Electronic Micro Banking System for Remote and Rural Areas Using Arm Processor

T. Deepa[1] G. Sathishkumar[2]
[1]M.E Student [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Kalaignar Karunanidhi Institute of Technology

Abstract— Today, banks have realized that their next huge customer base is not in the urban setting but in the often-neglected rural areas. Infrastructure of rural areas is not as rich as urban counterparts. Reaching the people in rural areas is not so easy compared to urban areas. To create a secured handheld doorstep banking system, it is a mobile banking system which is used to provide much secured and easy of banking service for the people from rural areas and remote villages. The transaction simply cannot be done by inserting card and PIN number, it also requires fingerprint identification and OTP for every transaction to improve more secure. Once this kind of systems is launched by banks, the customer can have easy banking services with the bank where the customer is member. This system is used as banking machine with connected to banking server which is carried by the banking person who is authorized by the respective bank. Also the money transferring can be done by the same banking person.

Key words: Global Positioning System, Global System for Mobile Communication, Smart SD memory card, Smart Card Reader, Fingerprint authentication, Panic Button, Touchscreen Controller, LPC 1764 controller and ARM Cortex M3 processor

I. INTRODUCTION

In today's real time modern industrialized world security systems place a vital role. Simple tasks like going to the ATM and withdrawing money make people in villages miss their working hours and, as a result, lose a significant part of their income as well. Hence there is a need to design a system that helps those people who can't leave their business premises for banking transactions. Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated the money will be converted at an official exchange rate. Thus, ATMs often provide the best possible exchange rates for foreign travelers, and are widely used for this purpose.

A. Personal Identification Number (PIN):

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date or CVVC. Authentication is provided by the customer entering a Personal Identification Number (PIN).

B. Security:

Security, as it relates to ATMs, has several dimensions. ATMs also provide a practical demonstration of a number of security systems and concepts operating together and how various security concerns are dealt with. There is a computer industry security view that general public desktop operating systems have greater risks as operating systems for cash dispensing machines than other types of operating systems like Real-Time Operating Systems (RTOS).

II. RELATED WORK

The Personal Identification Number (PIN) is a common user authentication method used in various situations, such as in withdrawing cash from an Automatic Teller Machine (ATM), approving an electronic transaction, unlocking a mobile device, and even opening a door. However, a critical issue with PINs is that they are vulnerable to Shoulder-Surfing Attacks (SSAs). In other words, anyone who observes the logon procedure by looking over a user's shoulder can easily memorize his/her PIN. This kind of attack is an actual threat to the use of PINs because there are many cases in which PINs are used in public places and for financial transactions.

A. Shoulder-Surfing Resistant Pin-Entry Methods:

Most of the known shoulder-surfing resistant PIN-entry methods. The capacity of short-term memory and the real-time processing performance of a human are very limited. In these methods, the user is provided with random challenges and is asked to input appropriate responses, where the challenge-response tasks are designed in an asymmetric manner so that the legitimate user may answer the challenges easily while the amount of information carried in the challenge-response pairs exceeds the cognitive capability of a human observer who does not know the PIN. In addition, because the challenges involve some randomness, there are many possible input sequences for the same PIN, and a simple replay of the user's input does not allow an attacker to pass the PIN-entry test.

To unlock a smart phone, defining a new PIN space such as the android pattern lock is not a problem. However, if it is to be used for more generic purposes, compatibility matters. Changing the PIN space for a bank account will affect all ATMs and PIN pads, as well as existing software. The existing method should provide only a new interface and the traditional PIN set should remain unchanged. In this way, an ATM may display two options so that a user can choose between a regular PIN pad and the new interface.

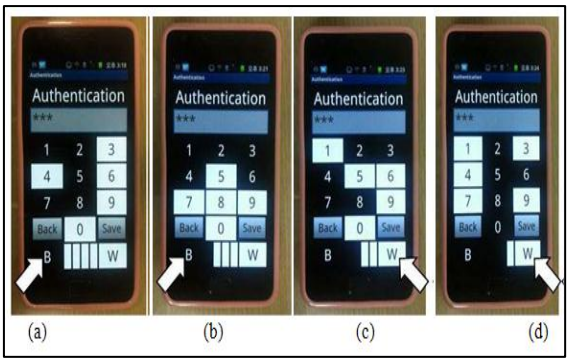

Fig. 1: An Example Round To Input 1 In IOC, Where The User Enters Black, Black, White And White In Sequence (A) Stage 1 (B) Stage 2 (C) Stage 3 (D) Stage 4

The Figure 1 shows an example of the Immediate Oracle Choice (IOC) variant is the most practical method. The principal idea of IOC is to display digits as two distinct sets by randomly coloring half of the keys black and the other half white. The user recognizes the set in which the current PIN digit is and presses one of the two keys representing each set. To uniquely determine a PIN digit, four stages are required. Thus, a common 4-digit PIN requires 16 stages.

B. PIN Entry Methods:

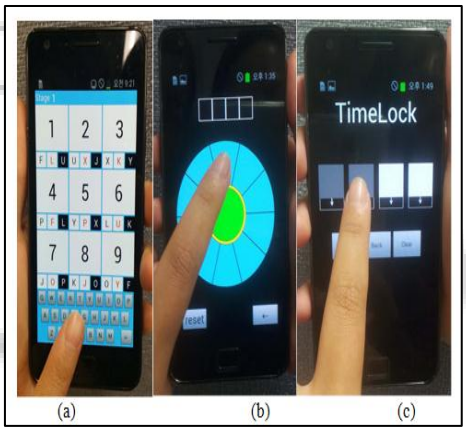

Fig. 2: PIN Entry Methods (A) Colorpin (B) Phonelock (C) Timelock

In Figure 2(a) shows an implementation of ColorPIN. It redefines a PIN such that a PIN digit is a combination of a number and a color, where the color is selected from black, red, and white. While the original version used a separate commercial PC keyboard, so that the challenge and the keypad fit a single screen.

For each digit of a PIN, the user is asked to find the letter colored with the PIN color under the PIN number. In the example of Figure 2(a), the user inputs the first PIN digit 1, black by typing F, the black-colored letter under 1. It should be noted that ColorPIN essentially enlarges the PIN set and asks a user to remember more information for a PIN. Consequently, it is not compatible with a regular PIN.

In Figure 2(b) shows the Phone Lock. It displays a graphical wheel with ten sectors. In the audio version of Phone Lock, when a user touches any sector, the phone tells the user a random number between zero and nine, example, three. The user then scrolls the circle, touching adjacent items in turn, hearing four, five, six, etc. in turn. It is also possible to jump to a more distant number. Finally, when the user encounters the target, s/he inputs it by dragging that item to the center of the wheel and releasing the screen. For security, the position of the numbers is randomized for each PIN digit, and the audio signals are transmitted through an isolated channel.

In Figure 2(c) shows the TimeLock. It only uses PIN digits among 1,2,3,4,5. Then, to obtain sufficient resistance against guessing attacks, an additional factor, specifically, the order in which the four buttons are pressed is defined to be a part of the PIN. This makes time lock partially vulnerable to even a single shoulder-surfing attack and incompatible with the standard PIN.

III. PROPOSED BANKING DESIGN

Today, banks have realized that their next huge customer base is not in the urban setting but in the often-neglected rural areas. However, reaching this customer base is not so easy, primarily because the rural areas are not as infrastructure-rich as their urban counterparts. Simple tasks like going to the ATM and withdrawing money make people in villages miss their working hours and, as a result, lose a significant part of their income as well. Hence there is a need to design a system that helps those people who can't leave their business premises for banking transactions.

The main idea of micro-bank system is that the bank should employ special persons who are licensed as the Business Correspondents (BC) to carry a micro bank machine with them. Each BC will be allocated to a particular micro-bank machine.

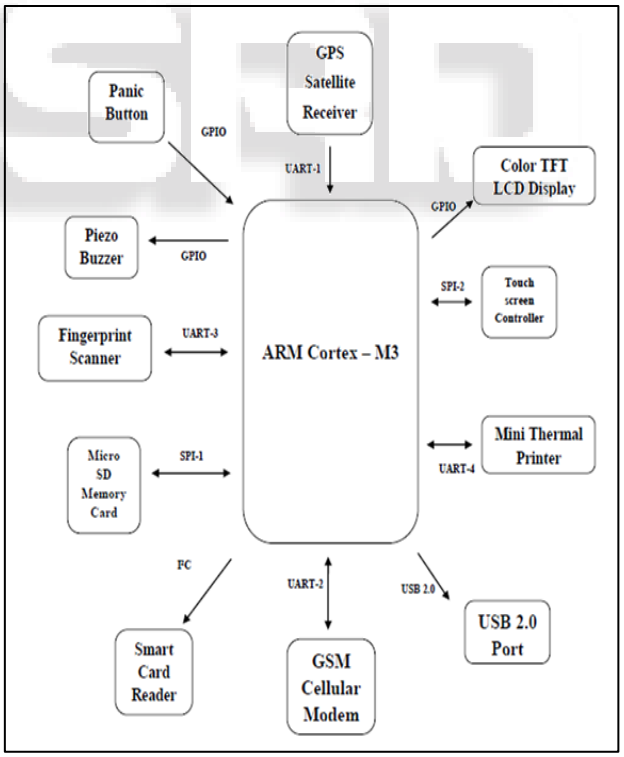

Fig. 3: Doorstep Banking System

Figure 3 shows the Doorstep Banking System, the project aim is to create a secured handheld doorstep banking system called Micro-Bank machine to provide service to the customers in rural areas and remote places such as villages. The system can also be operated within and beyond the normal banking hours. The primary aim of the handheld machine is to provide banking services such as cash

withdrawals and cash deposit without the person ever going to a bank.

A. Arm Cortex-M3:

The ARM Cortex family of processors provides a standard architecture to address the broad performance spectrum required by these diverse technologies. The ARM Cortex family includes processors based on the three distinct profiles of the ARMv7 architecture; the A profile for sophisticated, high-end applications running open and complex operating systems; the R profile for real time systems; and the M profile optimized for cost-sensitive and microcontroller applications.

Table 1 shows the comparison between ARMTDMI-S and CORTEX-M3 processor. The Cortex-M3 processor is a 32-bit processor, with a 32-bit wide data path, register bank and memory interface. There are 13 general-purpose registers, two stack pointers, a link register, a program counter and a number of special registers including a program status register. The Cortex-M3 core contains a decoder for traditional Thumb and new Thumb-2 instructions, an advanced ALU with support for hardware multiply and divide, control logic, and interfaces to the other components of the processor.

Features	ARM7TDMI-S	Cortex-M3
Architecture	ARMv4T(Von Neumann)	ARMv7-M (Harvard)
ISA support	Thump / ARM	Thump / Thump-2
Pipeline	3- stage	3 stage + branch speculation
Interrupt latency	24-42 cycles	12 cycles
Sleep modes	None	Integrated
Memory protection	None	8 region memory protection unit
Interrupts	FIQ / IRQ	NMI + 1 to 240 physical interrupts
Dhrystone	0.95 DMIPS/MHz	1.25 DMIPS/MHz
Power consumption	0.28 mW/ MHz	0.19 mW /MHz
Area	0.62m^2 (Core only)	0.86m^2 (core & peripherals)*

Table 1: ARM7TDMI-S AND CORTEX-M3 COMPARISON (100mhz Frequency On TSMC 0.18G)

B. LPC 1764 Microcontroller:

The LPC1769/68/67/66/65/64/63 is ARM Cortex-M3 based microcontrollers for embedded applications featuring a high level of integration and low power consumption. The peripheral complement of the LPC1769/68/67/66/65/64/63 includes up to 512 kB of flash memory, up to 64 kB of data memory, Ethernet MAC, USB Device/Host/OTG interface, 8-channel general purpose DMA controller, 4 UARTs, 2 CAN channels, 2 SSP2 controllers, SPI interface, 3 I2C-bus interfaces, 2-input plus 2-output I2S-bus interface, 8-channel 12-bit ADC, 10-bit DAC, motor control PWM, Quadrature Encoder interface, four general purpose timers, 6-output general purpose PWM, ultra-low power Real-Time Clock (RTC) with separate battery supply, and up to 70 general purpose I/O pins. The LPC1768/67/66/65/64/63 operates at CPU frequencies of up to 100 MHz. The LPC1769 operates at CPU frequencies of up to 120 MHz.

C. Fingerprint Authentication:

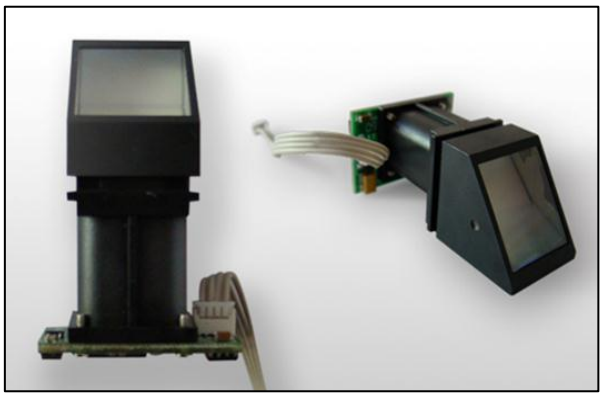

Fig. 4: Fingerprint Scanner

Figure 4 represents the Fingerprint Scanner. It includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library.

IV. FLOW OF CONTROL

The customer who needs micro-bank service must call the customer care division of the bank and inform whether he wants to withdraw/deposit money. The bank server will choose the appropriate micro-bank unit and will send a query message to that. The micro-bank machine should reply with an acknowledge message when it sees the bank query. The server will then dispatch a message about the details of the customer including his account balance. The message also contains a One-Time Password (OTP) to the micro-bank machine that is allocated for that transaction. The same OTP is also sent to the customer mobile. The micro-bank system is always connected to the central banking server using GSM communication.

The BC has to enter a touch screen password using the QVGA Touch screen TFT LCD Display in order to physically unlock the screen. The BC can unlock the screen anytime he wishes, but like a smart phone, the screen will automatically get locked after a fixed (1 min) period of inactivity. Each micro-bank machine is permitted to be used only within a particular region in order to prevent an illegal usage out of that region and thus the device is locked in terms of its position. The current location of the device is tracked from GPS signals and the position is constantly verified with the region previously indicated by the server. This also helps to keep track of the location of the micro-bank machine in the event of misuse or a theft condition. An out of region condition brings the device to a halt and the error info is sent to the bank server. On meeting the customer, the BC will verify the OTP on his device with that of the customer mobile. The customer needs to verify the OTP in his mobile against the micro-bank device. This mutual verification will authenticate both parties, and the transaction can now be started.

The identity of BC is first verified using a built in Fingerprint Scanner. This is to ensure that the device has not been ended up in the wrong hands. The device stores the

fingerprint of the BC as well as the entire customer base in that region in its database. Now the customer will be asked to enter his fingerprint. It is also verified. This ensures the authenticity of each party.

Once the fingerprint verification is done, BC needs to enter a 4-PIN secret number on the touch screen keypad shown in the TFT display. The customer is then allowed to insert his smartcard into its slot. The device has a Smartcard Reader functionality that grabs the details such as the customer ID, customer name and account number information from the smartcard and will be verified against the server sent message. The smartcard is a permanent EEPROM memory that has got the customer details stored. Now it the customers turn to enter his 4-PIN secret number on the touch screen keypad, similar to that on the ATM machines. Once the PIN number is entered and verified, the machine will unlock the device for the final step in the transaction. The customer will now be asked to enter the amount to be withdrawn on the touch screen display and the BC will dispatch the money to the customer. The customer must make a confirmation by typing the 4-PIN secret number again. The device checks this and sends a "money paid" message to the bank server.

If the customer wants to deposit the money, he/she needs to enter the amount as previously described and the cash should be handed over to the BC. Now the BC will enter the 4-PIN secret number again. The device verifies this and sends a money collected message to the bank server. The device uses a Mini-Thermal Printer to automatically print the receipt as soon as the message has been sent. The bank server immediately sends a Transaction over message to the machine indicating the completion of the entire transaction.

V. RESULT AND DISCUSSION

Figure 5 shows the output of doorstep banking system. The machine is intended for rural area, power will be not be easily available in remote places. So, the system operates with battery power.

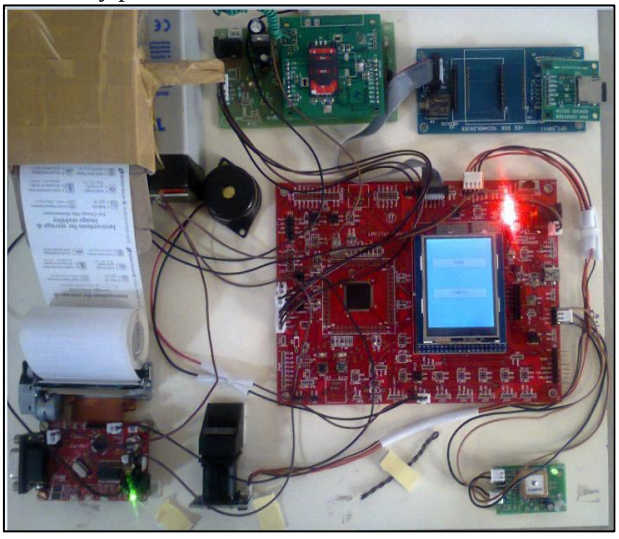

Fig. 5: Output of Doorstep Banking System

Low power 32-bit ARM Cortex-M3 microcontroller enables highly deterministic operation using battery power only. Initially, store the fingerprint in configure mode. Then starts the process in demo mode. Demo mode deals with record and retrieve the data. Data record has two types of modes: Offline and Online.

Both offline and online mode has indoor and outdoor operations. Offline mode transactions are stored in memory card. Online mode transactions are based on feasibility of GSM connections. ARM Cortex-M3 supports Harvard architecture and can be operated in battery power supply. The location of the machine is tracked by using GPS module. Printer is used to print the transaction details of the customer. Panic button feature prevents a money theft from BC.

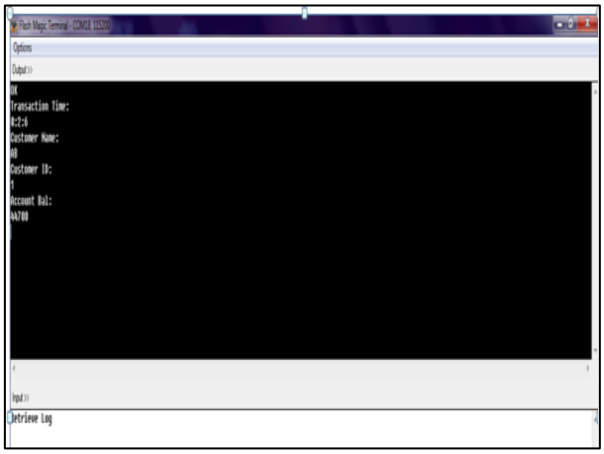

Fig. 6: Output of Data Retrieve

Figure 6 shows the output of Data Retrieve. Flash magic is used to retrieve the offline mode transactions details of the customer via USB port. It would save people time and money as they need not leave the place where they are. The system can also be operated within and beyond the normal banking hours. Offline mode is available to operate it in completely remote areas where 6 even GSM communication is not available. Storage capacity of fingerprint scanner is in greater than 250. But can be extended to more than thousand if required. Panic button feature prevents a money theft from BC. Because the machine is intended for rural area, power will be not be easily available in remote places. So, the system operates with battery power.

VI. CONCLUSION

This is a real-time based paper which tells that there is a handheld doorstep banking system for the people in rural areas. This system is a very easy procedure and support more secured operations. This system is helps to avoid excess transaction fees. This is more systematic approach for the people in remote areas and it would save people time and money. The security system ensures more reliable for the people and give a very good protection of the consumers curbing theft. As this is protected by the panic button hence can send information to the police station and bank if any unwanted or forced entry inside the area and can protect the business correspondent and consumers in the most efficient way.

REFERENCES

[1] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014.

[2] C. S. Kim and M.-K. Lee, "Secure and user friendly PIN entry method,"in Proc. 28th Int. Conf. Consum. Electron., 2010, p. 5.1–1.
[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. CCS, 2004, pp. 236–245
[4] G. T. Wilfong, "Method and apparatus for secure PIN entry," U.S. Patent 5 940 511, May 30, 1997.
[5] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proc. SOUPS, 2007, pp. 13–19.
[6] J. Thorpe, P. van Oorschot, and A. Somayaji, "Pass-thoughts: Authenticating with our minds," in Proc. NSPW, 2005, pp. 45–56.
[7] A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN entry through indirect input," in Proc. CHI, 2010, pp. 1103–1106.
[8] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. SOUPS, 2006, pp. 56–66.
[9] A. Bianchi, I. Oakley, V. Kostakos, and D.-S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in Proc. TEI, 2011, pp. 197–200.
[10] A. Bianchi, I. Oakley, and D.-S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry," Interact. Comput., vol. 24, no. 5, pp. 409–422, 2012.
[11] M. G. Kuhn. (1997). Probability Theory for Pickpockets, ee-PIN Guessing Online]. Available: http://www.cl.cam.ac.uk/~mgk25/
[12] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proc. 13th Conf. USENIX Security Symp., 2004, pp. 151–164
[13] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking PINs," in Financial Cryptography (LNCS), New York, NY, USA: Springer-Verlag, 2012, pp. 25–40
[14] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. NDSS, 2012, pp. 50–58.
[15] R. Kuber and W. Yu, "Tactile vs graphical authentication," in EuroHaptics (LNCS). New York, NY, USA: Springer-Verlag, 2010, pp. 314–319.
[16] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication usable in front of prying eyes," in Proc. CHI, 2008, pp. 183–192.
[17] A. D. Luca, E. von Zezschwitz, and H. Hußmann, "Vibrapass: Secure authentication based on shared lies," in Proc. CHI, 2009, pp. 913–916.
[18] A. Bianchi, I. Oakley, J. K. Lee, and D.-S. Kwon, "The haptic wheel: Design & evaluation of a tactile password system," in Proc. CHI, 2010, pp. 3625–3630.
[19] A. Bianchi, I. Oakley, and D.-S. Kwon, "The secure haptic keypad: A tactile password system," in Proc. CHI, 2010, pp. 1089–1092.
[20] A. Bianchi, I. Oakley, and D.-S. Kwon, "Spinlock: A single-cue haptic and audio PIN input technique for authentication," in HAID (LNCS). New York, NY, USA: Springer-Verlag, 2011, pp. 81–90.
[21] A. Bianchi, I. Oakley, and D.-S. Kwon, "Open sesame: Design guidelines for invisible passwords," IEEE Comput., vol. 45, no. 4, pp. 58–65, Apr. 2012.
[22] M. Bell and V. Lovich, "Apparatus and methods for enforcement of policies upon a wireless device," U.S. Patent 8 254 902, Aug. 12, 2012.
[23] G. A. Alvarez and P. Cavanagh, "The capacity of visual short-term memory is set both by visual information load and by number of objects," Psychol. Sci., vol. 15, no. 2, pp. 106–111, 2004.

