Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (3): 154-165, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.154.165

LabVIEW Based PIN Hider on ATM Cards: A Transform Domain Secret Concealment Approach

Sundararaman Rajagopalan, Siva Janakiraman, B. Swaminath, Har Narayan Upadhyay, K. Thenmozhi and Rengarajan Amirtharajan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

Corresponding Author: Sundararaman Rajagopalan, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

ABSTRACT

The day to day advancements in science and technology resulted in enormous data transaction and demand for secure communication and e-banking are not an exception. The usage of ATMs for cash withdrawal and other transaction related works is massive. Looking at the elements required by a customer for ATM utility, the debit card and secure PIN are being sent separately by postal service to the customers of many banks for increased security. However, tampering is always possible because of the unique mode of sending the both card as well as PIN authentication to the customers. Here we suggest an alternative method to enhance the security with respect to debit card and PIN communication to the customers with LabVIEW based transform domain steganography approach where the PIN will be hidden in the scanned Debit card image with the help of Discrete Cosine Transform (DCT) and swapping algorithm. This transformed image will be e-mailed to the customers. Proper retrieval algorithm will be used by the concerned customers to reveal the secret PIN authentication. Histogram report, error metrics like MSE and PSNR have also been discussed in this study for sample ATM debit card image.

Key words: Steganography, ATM card security, random image steganography, transform domain steganography, DCT based steganography, LabVIEW based steganography

INTRODUCTION

While every walk of human life needs some sort of information for necessities, the concern is how safe the data is reaching the other end. While sitting peacefully and thinking about the pride of technology, one must understand the effects caused by the so called innovations and breakthroughs. In fact, breakthroughs have become breaking elements through the self border i.e., Lakshman Rekha drawn to protect one's privacy. But sitting time will not help in revamping the system back, as the heavy onus pressures us to run and stop incoming threats. Over the period, cryptography, steganography and watermarking are providing helping hand to face the threats of information theft. Information hiding (Cheddad *et al*., 2010; Amirtharajan and Rayappan, 2012a-e, 2013; Amirtharajan *et al*., 2013a-j; Janakiraman *et al*., 2012a, b, 2014a, b; Zhao and Luo, 2012; Mohammad *et al*., 2011; Salem *et al*., 2011; Ramalingam *et al*., 2014a, b; Thien and Lin, 2003; Luo *et al*., 2011) methods have been implemented in both spatial as well as transform domains.

As for as, spatial image steganography is concerned LSB substitution (Chan and Cheng, 2004), random image steganography (Amirtharajan *et al*., 2012b; Thanikaiselvan *et al*., 2012a-c, 2013a, b), pixel differencing (Wu and Tsai, 2003; Zhang and Wang, 2004), pixel indicator based approaches (Janakiraman *et al*., 2012a, b, 2013) and other adaptive (Amirtharajan and Rayappan, 2012a, c) have been experimented in the past. DCT (Wong *et al*., 2007; Qi and Wong, 2005) based steganography is one of the earlier transform domain based proposed methods. Also wavelet based (Amirtharajan and Rayappan, 2012d) approaches, FPGA based hardware stego approaches (Rajagopalan *et al*., 2012a, b, 2014a-d; Rajagopalan and Upadhyay, 2011; Janakiraman *et al*., 2014a, b), firmware and OFDM based information security (Thenmozhi *et al*., 2012; Praveenkumar *et al*., 2012a, b, 2013a, b, 2014a-j) have also been forming the part of security algorithms.

Bank transactions have seen various advancements in the past decade. Written work has been almost reduced with the emerging technologies in the IT sector that has extended the helping hand for banking sector. Regarding the money transactions, almost every customer uses debit card for money withdrawals from the ATMs. In this approach, secure communication of secret PIN to the customers to access ATM cards has been discussed. The proposed method uses DCT based transform domain steganography, where the PIN bit embedding is done with a swapping coefficients algorithm.

PROPOSED METHODOLOGY

Let, I(x, y) be the RGB image of a sample ATM card with the subsets of R, G and B coordinates, i.e., {IR(x,y), IG(x,y), IB(x,y) } ∈ I(x,y). The ATM card image considered here is rectangular in shape such that number of rows in the image is less than the number of columns. The image resolution is chosen by keeping in mind that the image will have finite 'N' number of 8×8 blocks. The proposed algorithm is based on discrete cosine transform where the secret PIN hiding happens in some of the 16 pairs of locations of the 8 × 8 blocks.

The DCT computing I, jth element of DCT of an image can be calculated by the following Eq. 1:

$$DCT(i,j) = \frac{1}{\sqrt{2N}} f(i) f(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$
$$f(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{if } u > 0 \end{cases} \quad (1)$$

Let us consider a block of 8×8 pixels 'A' from one of the R, G, B layers of ATM card sample image considered here:

$$A = \begin{pmatrix} 149 & 132 & 115 & 111 & 118 & 126 & 132 & 136 \\ 206 & 171 & 143 & 145 & 155 & 149 & 131 & 120 \\ 252 & 197 & 159 & 172 & 187 & 165 & 126 & 102 \\ 238 & 181 & 147 & 168 & 187 & 164 & 126 & 108 \\ 187 & 147 & 129 & 151 & 170 & 160 & 145 & 143 \\ 140 & 128 & 125 & 139 & 154 & 161 & 167 & 173 \\ 114 & 123 & 127 & 128 & 138 & 156 & 165 & 163 \\ 103 & 122 & 127 & 117 & 123 & 144 & 148 & 135 \end{pmatrix}$$

As an initial step, threshold value of 128 has to be subtracted from each of the 8×8 block cover pixels, therefore:

$$B = A - 128 = \begin{pmatrix} 21 & 4 & -13 & -17 & -10 & -2 & 4 & 8 \\ 78 & 43 & 15 & 17 & 27 & 21 & 3 & -8 \\ 124 & 69 & 31 & 44 & 59 & 37 & -2 & -26 \\ 110 & 53 & 19 & 40 & 59 & 36 & -2 & -20 \\ 59 & 19 & 1 & 23 & 42 & 32 & 17 & 15 \\ 12 & 0 & -3 & 11 & 26 & 33 & 39 & 45 \\ -14 & -5 & -1 & 0 & 10 & 28 & 37 & 35 \\ -25 & -6 & -1 & -11 & -5 & 16 & 20 & 7 \end{pmatrix}$$

The DCT of block B can be computed by the following Eq. 2:

$$D = MBM^T \tag{2}$$

where, M is a DCT matrix and M^T is the transpose of M.

$$M = \begin{pmatrix} 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 \\ 0.4904 & 0.4157 & 0.2778 & 0.0975 & -0.0975 & -0.2778 & -0.4157 & -0.4904 \\ 0.4619 & 0.1913 & -0.1913 & -0.4619 & -0.4619 & -0.1913 & 0.1913 & 0.4619 \\ 0.4157 & -0.0975 & -0.4904 & -0.2778 & 0.2778 & 0.4904 & 0.0975 & -0.4157 \\ 0.3536 & -0.3536 & -0.3536 & 0.3536 & 0.3536 & -0.3536 & -0.3536 & 0.3536 \\ 0.2778 & -0.4904 & 0.0975 & 0.4157 & -0.4157 & -0.0975 & 0.4904 & -0.2778 \\ 0.1913 & -0.4619 & 0.4619 & -0.1913 & -0.1913 & 0.4619 & -0.4619 & 0.1913 \\ 0.0975 & -0.2778 & 0.4157 & -0.4904 & 0.4904 & -0.4157 & 0.2778 & -0.0975 \end{pmatrix}$$

For the 8×8 cover block considered here, the DCT coefficients after performing two matrix multiplications as given in Eq. 2 will be:

$$D = \begin{pmatrix} 159.792 & 44.0375 & 20.2891 & 79.7696 & 24.2564 & -0.3456 & -0.0162 & -0.3147 \\ 35.5743 & 107.827 & 13.9867 & 38.3195 & 25.7803 & -0.3556 & 0.1716 & -0.068 \\ -98.1953 & -65.6127 & 15.7534 & -47.9744 & -39.6939 & -0.3991 & 0.051 & 0.069 \\ -42.1996 & -85.5209 & 21.5592 & -29.3982 & 0.1282 & 0.3056 & 0.088 & 0.3314 \\ -36.5096 & 0.3841 & 0.1913 & 0.0373 & 0.5 & -0.1876 & 0.4619 & 0.2566 \\ 0.3716 & -0.419 & -0.4743 & 0.4795 & -0.007 & -0.1165 & -0.3751 & -0.1704 \\ 0.0876 & 0.1238 & 0.3 & -0.3062 & 0.2072 & 0.2193 & -0.5066 & 0.2173 \\ -0.069 & 0.1077 & 0.0076 & 0.4998 & 0.3608 & 0.4071 & -0.1195 & 0.1827 \end{pmatrix}$$

The quantization of D can be done by dividing each element of D by the corresponding quantization matrix element and rounding it to the nearest integer as following in Eq. 3:

$$C(m,n) = \text{Round}\,(D(m,n)/Q_{90}(m,n)) : m,n \in \{1,2,3,4,5,6,7,8\} \tag{3}$$

where, C is the matrix of quantized and rounded coefficients C(m, n), Q_{90} is the quantization matrix which gives best quality image but with low compression. The quantization matrix Q_{90} considered in this study is:

$$Q_{90} = \begin{pmatrix} 3 & 2 & 2 & 3 & 5 & 8 & 10 & 12 \\ 2 & 2 & 3 & 4 & 5 & 12 & 12 & 11 \\ 3 & 3 & 3 & 5 & 8 & 11 & 14 & 11 \\ 3 & 3 & 4 & 6 & 10 & 17 & 16 & 12 \\ 4 & 4 & 7 & 11 & 14 & 22 & 21 & 15 \\ 5 & 7 & 11 & 13 & 16 & 12 & 23 & 18 \\ 10 & 13 & 16 & 17 & 21 & 24 & 24 & 21 \\ 14 & 18 & 19 & 20 & 22 & 20 & 20 & 20 \end{pmatrix}$$

After quantizing and rounding off as per Eq. 3:

$$C = \begin{pmatrix} 53 & 22 & 10 & 27 & 5 & 0 & 0 & 0 \\ 18 & 54 & 5 & 10 & 5 & 0 & 0 & 0 \\ -33 & -22 & 5 & -10 & -5 & 0 & 0 & 0 \\ -14 & -29 & 5 & -5 & 0 & 0 & 0 & 0 \\ -9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Now, this C contains 44 zeros out of 64 coefficients which means 68.75% of the 8×8 block is occupied by zeros which indicate the compression done. The next step is to hide the PIN into the blocks of quantized DCT. The data hiding can be implemented on the selected ATM card RGB image based on the following parameters:

- T: Trilayer parameter which may take any one value from {1, 2, 3} ⇒ {R, G, B}
- {B}: Set of 16 blocks to guide the embedding process
- {L}: L is a pair of quantized pixel locations to denote the PIN bit hiding in a specific block b⊂{B}

The trilayer parameter T will be decided by the LabVIEW based random number generator for which the VI is shown in Fig. 1.

The random numbers generated are between 1 and 3 to indicate the R, G and B layers. Figure 2 shows the random numbers generated for five trials displayed in the front panel 2D array. It has been observed that the number 1 occurs 26 times (6+4+5+6+5), 2 occurs 27 times (5+5+7+4+6) and 3 is present for 27 times (5+7+4+6+5) in five sample trials. Approximately 1, 2 and 3 occur nearly 1/3 times in each trial of 16 iterations.

Let us consider the C matrix is in the red layer and we assume that T = 1 which is generated by random number generation process. Also we consider that the C is a subset of {B}:C ⊂ {B}. The pair of quantized pixel locations to indicate the bit embedding is $\{R_3C_3, R_4C_1\} \in \{L\}$. Here R_3C_3 represent row 3-column 3 element and R_4C_1 indicates that of row 4-column 1. In the Matrix C, $R_3C_3 = 5$ and $R_4C_1 = -14$.

The proposed approach embeds one bit/8×8 block in order to enhance the security. From the 16 message bits set M = {m1 ... , m16}, a bit is embedded into an 8×8 block based on the following rules:

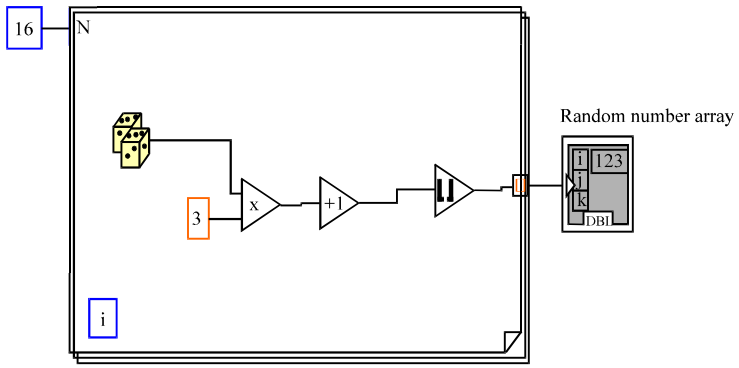

Fig. 1: Random number generation to decide the bit embedding layer 'T'

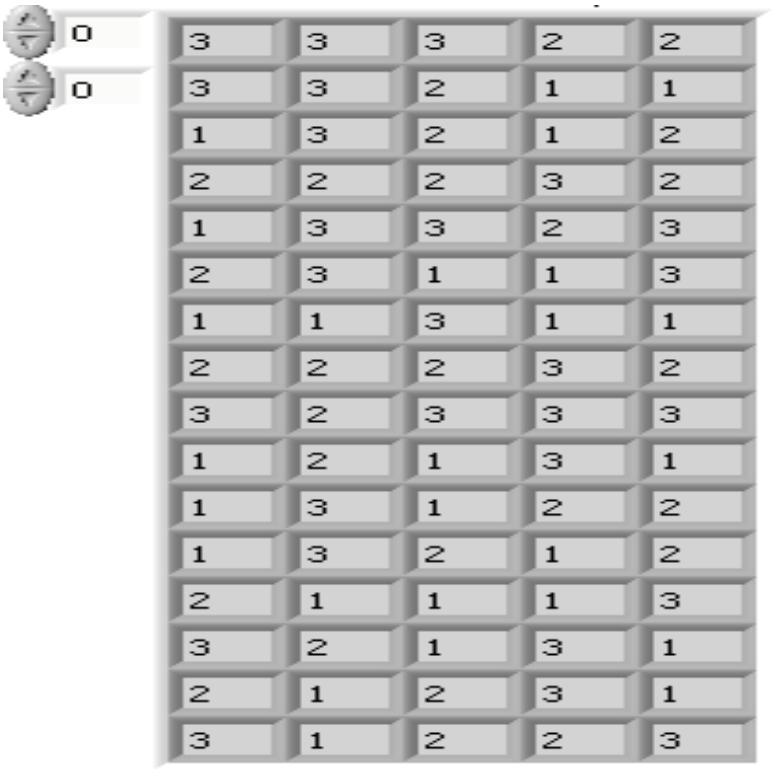

Fig. 2: Front panel indicator showing random number 2D array

Rule 1: If $m_i = 0$, then:

$$S(R_4C_1) = \left\{ \begin{matrix} R_4C_1 \text{ if } R_4C_1 < R_3C_3 \\ \text{Swap } R_4C_1 \text{ and } R_3C_3 \text{ if } R_4C_1 > R_3C_3 \end{matrix} \right\}$$

$$S(R_3C_3) = \left\{ \begin{matrix} R_3C_3 \text{ if } R_4C_1 < R_3C_3 \\ \text{Swap } R_4C_1 \text{ and } R_3C_3 \text{ if } R_4C_1 > R_3C_3 \end{matrix} \right\}$$

Rule 2: If $m_i = 1$, then:

$$S(R_4C_1) = \begin{Bmatrix} R_4C_1 \text{ if } R_4C_1 > R_3C_3 \\ \text{Swap } R_4C_1 \text{ and } R_3C_3 \text{ if } R_4C_1 < R_3C_3 \end{Bmatrix}$$

$$S(R_3C_3) = \begin{Bmatrix} R_3C_3 \text{ if } R_4C_1 > R_3C_3 \\ \text{Swap } R_4C_1 \text{ and } R_3C_3 \text{ if } R_4C_1 < R_3C_3 \end{Bmatrix}$$

These two rules are decisive in hiding PIN bits in 8×8 DCT compressed blocks. Here, the LSB substitution is not done to hide the information but swapping of coefficients will be done in order to hide the message bits. As only one bit will be embedded per 8×8 block, except the R_3C_3 and R_4C_1 coefficients, others remain unchanged. Based on these two rules, the remaining 15 bits will be embedded in selected 8×8 blocks from the three R, G and B layers.

RESULTS AND DISCUSSION

The algorithm was implemented on a sample ATM card image of size 224×344. The DCT was applied on all the 1204 8×8 blocks. Initially a four digit PIN value 1838 was considered to analyze the embedding process. The equivalent binary representation of considered PIN is 0001100000111000_2 assuming four bits per digit. As this binary pattern had only five ones, selected pair in five selected 8×8 blocks of DCT co-efficients were swapped to indicate the embedding of logic '1' in the transformed image. In order to follow uniformity to reduce the key length, the embed location set {L} was chosen as $\{R_3C_3, R_4C_1\}$, which means in all the five blocks the co-efficients in these two locations will be swapped to indicate the hidden bit '1'. Moreover, this process is not hiding the information through LSB substitution technique but by swapping non-zero coefficients. For this pattern of 1838, red layer was used to embed bit '1' in the 20th 8×8 block, green layer was hiding the bit '1' in 20th block of its layer and three logic '1' bits were embedded in 51, 54 and 814 blocks of blue layers. These details are shown in Table 1.

This study also considered another sample PIN FFFFh which has 16 logic '1's. These 16 one's were hidden in 16 8×8 blocks based on the characteristic of the blocks and after randomizing the bits with a guiding block. Six red blocks, five green blocks and blue blocks were utilized to secure the PIN. The PSNR after hiding 6 bits (swapping) in red layer was at 50.396, where it was 56.225 for one bit concealment in red layer. Normally the PSNR value for LSB embedding with k = 1 is approximately 51 dB considering full embedding on the sample image. But here the maximum

Table 1: MSE and PSNR results for sample ATM card image

No. of blocks used for hiding 1 bit per block (m = 1)	Layer	Embedded 8×8 block locations	MSE	PSNR (dB)
1	Red	20	0.1550	56.225
1	Green	20	0.1634	55.997
3	Blue	51, 54, 814	0.2204	54.698
6	Red	52, 152, 555, 732, 882, 1201	0.5935	50.396
5	Green	41, 104, 471, 941, 1201	0.4167	51.932
5	Blue	51, 54, 814, 859, 1201	0.3067	53.263

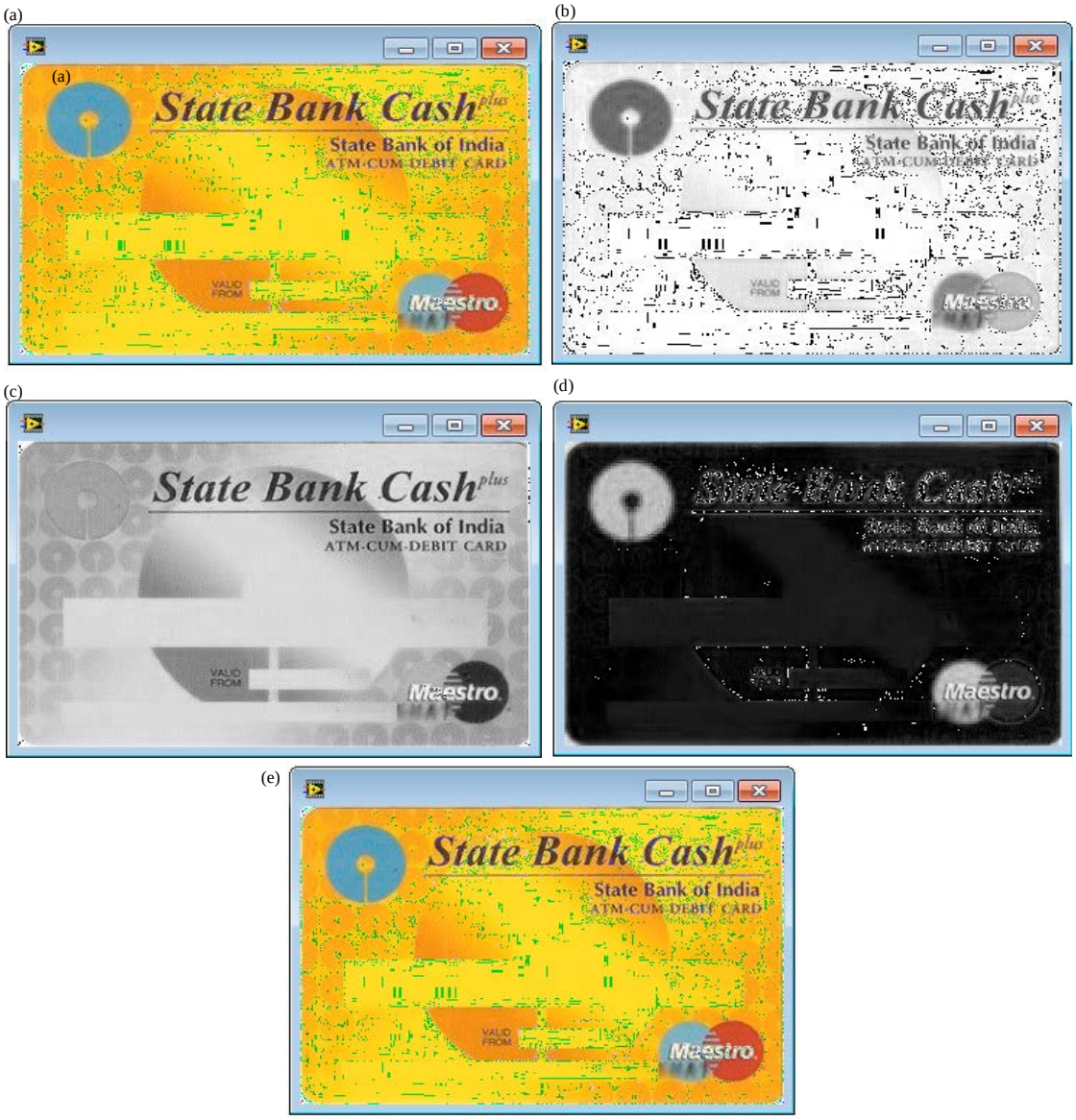

Fig. 3(a-e): (a) Cover image of sample ATM card, (b) Stego red layer, (c) Stego green layer, (d) Stego blue layer and (e) Combined RGB stego image

possible bits that can be embedded in the selected image is 16. Moreover, the process of embedding is swapping and not LSB embedding on the image blocks. Therefore, the PSNR rises upto 56.225 dB as a result of one bit embedding (swapping) in red layer (20th 8×8 block) and drops down to 50.396 when 6 bits are embedded in red layer. The deviation in the PSNR value may be attributed to decompression affected by the coefficient swapping. Figure 3 show the sample SBI ATM card cover image, stego red image, stego green image, stego blue image and stego sample ATM card RGB image. Figure 4 display the histogram report of red, green and blue layers of sample SBI ATM card image.

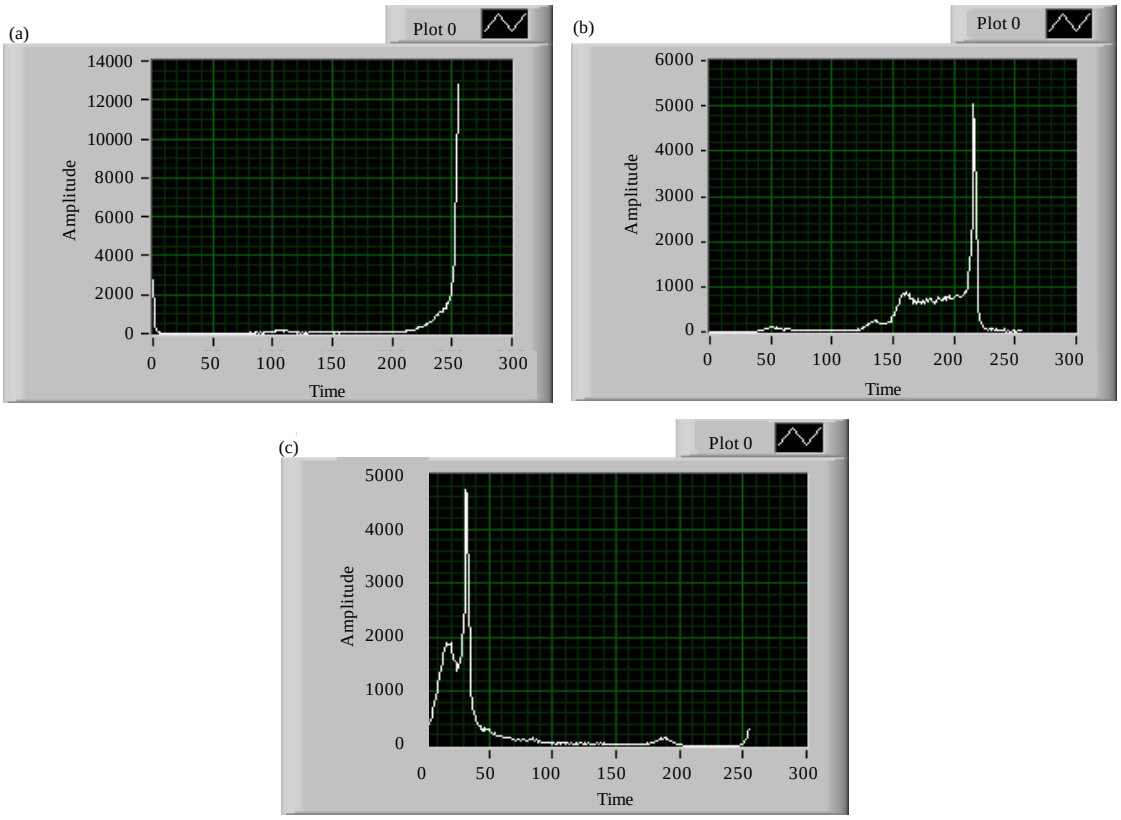

Fig. 4(a-c): Histogram reports of (a) Red, (b) Green and (c) Blue layers for sample ATM card image

CONCLUSION

A transform domain steganography approach to secure ATM PIN communication has been proposed in this study. Even though, the concern is the knowledge of information hiding techniques among common men, the idea is to address the need for information security in banking. As for as net banking is concerned, two way and three way security net guards are deployed by many of the global, nationalized and private banks. This proposed approach may have a possibility of enhancing the PIN protection and can be an alternate to tackle the ATM PIN theft. This approach can be more strengthened by randomizing the embedding process in other ways with PRNGs such as LFSR, multiple LFSRs etc.

ACKNOWLEDGMENT

Authors wish to acknowledge SASTRA University, Thanjavur for extending infrastructural support to carry out the study.

REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012a. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

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

Amirtharajan, R. and J.B.B. Rayappan, 2012c. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012e. 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. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

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

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. 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, 2013c. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

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

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

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

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013g. 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, 2013h. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

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

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

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

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

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

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

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., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

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

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

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

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

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

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, 2014a. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

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

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

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. 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, 2014e. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

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

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

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014i. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

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

Qi, X. and K. Wong, 2005. An adaptive DCT-based mod-4 steganographic method. Proceedings of the IEEE International Conference on Image Processing, Volume 2, September 11-14, 2005, Genoa, Italy, pp: II-297-II-300.

Rajagopalan, S. and H.N. Upadhyay, 2011. Stego system on chip with LFSR based information hiding approach. Int. J. Comput. Appl., 18: 24-31.

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. Proc. Eng., 30: 806-813.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J., 10.1155/2014/192512

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

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014c. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014d. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

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. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

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

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

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

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inform. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn., 36: 2875-2881.

Wong, K., X. Qin and K. Tanaka, 2007. A DCT-based Mod4 steganographic method. Signal Process., 87: 1251-1263.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Zhang, X. and S. Wang, 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett., 25: 331-339.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.