Cryptosystem for Secure Parking

siti salwa md noor
Universiti Teknologi MARA
7 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Noorita Tahir
Universiti Teknologi MARA
152 PUBLICATIONS **712** CITATIONS
SEE PROFILE

Ihsan Mohd Yassin
Universiti Teknologi MARA
102 PUBLICATIONS **421** CITATIONS
SEE PROFILE

A.M. Samad
Institute of Electrical and Electronics Engineers
126 PUBLICATIONS **365** CITATIONS
SEE PROFILE

Cryptosystem for Secure Parking

Siti Salwa Md Noor[1], *Nooritawati Md Tahir*[2] , *Ihsan Ahmad Yassin*[3] *and Abd Manan Samad*[4]
Faculty of Electrical Engineering[1,2,3]
Faculty of Architecture, Planning and Surveying[4]
Universiti Teknologi MARA
40450 Shah Alam Selangor
Malaysia
Corresponding Author: ct_salwamn@yahoo.com

Abstract: **Encryption and decryption technique is normally applied for security enhancement namely by hiding data, messages or images. In this paper, encryption and decryption method based on Hill Cipher is implemented in a car park is discussed. The main focus of applying encryption and decryption on the system is to conceal the images of car plate stored in the database. In addition, prevention from attackers on a system and vehicle is also the aimed on implementing the cryptosystem. Results attained proven that the proposed method is apposite with less computational complexity.**

***Keywords-** decryption,encryption, car park, plate recognition,secuirty*

I. Introduction

The history of cryptograph begins thousands of years ago. The technology of such secret communication is called cryptology, as using Morse code. Cryptology has long been employed by military, businesses and organizations to protect their messages. Today, encryption is used to protect storage of data and transactions between computers. However, in this paper encryption and decryption is proposed as a security measure in car park system. The overall block diagram is as shown in Figure 1.

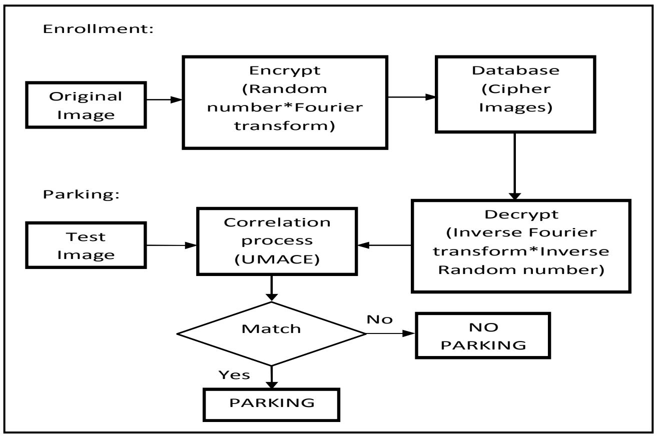

Enrollment:
Original Image
Encrypt (Random number*Fourier transform)
Database (Cipher Images)
Parking:
Test Image
Correlation process (UMACE)
Decrypt (Inverse Fourier transform*Inverse Random number)
Match
No
NO PARKING
Yes
PARKING

Figure 1. Block diagram of proposed scheme.

Cryptosystem is proposed to be implemented in parking lot subsequent to car plate detection followed by recognition based on the capability of UMACE for car plate recognition as described in [10]. Here, specific PSR value is set to conform that the car is registered in the system based on the correlation output that exhibited a sharp peak as shown in Figure 2. Otherwise, the imposter plate will lead to indiscernible peak with low PSR value.

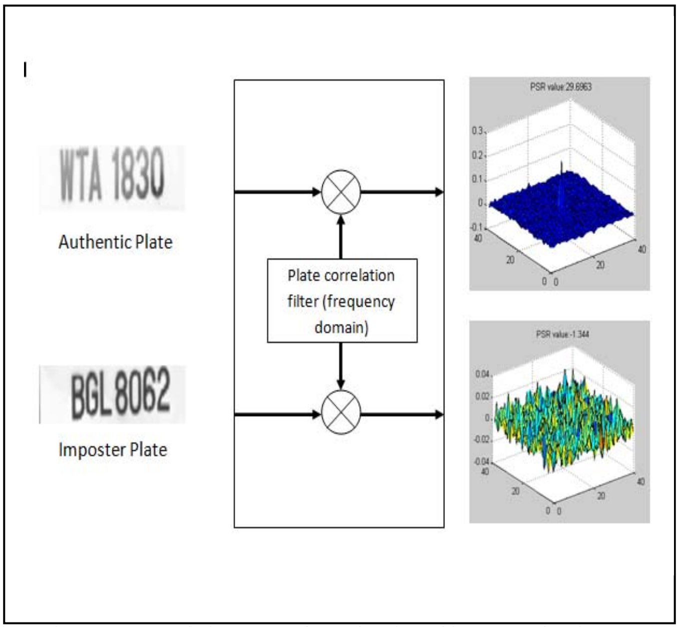


Figure 2. Correlation output for authentic and imposter plate image.

Recently, there are numerous encryption and decryption technique proposed that highlighted each benefits over other methods. Generally, there are four properties that need to be fulfilled in designing good template protection scheme namely diversity, revocability, security and performance [2]. Encryption using orthogonal polynomials based transformation domain (OPT) [1] will de-correlate the intelligible information present in the image. The end result of this method provides very low encryption PSNRs implying effective encryption. Chandana et al. [3] presented visual cryptographic system which considered as a good candidate for secure visual data transmission in system with limited bandwith. The system will change the information stored in the picture through intensity value by performing separately the three layers of color that is red, green and blue. Next, Gupta et al. [7] introduced a block based transformation algorithm based on the combination of image transformation and choas base image encryption algorithm. Increasing the number of blocks by using smaller block size resulted in a lower correlation and higher entropy. Further, chaotic systems can produce the pseudo random sequences with good randomness as discussed in [8]. The couple chaotic maps showed advantages of large key space and high level security. It is suited to be applied in fast real time encryption applications due to high throughput. Furthermore, the binary representation of the hidden data [6] is used to overwrite the Least Significant Bit (LSB) of each byte within the encrypted image randomly. The values of the correlation and entropy is expected to be the same, thus it will be used to reduce the chance of the encrypted image being detected. Other method, known as Hill cipher algorithm which is simple and eliminates the computational complexity is discussed in [4] and [5] where codes and ciphers formed secret communication. A code will replace words, phrases, or sentences with groups of letters or numbers, while a cipher rearranged letters or used substitutes to disguise the message. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the psuedocode algorithm and in each instance, by a key. Also, encryption by stream cipher using Non-Linear Shift Back Register based on Discrete Cosine Transform (DCT) coefficients reported in [9]. The algorithm will not encrypt bit by bit the whole image but only selective DCT coefficients will be encrypted, thus it is difficult to predict and provide high level of security.

II. THEORY APPROACH

A. Hill Cipher

Hill Cipher is a poly graphic substitution cipher based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. The 'key' for a hill cipher is a matrix, example matrix 3 by 3. However, it can be any size (as long as it is square matrix):

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$

Create vector that correspond to the letter and perform matrix multiplication.

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

B. Fast Fourier Transform

Fast Fourier Transform (FFT) is an efficient implementation of Discrete Fourier Transform (DFT) and is used in digital image processing. FFT is applied to convert an image from the spatial domain into frequency domain. Applying filters to images in frequency domain is computationally faster than to do the same in the spatial domain.

The definitions of the transform (to expansion coefficients) and the inverse transform are given below:

F(u,v) = SUM{ f(x,y)*exp(-j*2*pi*(u*x+v*y)/N) }

and

f(x,y) = SUM{ F(u,v)*exp(+j*2*pi*(u*x+v*y)/N) }

where u = 0,1,2,...,N-1 and v = 0,1,2,...,N-1
x = 0,1,2,...,N-1 and y = 0,1,2,...,N-1
j = SQRT(-1)
and SUM means double summation over proper x,y or u,v ranges.

III. PROPOSED SCHEME

The proposed technique is similar as Hill cipher algorithm based on matrix manipulation [5]. Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the input image. In addition its simplicity is due to matrix multiplication and inversion for enciphering and deciphering. The proposed algorithm is as listed below:

```
START
    • Acquire & resize image to 92 by 92

    /*ENCRYPTION*/
    • Generate Random Number
    • Multiply Image with random number and
      transform to frequency domain
    /*DECRYPTION*/
    • Attain encrypted image
    • Invert image via FT & and transpose random
      matrix

    • Obtain original image and authenticate with
      query image
END
```

IV. Experimental Result

In this section, the developed technique of encryption and decryption will be evaluated. The proposed scheme is tested based on 30 images. Figure 3 showed the result of encryption and decryption based on the proposed method and comparison is done based on DCT**.** Initially, each enrolled car plate images will be encrypted and stored in the database.

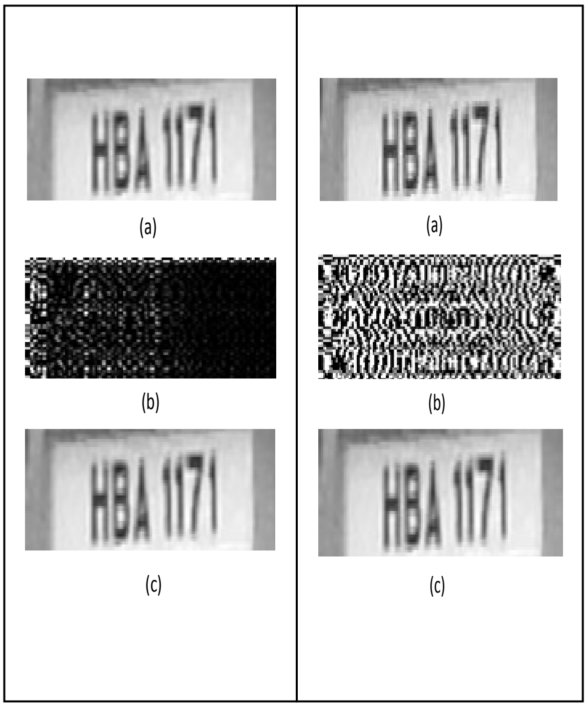
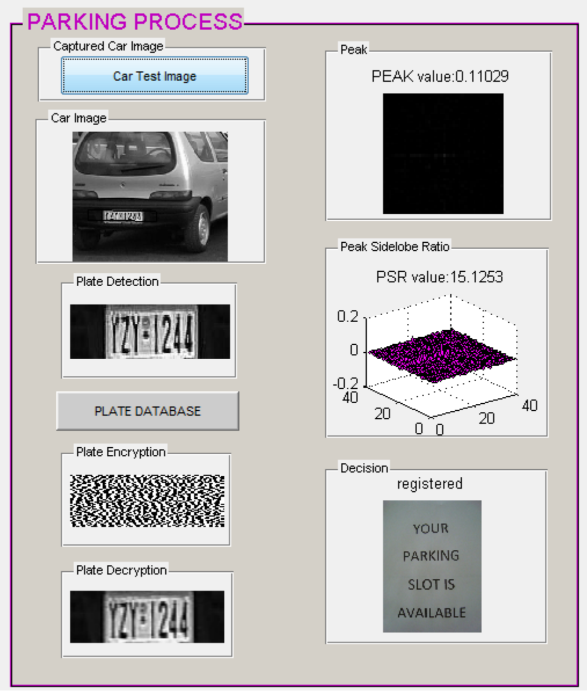


Figure 3. (a) Original image, (b) left to right – Encrypted Images based DCT and the proposed method (c) Decryption images

Further, Figure 4 and 5 demonstrated the decryption and recognition for parking process. Firstly, for a car to be allowed to park in the parking lot, plate detection will be done based on the car plate image captured. This car plate image will be the query or test image. Next, the plate will be authenticated with the registered user in the database prior to allowable for parking entrance. Figure 4 demonstrated a registered user that will be allowed to park based on decryption followed by success recognition due to high PSR value from the UMACE filter, whilst Figure 5 indicated an imposter car plate upon decryption of all database images as well as low PSR value generated from the UMACE filter that verified unregistered user.



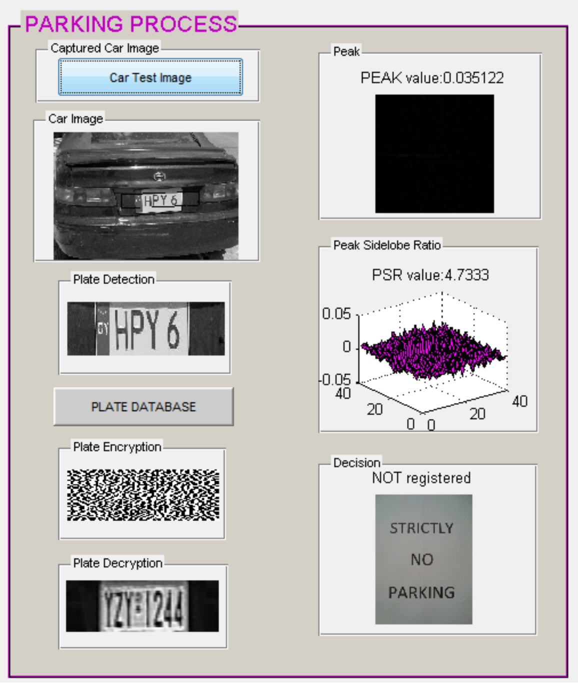
PEAK value:0.11029

PSR value:15.1253

registered

YOUR PARKING SLOT IS AVAILABLE

Figure 4. Encryption and decryption in parking process with car plate registered in database.



PEAK value:0.035122

PSR value:4.7333

NOT registered

STRICTLY NO PARKING

Figure 5. Encryption and decryption in parking process with car plate not registered in database.

In addition, two criteria are also implemented to evaluate and validate the performance of the cryptosystem namely correlation analysis and time consumption. Firstly, sample of the correlation coefficient analysis is as tabulated in Table 1. It is observed that for the proposed method, the result of the correlation coefficient is minimal which implied that no correlation existed between the original and its corresponding encrypted images and the average correlation coefficient is better than DCT.

Table 1: Correlation coefficient

Images	**DCT**		**Proposed**	
	encrypt	***decrypt***	***encrypt***	***Decrypt***
Img1	0.00276	0.00197	0.00108	0.00110
Img2	0.00148	0.00212	0.00108	0.00110
Img3	0.00149	0.00213	0.00243	0.00110
Img4	0.00148	0.00197	0.00108	0.00155
. . . .	. . . .	. . . .	. . . .	. . . .
Img30	0.00153	0.00234	0.00110	0.00110
Average	0.00175	0.00210	0.00135	0.00119
	0.0019319		**0.0012751**	

Next, the time consumption to perform both encryption and vice versa based on DCT and the proposed method is also evaluated. As tabulated in Table 2, again the average of encryption and decryption using the proposed method is better than DCT.

Table 2: Time consumption

Images	**DCT**	**Proposed**
Img1	0.0234	-0.0012
Img2	0.0112	-0.0124
Img3	-0.0869	-0.0119
Img4	0.1902	-0.0061
. . . .	. . . .	. . . .
Img30	0.0540	0.0101
Average	**0.03838**	**-0.0043**

V. CONCLUSION

As a conclusion, the encryption and decryption method proposed to be applied in car plate recognition system is validated. Performance measured shown that the proposed algorithm obtained minimal correlation between original and encryption images that confirmed the proposed cryptosystem is suitable for security as well as high computational speed. Moreover, the key that generated the random number is difficult to crack due to the size of random number that generated almost 72M possibilities that need to be marched for spoofing. Further work includes validation of the cryptosystem security strength.

REFERENCES

[1] R. Krishnamoorthi and P.D. sheba Kezia Malarchelvi, ‘Selective Combinational Encryption of Gray Scale Images using Orthogonal Polynomials based Transformation’, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2005

[2] Anil K.Jain, Karthik Nandakumar, and Abhishek Naga, ‘Biometric Template Security, Hindawi Publishing Corporation’, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416, 17 pages.

[3] B.SaiChandana, S.Anuradha, ‘A New Visual Cryptography Scheme for Color Images’, International Journal of Engineering Science and Technology, Vol.2(6),2010,1997-2000.

[4] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena, ‘Image Encryption using Self-Invertible Key Matrix of Hill Cipher Algorithm’, 1st International Conference on Advance in Computing, Chikli, India, 21-22 February 2008.

[5] Ramchandra S. Mangrulkar and Pallavi V.Chavan, ‘Encrypting Informative Image by Key Image using Hill Cipher Technique’, International Journal of Recent Trends in Engineering, Vol. 1, May 2009.

[6] Mohammad Ali Bani Younes and Aman Jantan, ‘A New Stegnography Approach for Image Encryption Exchange by using Least Significant Bit Insertion’, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6,June 2008.

[7] Kamlesh Gupta and Sanjay Silakari, ‘Choase Based Image Encryption using Block Based Transformation Algorithm’, IJCNS International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.

[8] Shubo Liu, Jing Sun and Zhengquan Xu, ‘An Improved Image Encryption Algorithm based on Chaotic System’, Journal of Computer, Vol.4, No. 11, November 2009.

[9] Lala Krikor, Sami Baba, Thawar Arif and Zyad Shaban, ‘Image Encryption using DCT and Stream Ciphe’r, European Journal of Scientific Research, ISSN 1450-216X Vol.32 No.1(2009),pp.47-57.

[10] Siti Salwa Md Noor and Nooritawati Md Tahir, ‘Plate Recognition Based on UMACE Filter’, International Conference on Computer Applications and Industrial Electronics (ICCAIE), Dec 2010, Malaysia.