There are basically two types of LSB methods LSB replacement and LSB matching [9]. In both the cases data to be hidden is represented in binary form. This method is simple and implement with low cost.LSB replacement embeds a message into the cover image by replacing the LSBs of the cover image with message bits to arrive at the stego image. The method increases even pixel values either by one or leaves them unmodified, while odd values are left unchanged or decreased by one. As a result, there exists an imbalance in the embedding distortion in the stego image.

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. We can embed three bits of information in each pixel in a 24 bit image, Each LSB position of the three eight bit values[3] carry one bit . Increasing or decreasing the value by changing the LSB does change the appearance of the image. Amount of data that can be embedded is called as embedding capacity and distortion present during embedding is called as embedding distortion[1].LSB method has average embedding capability. LSB replacement embeds a message into the cover image by replacing the LSBs of the cover image with message bits to arrive at the stego image. The OPAP method greatly improved method to reduse the image distortion problem caused by the LSB replacement. In this OPAP method, if message bits are embedded into the right most LSBs of an n -bit pixel, other bits are adjusted by a simple evaluation. These bits are either replaced by the adjusted result or otherwise kept unmodified if the adjusted result offers a smaller distortion.

This system uses a new data embedding method Adaptive Pixel Pair Matching(APPM) which reduce the embedding and provides more embedding efficiency.

3. Adaptive Pixel Pair Matching (APPM)

APPM is proved to offer better security against detection and lower distortion, it explore a better mechanism and provide better security and lower distortion for embedding data in colored images. Also, performance in terms of payload can be improved. In colored images, which consists three different colored layers, in each layer one can embed message bits so that the capacity of the Adaptive Pixel Pair Matching can be improved without any distortion in the original colored image.

The main concept of APPM-based data-hiding method is that it takes the pixel pair (x, y) as the reference, and then searching a coordinate (x',y') within Φ(x, y),which is the a predefined neighborhood set . such that f(x', y') = S_B, where f is the extraction function and S_B[1] is the message which is to be concealed. Then replacing (x, y)with(x', y')[1]. Take the the cover image of size M×M, *S* is the message bit which is to be concealed. Then calculate the value of *B* such that all the message bits can be embedded. The message digits are then sequentially concealed into pairs of pixels. To find *cB* and$\Phi_B(x,y)$, solvethe discrete optimization problem.Then construct a nonrepeating random embedding sequence *Q* using the key the *Kr*. To embed a message digit S_B,first select two pixels (x, y) in the cover image according to the embedding sequence *Q*, and then calculate the modulus distance between S_B and f(x, y), then replace (x, y) with (x + x', y+y').

$$d=S_B-f(x,y)\text{mod}B$$

For APPM-based method, to conceal a digit S_B ,the range of S_B is between 0 and B-1, and a coordinate (x', y') in Φ(x, y) has to be found such that f(x',y') = S_B. Therefore, the range of (x ,y) must be integers between 0 and B-1, and each integer must occur at least once. To reduce the distortion, the number of coordinates in Φ (x, y) should be as small as possible. The values of Φ(x, y) and f(x, y) significantly affect the stego image quality. The designs of Φ (x, y)and f(x, y) should satisfy the requirement that the summation of the squared distances between all coordinates in Φ(x, y) and f(x, y) has to be the smallest. This is because, during embedding, (x, y) is replaced by one of the coordinates in Φ(x, y). Suppose there are B coordinates in Φ(x, y), i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x, y) by one of the coordinates in Φ(x, y) is equivalent. The averaged MSE can be obtained by averaging the summation of the squared distance between and other coordinates in Φ(x, y). Thus, given a Φ(x, y), the expected MSE after embedding can be calculated by

$$\text{MSE}_{\Phi(x,y)}=\frac{1}{2B}\sum_{i=0}^{B-1}((x_i-x)^2+(y_i-y)^2)$$

In APPM, based on these f(x, y) and Φ(x, y) the secret data is embedded . Let

$$f(x, y)=(x+c_By)\text{mod } B$$

Solve the discrete optimization problem to find Φ(x, y) and f(x, y).

Minimize: $\sum_{i=0}^{B-1}((x_i-x)^2+(y_i-y)^2)$
Subject to: $f(x_i,y_i)\in\{0,1,B-1)$ [1]
$f(x_i,y_i)\neq f(x_j,y_j)$,if i≠j

Given an integer B and an integer pair (x,y) , The B pairs of (x_i,y_i) are obtained by solving this equation and which is denoted by $\Phi_B(x,y)$ .The $\Phi_B(x,y)$ represents a neighborhood set of (x,y) . Table I lists the constant c_B, for a given B, it is possible to have more than one c_B and $\Phi_B(x,y)$ satisfying the above equation. Table I only lists the smallest c_B.The embedding procedure and extraction procedure for data hiding are given below.

A) Embedding Procedure

Consider the cover image of size *M*×*M*, then each of R, G, B channels will be of size *M*×*M*. *S* is taken as the message bits to be concealed for each channel image. First we want to calculate the minimum value of *B* such that all the message bits can be embedded. Then, each message digits are sequentially concealed into the pixel pairs according to the embedding sequence. The embedding procedure is shown in the following steps.

1) First calculate the minimum value of B satisfying |M×M / 2| ≥|SB|, and convert S into a list of binary numbers with a B-ary notational system SB.
2) Solve the discrete optimization problem to obtain cB and ΦB(x, y).

3) Record the coordinate (x', y') In the region defined by ΦB(x, y) such that f(x', y') = i, 0 ≤ i ≤ B-1.
4) The nonrepeating random embedding sequence Q is constructed by using the secret key Kr.
5) To embed a message digit sB, two pixels (x, y) in the cover image are selected according to the embedding sequence Q, and calculate the modulus distance between sB and f(x, y)
6) d=SB-f(x,y)modB
7) Then replace (x, y) with (x + x', y + y').
8) Repeat step 5, until all the message bits are embedded.

In real applications, we can solve all c_B and $\Phi_B(x,y)$ at once. With the knowledge of c_B and , $\Phi_B(x,y)$,there is no need to perform Step 2 in the embedding phase.

Table 3.1: List of the constant c_B for 2≤ B ≤64

c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4	4
c_{19}	c_{20}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}	c_{27}	c_{28}	c_{29}	c_{30}	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
4	8	4	5	5	5	5	10	5	5	5	12	12	7	6	6	10
c_{36}	c_{37}	c_{38}	c_{39}	c_{40}	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	c_{46}	c_{47}	c_{48}	c_{49}	c_{50}	c_{51}	c_{52}
15	6	16	7	7	6	12	12	8	7	7	7	7	14	14	9	22
c_{53}	c_{54}	c_{55}	c_{56}	c_{57}	c_{58}	c_{59}	c_{60}	c_{61}	c_{62}	c_{63}	c_{64}					
8	12	21	16	24	22	9	8	8	8	14	14					

We can illustrate the embedding procedure by using a simple example. Consider a cover image of size 512× 512 with embedding requirement of 520,000 bits. The minimum value of B can be obtained by solving this equation.
(512×512×log2B)/2≥520000 ,B= 16

C_{16}=6 (from the table)

Therefore, the 16-ary notational system can choose as the embedding base. $\Phi_{16}(x,y)$ can be obtained by solving (1). The 16 (x̂i , ŷi)'s in $\Phi_{16}(0,0)$ are recorded such that f(xî,ŷi)= i ,0≤ i ≤ B-1. Fig. 1 shows the neighborhood set $\Phi_{16}(0,0)$ and (x̂i , ŷi) , where 0 ≤ i ≤ 15. Suppose a digit1_{16} is to be concealed in a pixel pair (10,11) that in a 16-ary notational system. First calculate the modulus distance between 1_{16} and f(10,11) is

d=(1-12) mod16=5 and ($\hat{x}_5$, $\hat{y}_5$)=(-1,1) therefore, we replace (10,11) by (10-1,11+1)=(9,12)

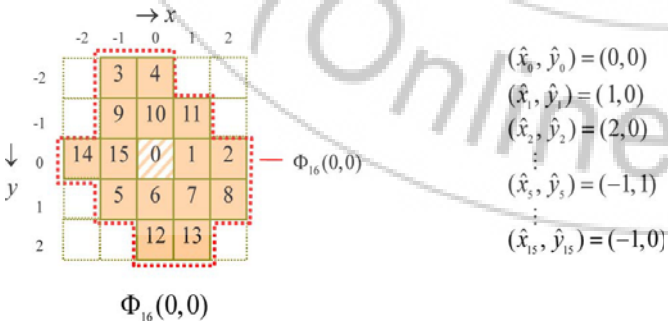

Figure 1: Neighborhood set Φ16(0,0) and(x̂i , ŷi),where 0 ≤ i ≤ B-1

B) Extraction Procedure

The extraction procedure is easy than embedding. The extraction is done by using the key. To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure[1]. The embedded message digits are the values of extraction function of the scanned pixel pairs.

1) Using a key Kr Construct the embedding sequence Q
2) According to the embedding sequence Q ,select two pixels (x', y')
3) Calculate f(x', y'), the result is the embedded digit.
4) Until all the message digits are extracted, repeat steps 2 and 3
5) Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream.

The extraction procedure can also explain with the previous example. Let the scanned pixel pair be (x',y')=(9,12). The embedded digit in a 16-ary notational system can be extracted by solving

$$f(9,12)=(9+6\times12)\bmod 16=1_{16}$$

4. Proposed Method

In this section, we introduce a new ATM model to enhance the security in the banking region.After the invent of ATM the banking became much more easier but the chance of misuse of the ATMs increases day by day .In this proposed system the customer can embed his password into any image as his choice by using the server in bank or at the home itself. In the ATM counter customer can login to his account by using this image along with the ATM card. After implementing this system the bank will provide two pins to the customer one can be used as the pin for the ATM card and the customer can embed other pin into any image. At the time of login the user insert his usb in the machine and choose the image in which he embed the PIN, then insert his ATM card and enter the PIN for the ATM card. If both the passwords matches together he can login to his account. This will avoid the problem of card theft and pin theft.

A. Block diagrams

The two main subsystems are encoding at the client side and decoding at the receiver side. The block diagrams are shown below.

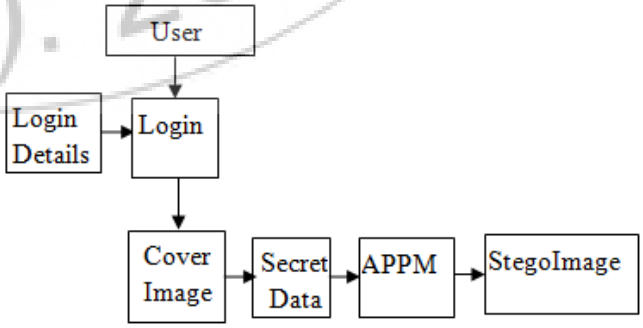

Figure 2: Encoding

The embedding of PIN no. into the image is shown in this fig2.The user can login to the server by using the user id and password. Then choose an image. The concealing media is called cover or host media. If this cover media is a digital image, it is called a cover image. The data embedding into the image by using the adaptive pixel pair matching stegnography. The altered cover image containing the secret information is called a stego-image . APPM explores a better mechanism and provide better security and lower distortion for embedding data in colored images. Also, performance in terms of payload can be improved. The stego image will look identical to the cover image.

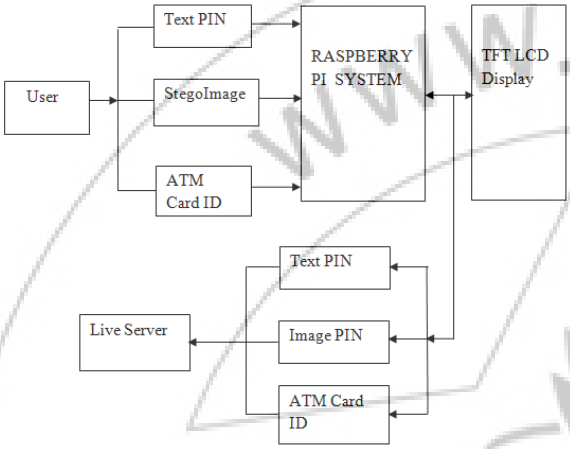

Figure 3: decoding

The decoding is done at the ATM counter. Where the user can enter his ATM card and pen drive, and then choose the stego image. The proposed system uses a TFT LCD display system and no keypad is provided. Customer can use the touch screen to do their operations. Linux operating system used in this system. In the ATM counter the login procedure includes two steps, first the user enter his USB and choose the stego image in which the PIN is embedded. Then swipe the ATM card and enter the text PIN into the raspberry pi system. When the customer enters his login details, the request passed to the live server. The server check the details he entered, if the details are matches together the screen displays that he is a valid customer otherwise an invalid customer.

B. The Raspberry Pi

The Raspberry Pi is a credit-card sized computer that plugs into your TV and a keyboard. It is developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools. Eben Upton, founder and former trustee of the Raspberry Pi Foundation. It is a capable little computer which can be used in electronics projects, and for many other things like spreadsheets, word-processing and games that our desktop PC does. It can also play high-definition video. The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZFS 700 MHz processor, VideoCore GPU, and it has 256 megabytes of RAM, later upgraded (Model B & Model B+) extend range to 512 MB. It does not include a built-in hard disk or solid-state drive, but it uses an SD card for booting and storage. Raspberry Pi is powered by a slightly aged ARM11 processor.

Figure 4: The raspberry pi-model B

Raspberry Pi-Basic Kit-512MB-Model B is used in this system. The Raspberry Pi organization making only the board. But we need many other basic components such as SD Card with loaded operating system(with NOOBS), micro USB cable, Ethernet and display cable. This basic kit comprises of all the necessary hardware units for using the Raspberry Pi, The kit fulfills these basic needs to start using the Raspberry Pi. The SD card included in the raspberry pi kit is loaded with multiple OS, so that the user can simply insert the SD card in the slot of the Raspberry Pi and directly choose from various options.

The Raspberry Pi does not come with a real-time clock, so an operating system must use a network time server, or ask the user for time information at boot time to get access to time and date for file time and date stamping. However, a real-time clock (such as the DS1307) with battery backup can be added via the I²C interface. Level 2 cache is 128 KB, used primarily by the GPU. The Broadcom SoC used in the Raspberry Pi is equivalent to a chip used in an old smartphone (Android or iPhone).The Raspberry Pi provides a real world performance. The Raspberry Pi chip operating at 700 MHz by default, it will not become hot enough so no need of heat sink or special cooling. The RaspberryPi primarily uses Linux kernel-based operating systems. The ARM11 used in the raspberry pi is based on version 6 of the ARM which is no longer supported by several popular versions of Linux, including Ubuntu. The NOOBS is used as the install manager for Raspberry Pi.

5. Result and Discussion

Nowadays the misuse of the ATMs increases day by day. The criminals steal user's credit card and password by illegal means and use this stolen information to produce counterfeit cards to be used for fraudulent transactions increasingly around the world.This is an effective method to improve the security in the ATM transactions. In this system a customer can do these transactions by using the stego image and the ATM card. The stego-image should resemble the cover image under casual inspection and analysis. The encoder usually employs a stegokey which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image. This will increase the security.

Figure 5: (a) cover image (b) stego image

The customer PIN no can be embedded in to any image using the APPM embedding procedure. The fig 5 shows the cover image and stego image. The image after embeding is similar to the actual image. So it is not easily detected by visual analysis. The criminals cannot find the image in which the password is embedded and did not extract the pin no. without knowing the secret key.

6. Conclusion

In accordance with the situation of the insecure ATMs at present, we design a new intelligent ATM model and transaction system by using the image processing technique. It can improve the security in the banking region. The conventional system needs to be replaced with this system where the transaction process becomes reliable, secure, and tension free.If the criminals stolen the user's bank card or the password, they cannot do the transactions because using card and password cannot verify the client's identity exactly. It uses simple and efficient data embedding method based on APPM. APPM is proved to offer better security against detection.

References

[1] A Novel Data Embedding Method Using AdaptivePixel Pair MatchingWien Hong and Tung-Shou Chen
[2] Image Steganography Techniques: An Overview Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi
[3] A Sesure Image Steganography Using LSB Technique and Pseudo Random EncodingTechnique
[4] N. Provos and P. Honeyman, "Hide and seek: An introduction tosteganography," IEEE Security Privacy, vol. 3, no. 3, pp. 3244,May/Jun. 2003
[5] Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital imagesteganography: Survey and analysis of current methods," SignalProcess., vol. 90, pp. 727–752, 2010
[6] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in Proc. Int. Workshop on Multimedia and Security, 2001, pp. 27–30
[7] D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005
[8] K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern
[9] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006
[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006
[11] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in Proc. SPIE, Security, Steganography., Watermarking of Multimedia,2007, vol. 6050, pp. 2–3.