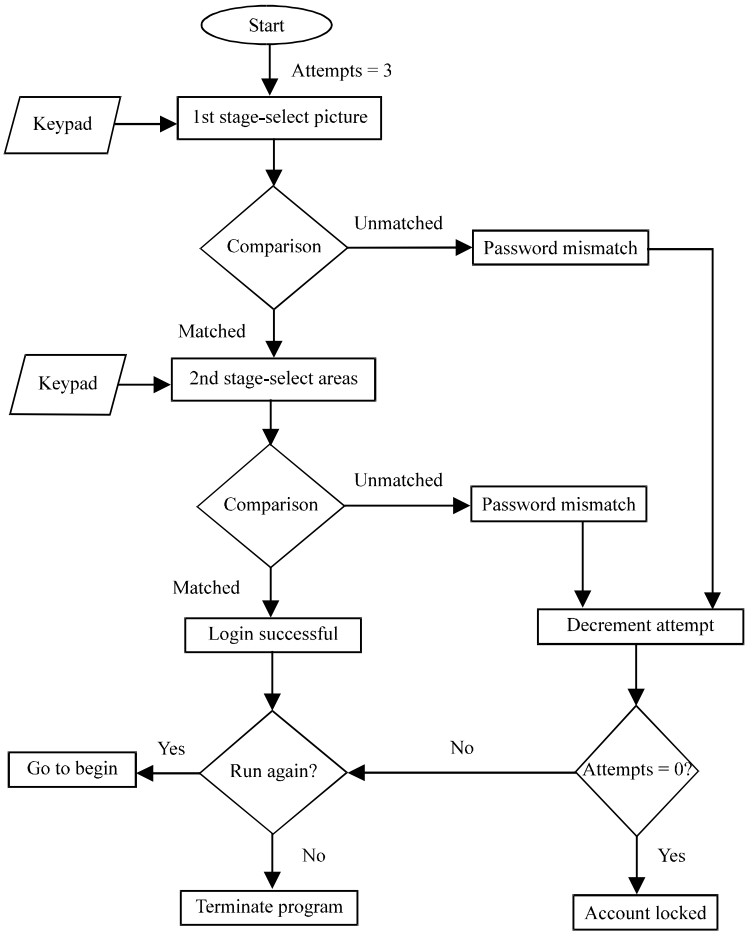

Fig. 4: Flowchart for verification process

maximum number of areas that can be selected on the image by the user (password length) is four. The selection box is moved with the help of keypad inputs 4 for left, 8 for up, 6 for right, 2 for down and 5 for selecting that portion of the image as one digit of the password. In case of mistake in the selection of the desired area, the user is given an option to deselect the last selected area. After the user completes setting the two levels of passwords, a success message is displayed on the character LCD.

Authentication/verification: The first stage of authentication involves the user selecting the correct image from a group of images displayed on the GLCD screen. When the user selects a wrong image, a "Password Mismatch" message is displayed warning the user that he has two more chances to type in the correct password before the account is locked. Once the user selects the correct image, a magnified version of the image is displayed along with the selection box on the screen. The user then has to select, in the correct sequence, portions of the image that he set as his password using the selection box. In case of mistake in the selection of the desired area, the user is given an option to deselect the last selected area. After selecting all the digits of the password, the user can give the required keyboard input to state that he has completed typing in the password. The verification process is shown in Fig. 4.

Initially the user identifies him as an existing user or new user. Existing users are directly taken to the password verification phase. The user then has to input his account number. Entering an invalid account number by the user displays an error message. For the first stage of verification, the user has to select one image from the four displayed on the GLCD screen. The user then proceeds to the second level of verification, where he has to select the areas in correct sequence from the selected image. Once the user enters the full password, a comparison process takes place where the entered password is compared with the original set password. In the case of mismatch either in the first stage or in the second stage of verification in terms of wrong positions/sequence/number of areas, a "wrong password" message appears. This detects the number of chances the user has to enter the correct password and after which the user is taken back to the start screen where he can again enter as a new or existing user. Finally, the account gets locked for the next 24 h when the user enters wrong password for three consecutive times. A "Password successful" message appears in the case of a perfect match and access to his account is granted.

Restrictions: The program does not allow the users to select the background white spaces as password characters and thus displays "Invalid selection" message for the same in CLCD. It also prompts the user to select the password area again. This program allows the user to select a minimum of one area and a maximum of four areas as password. Thus, after every area selected, it prompts the user as to whether he wants to select the next area as his password. Whenever a user tries to set a password that is more than four characters in length, an error message is displayed and the program considers the first four areas selected by the user as the password. Once the two level of password setting is completed, a success message appears on the CLCD after which the user enters the verification phase. The user is also given the option to change password after every successful login.

RESULTS AND DISCUSSION

The maximum password spaces that can be supported by the scheme can be calculated as follows:

Size of the image = $m \times n$ and Size of grid square = $r \times s$

No. of non-overlapping grid squares available in the image, 'g'= $(m \times n)/(r \times s)$

No. of passwords spaces when all the users are allowed to select the password length 'k' (k-clicks) in a image with 'g'grids is given as g^k (1)

Total passwords spaces obtainable when the users are allowed to select the minimum password length k = 1 and maximum length of k in a image with 'g'grids where, $k \geq 1$ can be given as: $g^1+g^2+\ldots+g^k$ (2)

The sample results for pool of 4 images with sizes 100×100 each and selected image displayed in size 200×200 by the magnification factor of 2 with grid square (selection box) of size 40×40 in its top right corner displayed in the GLCD screen during the first stage, area selection in the second stage and final password confirmation message obtained in CLCD at the second stage are shown in Fig. 5.

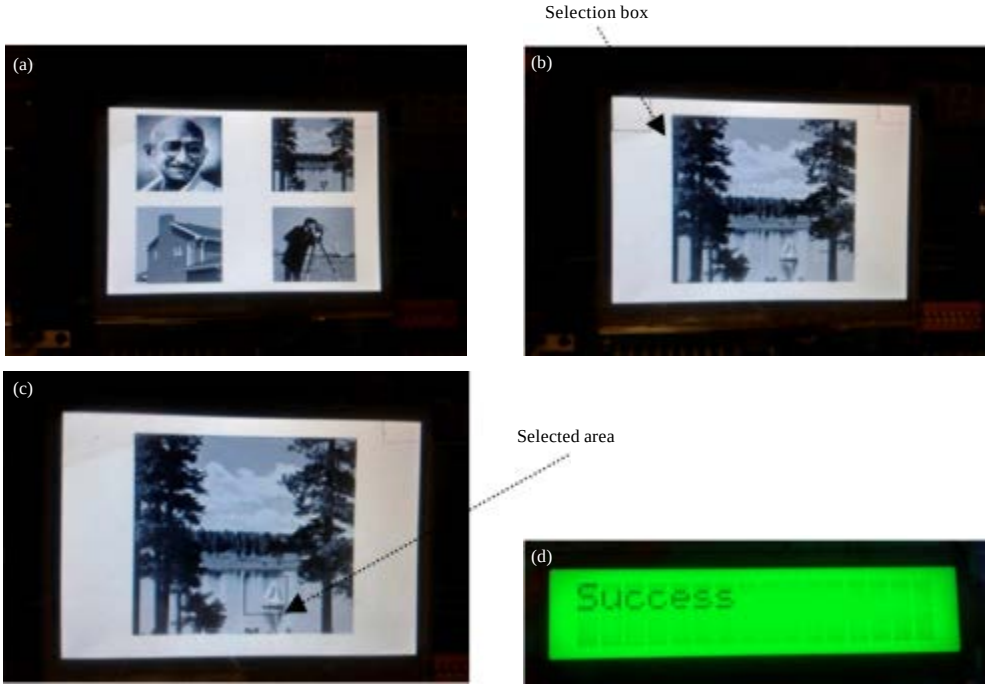

Fig. 5(a-d): (a) Image pool in first stage, (b) Selected image in magnified scale with selection box, (c) Area selection in magnified image and (d) Message after password matching

Features and factors of improvement: The popular pattern lock feature can only be used in smart phones and tablets i.e., where a touch screen is being used and so does not extend to basic phones. The image based password authentication scheme proposed here brings a solution to the problem and helps strengthen the security even in a low cost device with monochrome/colour display and keypad. Here, this method used an application level embedded processor that can access huge memory to support the image and password storage to manage multiple users. The use small sized images of grey format, reduces the memory requirement. The magnified display of selected images during the area selection process increases the potential number of areas that can be selected which in turn elevates the security and the possible number of users. Though this method fix a restriction on the maximum length of the password, the flexibility given by the algorithm for the users to select variable length for their password helps in accommodating as many users as possible. Reduction in the original size of the images stored can help minimizing memory requirement. More users can be lodged with few images by means of increasing the image magnification factor. The size of the selection box can be made still smaller which will increase the number of areas that can be selected. This in turn increases the number of password combinations and reduces threat of attack to a great extent. When the number of selection areas that a user can choose from increases, the system becomes capable of supporting a larger pool of users with non-overlapping passwords with a restriction on maximum number of areas to be selected as password.

Table 1 compares the use of various features and mechanisms between the proposed method and previous method (Wiedenbeck *et al*., 2005). The Table 2 shows a significant improvement in

Table 1: Comparison result on feature/mechanism of the proposed method

Features/mechanism	Pass points on embedded devices (proposed)	Pass points on PC (Wiedenbeck *et al.*, 2005)
Target platform	ARM Cortex-A8	PENTIUM- IV PC
Screen size used	3.5"	19"
Input device	Keypad	Mouse
Target application	Password authentication in standalone	
Embedded devices	Password authentication in PC	
Factors deciding the password	Image size	Image size
space	Grid square size	Grid square size
	Password length (max)	Password length (max)
	Magnification factor	
Click points	Square well defined boundaries	Grid square boundaries with tolerance
Preliminary verification	Yes (image selection from the pool	No (single user image will be displayed)
before actual password entry	of images displayed on the screen)	
Password length	Variable (within the maximum	Fixed (all users must have equal length)
	specified by the scheme)	
Grid square size	Variable	Variable
Magnification factor	Variable (selectable by	Fixed (pre-determined in the scheme)
	user from available options)	

Table 2: Comparison on password space and memory requirement

Method	Image size	Image type	Memory required for image storage	Grid square size	Magnification factor	No. of grid squares	Maximum/minimum length of password	Size of password space (given by Eq. 1 and 2)
Proposed	100×100	Gray	9.76 KB	20×20	2	100	4/1	101.1001×10^{5}
Wiedenbeck *et al.* (2005)	100×100	RGB	29.29 KB	20×20	1	50	4/4	6.25×10^{5}

size of the password space and reduction in the space required for image storage by the proposed method in comparison with earlier method by Wiedenbeck *et al.* (2005) when using equal sizes of image, grid square and maximum password length (clicks).

CONCLUSION

In the proposed image and area selection scheme the pixel values of the selected areas in the magnified image are compared for password authentication. This makes the image magnification factor used in the scheme to act as a novel security key. Thus, this scheme combines both authentication at image level and authentication at area level inside an image (pixel values) to provide a high level of security on embedded platform. Using the keypad and GLCD for the password selection makes the scheme also suitable for low end embedded devices for single user authentication without much demand on memory.

ACKNOWLEDGMENT

The authors wish to acknowledge SASTRA University for providing infrastructural support to carry out this study.

REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013a. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013b. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013c. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013e. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013f. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013g. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013h. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013i. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013j. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognit., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Hashemi, M., N. Ithnin and R. Pakdel, 2012. Multi touch graphical password: Usability features. Asian J. Applied Sci., 5 : 20-32.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Janakiraman, S., S. Rajagopalan, K. Thenmozhi, H.N. Upadhyay and J. Ramanathan *et al.*, 2013. Captivating CODEC Stego (CCS): A cover on camouflage. Res. J. Inform. Technol., 5: 160-170.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

Meng, Y., 2012. Designing click-draw based graphical password scheme for better authentication. Proceedings of the 7th International Conference on Networking, Architecture and Storage, June 28-30, 2012, Xiamen, Fujian, pp: 39-48.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013a. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Convolution and viterbi EN (DE) coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013c. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013d. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan, 2014a. Rubik's cube blend with logistic map on RGB: A way for image encryption. Res. J. Inform. Technol., 6: 207-215.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014b. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014h. Coded crypted converted hiding (C^3H)-a stego channel. J. Applied Sci., 14: 1786-1797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014i. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014j. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Amirtharajan, R.S. Janani, K. Thenmozhi and J.B.B. Rayappan, 2014k. Multi (Carrier+Modulator) adaptive system-an anti fading stego approach. J. Applied Sci., 14: 1836-1843.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014l. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhunisha, K. Thenmozhi and R. Amirtharajan, 2014m. Image Zoning? encryption. Res. J. Inform. Technol., 6: 368-378.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012a. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and seek in silicon: Performance analysis of Quad block Equisum Hardware Steganographic systems. Procedia Eng., 30: 806-813.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014. Modeling combo PR generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

Tazawa, H., T. Katoh, B.B. Bista and T. Takata, 2010. A user authenticaion scheme using multiple passphrases and its arrangement. Proceedings of the International Symposium on Information Theory and its Applications, October 17-20, 2010, Taichung, pp: 554-559.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inform. Syst. Software Applic., 270: 212-221.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013a. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013b. A graph theory practice on transformed image: A random image steganography. Sci. World J. 10.1155/2013/464107

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud., 63: 102-127.