Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Implementation of Database Image Encryption Using TSFS Techniques

M.Susithra[1*]
Pursuing M.Tech(ST),
SITE,Vellore Institute of Technology,
Vellore – 632014. India

M. Lawanya Shri[2]
Assistant Professor,
SITE,Vellore Institute of Technology,
Vellore – 632014, India

K.S. Umadevi[3]
Assistant Professor(Sr),
SCSE,Vellore Institute of Technology
Vellore – 632014, India

Abstract— Database security needs more attention in industrial, civilian and government domains. Organizations are storing huge amount of data in database for data mining and other types of analysis . In this proposed system we mainly focuses on providing enhanced security of images that are stored in databases, because any damage and misuse of sensitive data stored in database will affect the entire organization. For this purpose an efficient light weight database encryption technique using TSFS (Transposition, Substitution, Folding, and Shifting) algorithm is followed. TSFS algorithm is a symmetric key block encipherment algorithm that uses same key for both encryption and decryption. The security depends on the length of the key and also key expansion technique is used for providing more security for the database. In this algorithm only the images in the database are encrypted and thereby the speed of executing the queries is increased. Thus TSFS algorithm is very efficient and more secure when compared to other database security methods like physical security, operating system security, DBMS security.

Keywords— **Database Encryption, Image Encoding, Key expansion, Transposition, Substitution, Folding, Shifting.**

I. INTRODUCTION

Challenges for security in database are increased due to the overwhelming of data in database. Nowadays the insiders working in the company started playing the role of attackers . Database systems are usually deployed deep inside the company network and thus insiders has the easiest opportunity to attack and compromise them, and then own the data. So data must be protected from everyone including the insiders. There are so many conventional database security systems proposed for providing security for database but it was not so efficient. There are four methods of enforcing database security: physical security, operating system security, DBMS security, and data encryption. The first three methods are not totally satisfactory solutions to the database security problem, for the following four reasons. First, it is difficult to control the attack on raw data because the raw data exist in readable form inside a database. Second, it is impossible for the operating system and DBMS security to the disclosure of sensitive data, because the sensitive data must be backed up in storage median in case of system failure.

Third, it is hard to protect the confidential data in a distributed database system. Fourth, it is hard to verify that the origin of a data item is authentic, because an intruder may have modified the original data. Encryption of the data has the ability to solve all the three problems, If the data are not in a readable form, obtaining the data will be of no advantage to a person without the proper key to decrypt it. Thus the problem of data disclosure can be eliminated and the data authenticity problem can also be solved by encryption.

Existing system

Existing system uses an algorithm which provides security for data in data base . The security of data managed by these systems becomes crucial. Damage and misuse of sensitive data stored in the database not only affect a single user also affect entire organization. The recent development of web based applications and information systems have further increased the risk exposure of databases. The available security policies cannot provide a secure support for the sensitive data, which reside in the database, as the illegal and unauthorized users may obtain the readable data. So the sensitive data in database are vulnerable to attack because the data are stored in the form of plain text only .Since it is in the form of plain text any one can steal this data stored in database and there is possibility that they can make changes to the data ,which leads to wrong entries of data. So anyone can easily steal data stored in database. Though the algorithm used here(Chinese reminder theorem ,chip secured data, etc)were effective ,they were too complicated and the cost is too expensive.

The disadvantages of the existing system are:

- To control the attack on raw data is difficult.
- Disclosure of sensitive data occurs.

- Verification of authenticity of the origin of a data item is tedious.

Proposed system

Database encryption is the only solution to avoid the risk posed by this threat. Since encrypted data cannot be seen by anyone except the one who knows the decryption key or algorithm to decrypt the text and the one who actually encrypted it. Our system focuses on a security solution for protecting of images-at-rest, specifically protecting the images as data that resides in databases by using TSFS algorithm with three keys thus it provide more security for database. This algorithm improves the efficiency for executing the queries in database by encrypting only the sensitive data. TSFS (Transposition, Substitution, Folding, Shifting) algorithm, only the images in the database are encrypted by using this algorithm, so it will provide efficient execution of queries and give quick response to the users. TSFS is the symmetric - key block encipherment algorithm, for symmetric encryption, same key is used for encryption and decryption and security is dependent on the length of the key. Here we use three keys for the process of encryption and decryption.

For providing effective and more security for the database these three keys are expanded in into 12 sub keys by using the key Expansion Technique. The main strength of the algorithm is in the substitution transformation because selecting the key for finding the cipher gave more security to the encoded image . Images in the database are encoded and then the encoded images are taken as data. In this algorithm the numeric plaintext have numeric cipher text, character plaintext have character cipher text and if the input data is alphanumeric type then the output cipher text also in alphanumeric, so there is no need for change the data field type when the encrypted data are stored in the database.

The advantages of the proposed system are:

- The data type of plain text and cipher text is same.
- The attacker finds it difficult to analyze the recovered data .
- The number of keys are more which makes guessing of keys harder to the attacker.
- Variations between values of rows in keys provide more security for the data.
- It provides maximum security to the database.
- It also increases the process of encryption and decryption.

II. KEY EXPANSION

In this step, each key is expanded to many sub keys to be used in each round. In general the keys are expanded by an algorithm which includes shifting the rows and by using Add round key technique in AES . In the proposed scheme, three keys are used and each key is expanded to four sub-keys. The keys are generally a series of alphanumeric characters with 16digits in length. To enhance the security of this method, keys are usually stored in the form of 4X4 matrix and so the length should 16.Consider the given example below, where first the keys are converted into 16 digits by using padding technique and then stored the keys in the matrix. After that shifting the rows for key expansion and it will be used in real time process to expand the keys.

The following example describes how the three keys are expanded into 12 sub keys.
For example when the
Key1 value is 6978142036547013
Key 2 value is 8914175294516320
Key 3 value is 9041752945132012

Here, we get these keys by using a random key generator. It is not necessary that a random key generator must only be used for obtaining the key values. Key values are specified by the Users as they wish. First the keys are converted into numbers based on the position in the alphabets a-z (a-0, b-1------z-25). Then the keys are stored in 4*4 matrix form.

The keys are expanded based on shifting the rows.
Key1 is expanded into key10, key11, key12, k13.
For key10 - row 0 is not shifted, row 1 is shifted one time, row 2 is shifted two times and row 3 is shifted three times
For key11 - row 0 is shifted one time, row 1 is shifted 2 times, row 2 is shifted three times and row 3 is not shifted
For key12 - row 0 is shifted two times, row 1 is shifted three times, row 2 is not shifted and row 3 is shifted one time
For key13 - row 0 is shifted three times, row 1 is not shifted, row 2 is shifted one time and row 3 is shifted two time.

KEY 1

6	9	7	8
1	4	2	0
3	6	5	4
7	0	1	3

Key10

6	9	7	8
4	2	0	1
5	4	3	6
3	7	0	1

Key11

9	7	8	6
2	0	4	1
4	3	6	5
7	0	1	3

Key12

7	8	9	6
0	1	4	2
3	6	5	4
0	1	3	7

Key13

8	6	9	7
1	4	2	0
6	5	4	3
1	3	7	0

KEY 2

8	9	1	4
1	7	5	2
9	4	5	1
6	3	2	0

Key10

8	9	1	4
7	5	2	1
5	1	9	4
0	6	3	2

Key11

9	1	4	8
5	2	7	1
1	9	4	5
6	3	2	0

Key12

1	4	8	9
2	1	7	5
9	4	5	1
3	6	2	0

Key13

4	8	9	1
1	7	5	2
4	5	1	9
2	0	6	3

KEY 3

9	0	4	1
7	5	2	9
4	5	1	3
2	0	1	2

Key10

9	0	4	1
5	2	9	7
1	3	4	5
2	2	0	1

Key11

0	9	4	1
2	9	7	5
3	4	5	1
2	0	1	2

Key12

4	1	9	0
9	7	5	2
4	5	1	3
0	1	2	2

Key13

1	9	0	4
7	5	2	9
5	1	3	4
1	2	2	0

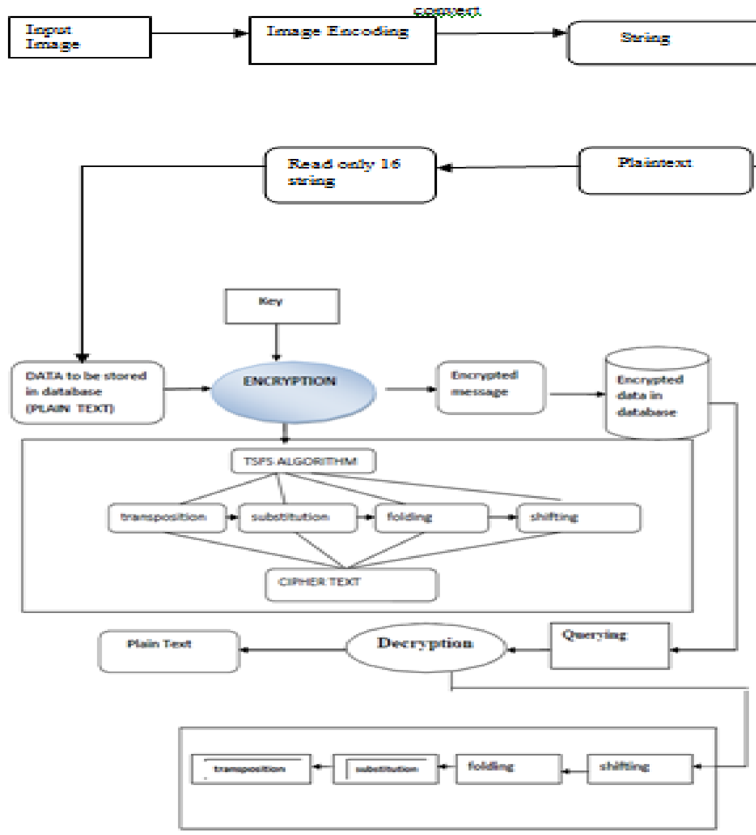
Figure.1 shows the key expansion process

III. DESIGN AND IMPLEMENTATION

Image Encoding

The images are very largely used in our daily life; the security of their transfer became necessary. Instead of encrypting an image in a chaotic signal directly, the proposed scheme uses two chaotic systems based on the thought of higher secrecy of multi-system. Input image is first encrypted which results in a series of encrypted text, which then converted into a series of binary numbers and then the plain text is extracted from the previously yielded binary series. Since the input to the algorithm should of 16 in length, the first 16 characters from the generated plaintext is extracted and passed as input to the algorithm.

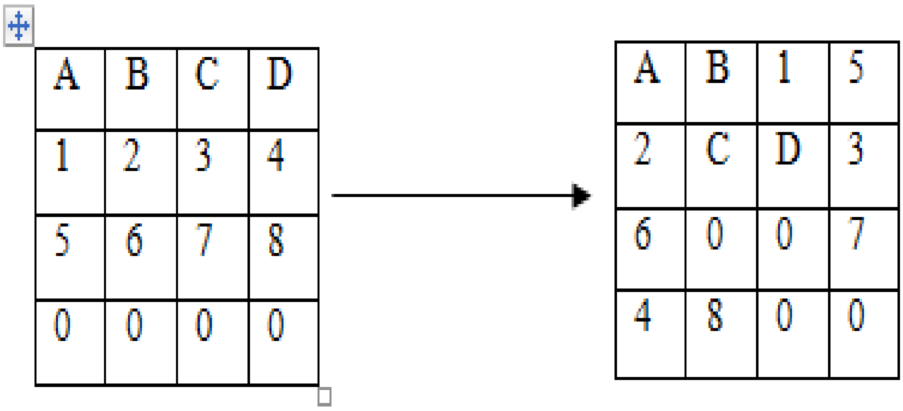
Overall view of the algorithm



IV. TSFS ALGORITHM

A. Transposition

In Transposition reordering of symbols takes places , For example if the symbol is in the first position in the plaintext, after reordering it may appear in any position (say 10th position). There is no substitution for any symbol instead only the location of the symbols are changed. For transposition the data is stored in 4*4 matrix and the data are taken diagonally and stored in another matrix of the consequence. Padding is done by adding zero to the remaining rows of the matrix. Input to this algorithm is taken from the series of encrypted text from an input image. Only the first 16 characters will be passed as an input to the algorithm.



A	B	C	D
1	2	3	4
5	6	7	8
0	0	0	0

A	B	1	5
2	C	D	3
6	0	0	7
4	8	0	0

B. Substitution

After transposition replace one symbol with another symbol. If the symbols in the plaintext are alphabetic characters replace with one character with another. For example we can replace letter A with D. The two substitution ciphers are mono alphabetic and poly alphabetic. In mono alphabetic, the relationship between the symbols in the cipher text is always one to one. In poly alphabetic, each occurrence of a character may have a different substitute. The relationship between the symbols in plaintext to a symbol in the cipher text is one to many.

$$\begin{bmatrix} A & B & 1 & 5 \\ 2 & C & D & 3 \\ 6 & 0 & 0 & 7 \\ 4 & 8 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} e & f & 5 & 9 \\ 6 & g & h & 7 \\ 10 & 4 & 4 & 11 \\ 8 & 12 & 4 & 4 \end{bmatrix}$$

Substitution ciphers can be categorized as either mono alphabetic ciphers or poly alphabetic ciphers. In mono alphabetic substitution, the relationship between symbols in the plaintext to a symbol in the cipher text is always one-to-one. In poly alphabetic substitution, each occurrence of a character may have a different substitute. The relationship between the symbols in the plaintext to a symbol in the cipher text is one-to-many. Here we use a new modified affine cipher for encryption. It is one of the mono alphabetic ciphers available.

Normally affine cipher is a combination of additive and multiplicative cipher. For this we have to use two keys one for additive cipher and another for multiplicative cipher.

By using this cipher the Encryption process is

C = (P x k1+k2) mod M

Decryption process is

P = ((C – k2) x k1-1) mod M.

In this cipher the multiplicative inverse of k1 only exists if k1 and M are co prime. Hence without the restriction on k1 decryption might not be possible. What is the key domain for any multiplicative cipher. The key must be in the range from 0 to 26. This set has only 12 members :1,3,5,7,9,11,15,17,19,21,23,25. Considering the specific case of encrypting messages in alphanumeric in English (i.e. M=26), So there are 12 x 26 or 312 possible keys. So it is easy for the cryptanalyst to find the key.

To overcome this draw back we slightly changes this affine cipher i.e. here we eliminate the process of multiplicative cipher and add one more additive cipher. In this cipher we give more importance for selecting the two keys for encryption. We expand the three keys into twelve keys and stored in the form of 4 x 4 matrix and also the entered data are also stored in the form of matrix. For encrypting the 0th row and 0th column data in the matrix we take the k1 from the same row and column of the expanded keys key10 and the k2 from key11 and the same format is used for encrypting the other data's in the matrix. Here for the first round we use the key 10 and key11 and for the second round we take the key k1 from key11 and k2 from key12 and the same process used up to the 11th round, in the 12th round we take k1 from key33 and k2 from key10. Based on this method keys are selected for encryption process.

The encryption function E, for any given letter x is

E(x) = (((k1+p) mod M) +k2) mod M

Where modulus M is the size of the alphabet and k1 and k2 are the key of the cipher.

In this cipher k1 is not need to be prime number.

The decryption function D is

D(E(x)) = (((E(x) – k2) mod M) – k1)mod M

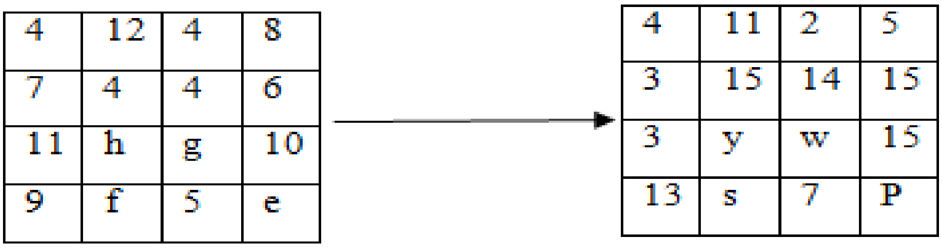
C. Folding

After substitution the result is taken as input to the folding method. Folding is the one of the transposition cipher like paper fold, the matrix is folded horizontally, vertically and diagonally.

$$\begin{bmatrix} E & f & 5 & 9 \\ 6 & g & H & 7 \\ 10 & 4 & 4 & 11 \\ 8 & 12 & 4 & 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 4 & 12 & 4 & 8 \\ 7 & 4 & 4 & 6 \\ 11 & h & g & 10 \\ 9 & f & 5 & e \end{bmatrix}$$

D. Shifting

In the shifting cipher the program replaces each digit of the number by its position within its array element. For decryption the position is given as an input based on the position the data is taken and that data is plaintext of the given cipher text.



4	12	4	8
7	4	4	6
11	h	g	10
9	f	5	e

4	11	2	5
3	15	14	15
3	y	w	15
13	s	7	P

V. Conclusion

Database attacks are increases in the risks of data disclosure. Many organizations must deal with legislation and regulation on data privacy. If sensitive data are encrypted before storage in the database, risks from security leaks can be eliminated and the security issues of the database will reduce by using three cryptographic keys for protecting the data. The proposed scheme is considered as efficient because it provides maximum security to the database and also increases the process of encryption and decryption using image. The proposed algorithm can be implemented for securing any corporate related accounting information.

References

[1] Kamaljit Kaur, K.S Dhindsa, Ghanaya Singh, "*Numeric To Numeric Encryption of Database: using 3Kdec Algorithm"*, IEEE International Advance Computing Conference, Partial, India, 2009.

[2] Min-Shiang Hwang, and Wei-pang. Yang ., "*Multilevel Secure Database Encryption With Subkeys*", Data and Knowledge Engineering, 1997.

[3] L.Bouganim and P.Puncheral, "*Chip-Secured data access*: Confidential data on untrusted servers", Proc. Of the 28th International Conference on Very Large Data Bases, Hong Kong, china, 2002.

[4] Tingjian Ge, Stan Zdonik, " *Fast,Secure Encryption for Indexing in a Column-Oriented DBMS*", IEEE 2007.

[5] M.S. Hwang and W.P. Yang, " *A Two-Phase Encryption Scheme for Enchancing Database Security",J.Systems and Software, 1995.*

[6] Song, S., J. Zhang, X. Liao, J. Du and Q. Wen, 2011. A novel secure communication protocol combining steganography and cryptography. Procedia Eng., 15: 2767-2772.

[7] Hani, M.K., H.Y. Wen and A. Paniandi, 2006. Design and implementation of a private and public key crypto processor for next-generation it security applications. Malaysian J. Comput. Sci., 19: 29-45.

[8] Jiancheng Zou, ChangZhen Xiong, Dongxu Qi, et al., "The Application of Chaotic Maps in Image Encryption", IEEE Proceedings of on NEWCAS 2005, pp. 331-334, June. 2005.

[9] A. Jolfaei and A. Mirghadri. A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1," Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10), Sanya, China, 2010.

[10] L. Xiangdong, Z. Junxing, Z. Jinhai, and H. Xiqin. Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation,"IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 1, 2008, pp. 64–68.

[11] T. Siegenthaler. Decrypting a class of stream ciphers using cipher text only, IEEE Transactions on Computers, C-34(1):81–85, January 1985.