Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 5 (2): 146-151, 2010
ISSN 1819-3579

Symmetric Crypto-Graphical Model

Fawaz Alsaade
King Faisal University, Al-Ahsa, Saudi Arabia

Abstract: Financial institutions play an important role in the development of a country. There are numerous ways to perform banking transactions. The main objective of this study is to fill the gap between electronic banking and conventional banking. The study presented a modular approach between electronic banking system and conventional banking system along with a flow chart. Normally in banking, user's authenticity is based on the verification of customer's signature, therefore, this study highlighted the solution of signature verification having different background, the issues regarding banking transactions and provided appropriate solutions for electronic banking system. However, in today's banking, cheques play a vital role but for electronic banking digital currency is needed. Overall, the solution and implementation of electronic money with conventional cheques is discussed in detail. Furthermore, the study tried to focus on the security of any image using symmetric key encryption.

Key words: Banking transactions, conventional banking, electronic banking, signature verification, image encryption

INTRODUCTION

Image plays a key role in the development of industry and education such that most of the time it keeps secrets. Presently, thousands of images are taken per day to record history. Image is the composite form of small units called pixels or picture elements. This study tried to focus on the security of any image using symmetric key encryption.

In the fastest cyber world, image plays a vital role for almost every electrical transaction with security to be very high priority for all transactions. In order to send and receive data, support of third party is needed and the risk is always associated with it. Therefore, a smart algorithm is required that will convert the important images into cipher and only the authorized persons can see that image after decrypting it. Since, image is one of the most important communication information, therefore, image encryption is considered a hot and an important research realm in secret communications, information security and copyright protection, etc. On the basis of thorough study of two-dimensional data structural characteristic of digital images, made adequate use of many inherent excellences of chaotic systems for security communications and information encryption such as non-periodicity, randomness, turbulence, good statistic characteristic, easy regeneration, wondrous sensitivity for initial values (Dinghui *et al*., 2008). Here an effective and sufficiently secure algorithm for image encryption was implemented.

Mallat and Tuunainen (2005) reported that wide enough acceptance and adoption of mobile payment technologies and systems is a prerequisite for consumer adoption of many, if not most, mobile commerce services. They presented results from two, concurrent sets of empirical data on merchant adoption of mobile payment systems. In addition to the potential advantages of mobile payments, they also identified several barriers to their adoption, most clearly in four categories: relative advantage, compatibility, complexity and costs

Claessens *et al*. (2002) stated that current technology is evolving fast and is constantly bringing new dimensions to our daily life. Electronic banking systems provide us with easy access to banking services. The interaction between user and bank has been substantially improved by deploying ATMs, phone banking, Internet banking, and more recently, mobile banking. This study discussed the security of today's electronic banking systems. The study focused on Internet and mobile banking and presented an overview and evaluation of the techniques that are used in the current systems. The issues discussed in this study are generally applicable in other electronic services such as e-commerce and e-government.

Menezes *et al*. (1996) stated that the general security requirements applied to electronic banking systems are (1). Confidentiality: Ensures that only authorized entities have access to the content of the exchanged information e.g., an eavesdropper should not be able to find out what transactions a particular user is executing, (2) Entity authentication: users should be sure that they are communicating with the real bank, before sending sensitive information to it; banks should know the identity of a user before processing its transactions, (3) Data authentication-i.e., data origin authentication and data integrity-allows one to detect manipulation and replay of data, by unauthorized parties; data manipulation includes insertion, deletion and substitution e.g., users and the bank want to be sure that the information they receive is genuine and fresh (not replayed) and (4) Non-repudiation: prevents an entity from denying previous commitments or actions e.g., a bank should be able to prove to a third party that a user performed a certain transaction, in case that user denies having performed it.

ENCRYPTION METHOD

Image is generally a combination of rows and columns or M×N, if the number of rows and columns increases, it means more and more data is present in the matrix that is generally called mega pixels image. In this case, still image for encryption is being used and its mathematical formula is given below:

$$S= f (x, y), 0\leq x\leq m; 0\leq y\leq n$$

where, m denotes the width of the image and n denotes the height of the image; for any point (x, y) in the region, f (x, y) denotes the pixel value of which point. Without the loss of the generality, the 256 degree gray image is being used as an example to explain the encryption, so the expression S= f (x, y) will denote the gray value in this study. The gray value corresponding to any point in a gray image is finite (0~255), so the value of the formula S = f (x, y) is limited. After the image has been digitalized, the formula S = f (x, y), corresponds a matrix. The row and column of each matrix element is the coordinate of the image displayed on a computer screen, and any element value of the matrix is the gray value of the related point (Dan and Xiaojing, 2008).

Initialization

Input

Load of Image for Encryption i.e.,

P_{RGB} = {bij; 1≤ i≤M 1≤ j≤N} where P is the input image, M is the height of RGB image and N is the width of the RGB image.

Mathematical form of RGB image mask is as follows:

$$P_{RGB}=\begin{pmatrix} P_{11} & P_{12}\cdots & P_{1K} \\ P_{21} & P_{22}\cdots & P_{2K} \\ . & . & . \\ . & . & . \\ P_{W1} & P_{W2} & P_{WK} \end{pmatrix}$$

Method

Encryption

First step is to encrypt an image by multiplying P image matrix with private key Kr and assigning new name of the matrix with P`.

- $P` := P_{RGB}.Kr$
- $P` = K_r.P$

$$Kr.P=\begin{pmatrix} K_r.P_{11} & K_r.P_{12}\cdots & K_r.P_{1K} \\ K_r.P_{21} & K_r.P_{22}\cdots & K_r.P_{2K} \\ . & . & . \\ . & . & . \\ K_r.P_{W1} & K_r.P_{W2} & K_r.P_{WK} \end{pmatrix}$$

Matrix shows the first form of encryption which is represented by P`. It is the product of pixel values private key Kr. The mathematical explanation of the above matrix is given below:

$$T\{\sum_{i=1}^{n} Kr.Pi\} \rightarrow \text{ASCII code } P' \in P`_{RGB}$$

where as:

$$(i, j) \in P_{RGB}$$

This is the second part of an encryption. In this case, the above matrix is encrypted into special ASCII code which is then used as cipher for transmission. It is secure as if anybody wants to decrypt that code he got nothing but the special code:

$$T\{P'\} \rightarrow \text{Special codes } \sum_{i=1}^{n} \varphi_i$$

$$\varphi_{RGB}=\begin{pmatrix} \varphi_{11} & \varphi_{12}\cdots & \varphi_{1K} \\ \varphi_{21} & \varphi_{22}\cdots & \varphi_{2K} \\ . & . & . \\ . & . & . \\ \varphi_{W1} & \varphi_{W2} & \varphi_{WK} \end{pmatrix}$$

Now the desired image is twice encrypted and ready to transmit to its destination. This image can be decrypted with this algorithm only with the help of its private key. The various decryption steps are as follows.

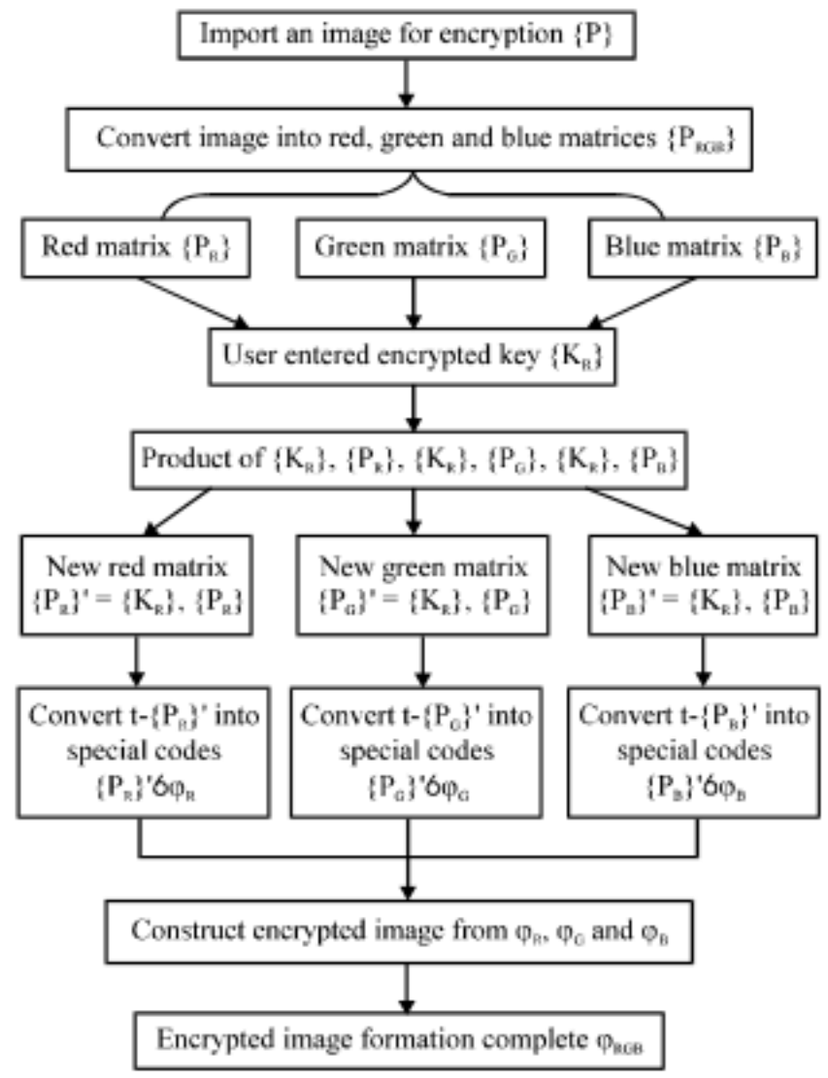

Fig. 1: Symmetric image encryption model

Now convert the encrypted matrix into ASCII code and then divide the new matrix by symmetric private key.

$$T\{\varphi_{RGB}\} \rightarrow T\{\sum_{i=1}^{n}\varphi_i\} \rightarrow \text{ASCII of P'}$$

P: =P`/Kr

$$\begin{pmatrix} K_r.P_{11} & K_r.P_{12}.... & K_r.P_{1K} \\ K_r.P_{21} & K_r.P_{22}..... & K_r.P_{2K} \\ . & . & . \\ . & . & . \\ K_r.P_{W1} & K_r.P_{W2} & K_r.P_{WK} \end{pmatrix}$$

$$P = P'/Kr \text{ or } T\{\{\sum_{i=1}^{n} P`i./Kr\} \rightarrow \{\sum_{i=1}^{n} Pi\}$$

Now this algorithm will help us to retrieve the original image. This encryption and decryption in Matlab was tested and then proposed a system. Encryption and decryption of an image are shown in Fig. 1 and 2.

EXPERIMENTS AND TESTING

Many researchers have already proposed different encryption and decryption models such as Elliptic Curve Integrated Encryption Scheme (ECIES) where public key and private key are used for encryption and decryption (Guan *et al*., 2008). The chaotic algorithms such as Chaotic Key-Based Algorithm (CKBA) were proposed by Yen and Guo (1999a, b, 2000)

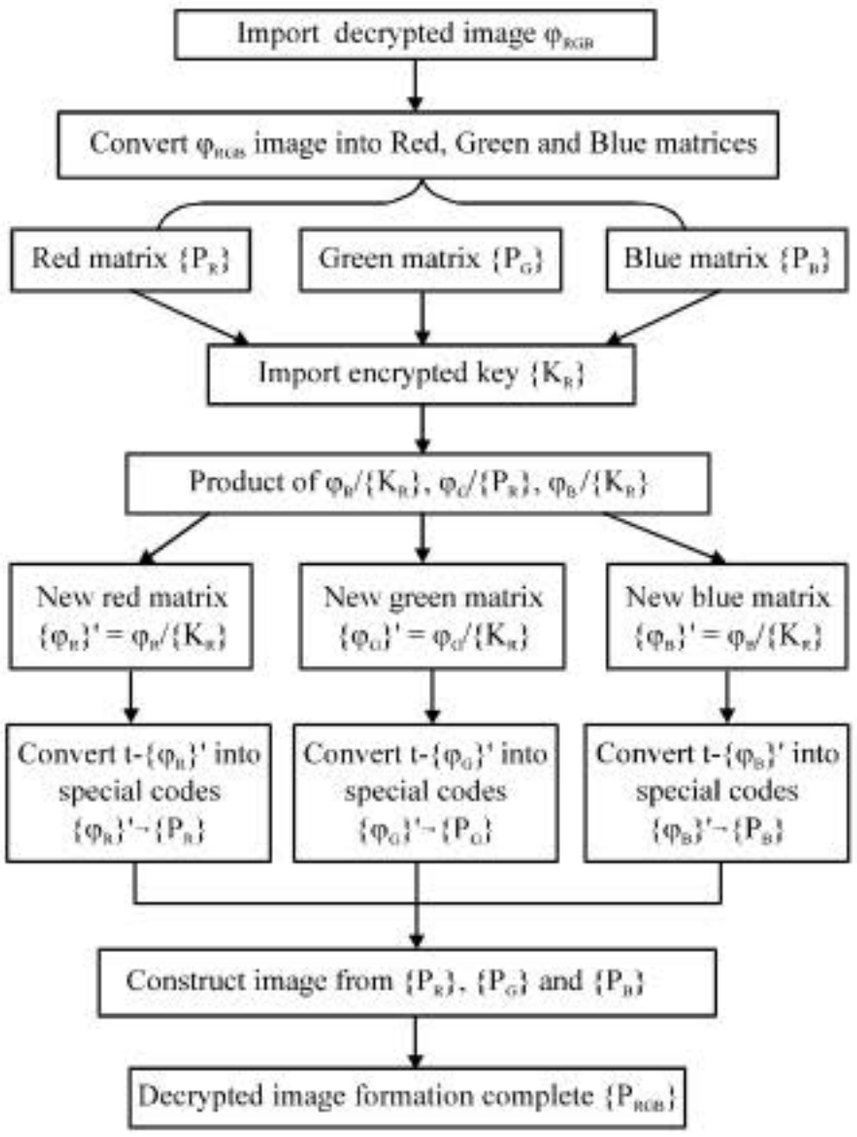

Fig. 2: Result of image encryption

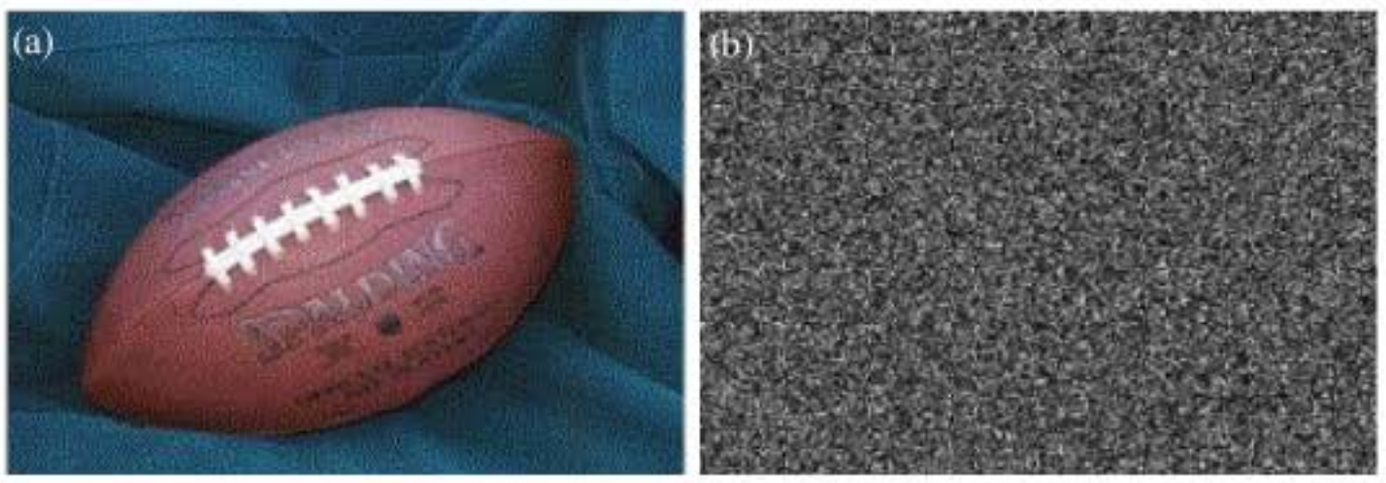

Fig. 3: The resultant images (a) original and (b) encrypted

in which a binary sequence as key is generated using chaotic system, and the image pixels are arranged according to the generated binary sequence, and then the scale-gray values of pixels are XORed or XNORed bit-by-bit to one of the two predetermined keys. Most of the experiments are combination of chaotic and discrete wavelet transform which are used for image transformation and coding (Delei *et al*., 2008). The Encryption filter is another way in this regard and it explains the advantage of large number of knight's tour, let the encryption-filter template matrix move along with the Knight's tour slip matrix and does the convolution (Wang *et al*., 2008).

Actually, the present experiments were chaotic based and the results were tested with the help of Mat laboratory for encryption and decryption which are so simple and easy to implement but private key is the only way of decryption. The resultant images are presented in Fig. 3.

CONCLUSION

The study proposed a new and effective scrambling method of image encryption based on chaotic encryption using private key. This algorithm was based on a private key encryption where as a single key is used in encryption and decryption and the size of key image can be much smaller than the secret image.

REFERENCES

Claessens, J., V. Dem, D. De-Cock, B. Preneel and J. Vandewalle, 2002. On the security of todays online electronic banking systems. Computer Security, 21: 253-265.

Dan, T. and W. Xiaojing, 2008. Image encryption based on bivariate polynomials. Proceedings of the 2008 International Conference on Computer Science and Software Engineering Dec. 12–14, IEEE Computer Society Washington, DC, USA, pp: 193-196.

Delei, J., B. Sen and D. Wenming, 2008. An image encryption algorithm based on knight tour and slip encryption-filter. Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Dec. 12–14, IEEE Computer Society Washington, DC, USA, pp: 251-255.

Dinghui, Z., G. Qiujie, P. Yonghua and Z. Xinghua, 2008. Discrete chaotic encryption and decryption of digital images. Proceedings of International Conference on Computer Science and Software Engineering, Dec.12-14, IEEE Computer Society Washington, DC, USA, pp: 849-852.

Guan, Z., Z. Chen, X. Nan, Z. Cao, X. Zhao and R. Chen, 2008. WebIBC: Identity based cryptography for client side security in web applications. Proceedings of 28th International Conference on Distributed Computing Systems, Jun. 17-20, IEEE Computer Society Washington, DC, USA, pp: 689-696.

Mallat, N. and V.K. Tuunainen, 2005. Merchant adoption of mobile payment systems. Proceedings of International Conference on Mobile Business, Jul. 11-13, IEEE Computer Society Washington, DC, USA, pp: 347-353.

Menezes, A., P. van Oorschot and S. Vanstore, 1996. Handbook of Applied Cryptography. 1st Edn., CRC Press, UK., ISBN-10: 0849385237.

Wang, Q., Q. Ding, Z. Zhang and L. Ding, 2008. Digital image encryption research based on dwt and chaos. Proceedings of Fourth International Conference on Natural Computation, Oct.18-20, IEEE Computer Society Washington, DC, USA, pp: 494-498.

Yen, J.C. and J.I. Guo, 1999a. A chaotic neural network for signal encryption/decryption and its VLSI architecture. Proceedings 10th VLSI Design/CAD Symposium, pp: 319-322.

Yen, J.C. and J.I. Guo, 1999b. A new image encryption algorithm and its VLSI architecture. Proceedings IEEE Workshop on Signal Processing Systems, Oct. 20-22, Taipei, Taiwan, pp: 430-437.

Yen, J.C. and J.I. Guo, 2000. Efficient hierarchical chaotic image encryption algorithm and its VLSI realization. IEE Proc. Vis. Image Signal Process., 147: 167-175.