ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Image Encryption Technique for Lightweight Cryptographic Implementation

Neha Patel
M.Tech,
Department of Computer Science & Engineering,
Disha Institute of Technology.

Manoj Singh
Assistant Professor,
Department of Computer Science & Engineering,
Disha Institute of Technology.

ABSTRACT:
Cryptography is the art of achieving security by encoding message to make them non-readable. Cryptography Techniques are the two categories- Symmetric Key Cryptography: -These are involves the usage of the same key for encryption and decryption. Asymmetric key cryptography: - These are involves the usage of one key for Encryption and another, different key for decryption.

Encryption:
In technical terms, the process of encoding plaintext messages back to plaintext messages is called encryption.

Decryption:
The reverse process of Transforming cipher text message back to plaintext message is called decryption.

INTRODUCTION:
Information Security is not simply computer security .where as computer security relates to securing computing systems against unwanted access and use , information security also includes issues such as information management, information privacy and data integrity .for ex. Information security in a library.

Need for information security

- The need for information security has also increased because the dependency of individuals and organization on compute has increased.
- Without security organization cannot successfully operate in global market unless and until they take adequate measures to secure the information.
- The database which is used or processed by organization and the data in the database is confidential.

CRYPTOGRAPHY:
Cryptography is the art of achieving security by encoding message to make them non- readable.

- Symmetric Key Cryptography:-These are involves the usage of the same key for encryption and decryption.
- Asymmetric key cryptography:-These are involves the usage of one key for Encryption and another, different key for decryption.

Encryption:
In technical terms, the process of encoding plaintext messages back to plaintext messages is called encryption.

Decryption:
The reverse process of Transforming cipher text message back to plaintext message is called decryption.

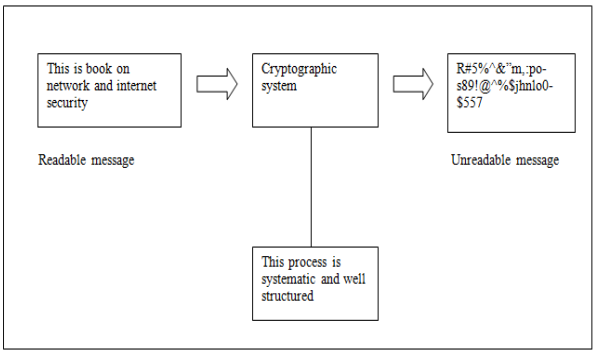


Figure: Cryptographic system

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Substitution and Permutation in Cryptography-

- Substitution:- S-box substitution is a process that accept the 48 bit input from the X-OR operation involving the compressed key and expanded RPT ,and produces a 32 bit output using the substitution technique .The substitution is performed by eight substitution boxes eight of the eight s-boxes has a 6-bit input and a 4-bit output. The 48-bit input block is divided into 8 sub-block and each such sub-block is given to an s-box.the s-box transforms the 6 bit input into a 4-bit output.
- Permutation-The output of s-box consists of 32 bits. these 32 bits are permuted using a p-ix. this straight forward permutation mechanism involves simple permutation. This is called p-box permutations .At the end of the 16 rounds. The final permutation is performed. This is a simple transposition based for instance, the 40^{th} input bit takes the position of the 1^{st} output bit and so on. The output of the final permutation is the 64 bit encrypted block.

LFSR-

A Linear feedback shift register (LFSR) is similar to a shift register with a feedback. The outputs of some of the flip flops in the shift register one feedback as input to a XOR gate and the output of XOR gate is the input to the first flip flop in the shift register .the initial value stored in the shift register is called the seed value and it can never be all zeros. Depending on the outputs feedback to the XOR gate a LFSR generates a random sequence of bits. Because of this property LESR are used in communication and error correction circuits for generating pseudo noise and pseudo random number sequences and they are also used in data encryption and data compression circuits in cryptography.

Stream Cipher v/s Block Cipher

- Stream cipher technique involves the encryption of one plain text bit at a time .the decryption also happen one bit at a time.
- Block ciphers-

  The block cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.

Problem in Information Security

- Maintain a comprehensive list of data that may be collected and the circumstances.
- For each type of data, what risks of misuse exist?
- Specify a policy for the collection of data and possible misuses.
- Identify personnel responsible for ensuring the policies are followed, and for remediation as needed.

For example, a library might require that patrons who wish to use a general-purpose computer first show their library card or ID. At that time, patrons should be informed what data will be kept from their session – will their use of the facility be logged? Will the amount of time be logged? Will different software packages, Internet sites or other records be kept, and if so will the data be linked to the patron's name? Finally, under what circumstances will any data collected be released.

- Information security risk must be assigned to specific personnel.

S-Box Implementation Problem:

- What is rationale for the bit scrambling step that is used for finding the replacement byte that goes into each cell of the S-box table?
- Let's say the first four words of the key schedule are w0, w1, w2, w3. How do we now obtain the next four words w4, w5, w6, w7?
- Byte-by-byte substitution.
- Shifting of the rows of the state array.
- Mixing of the columns.

Cryptanalysis:

Cryptanalysis is the Technique of decoding message from a non – readable format back to a readable format without knowing how they were initially

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

converted from readable format to non- readable format. In other words it is like breaking a code.

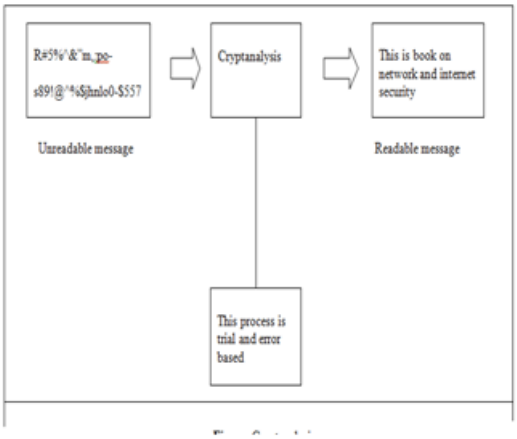


Figure: Cryptanalysis Methodology

5.2.1 Block Encryption standard for Transfer of data (BEST) Algorithm:

A Block Encryption Standard for Transfer of data (BEST) is proposed to achieve the diferent goals of security i.e., Availability, Confidentiality and Integrity. This new algorithm is based on the symmetric key encryption approach. . It enables us to achieve three primary security goals namely:

Availability:

It means that the information is accessible to authorized parties whenever they need it.

Confidentiality:

It ensures that computer related assets are accessed by only authorized parties.

Integrity: It means assets can be modified only by authorized parties or only in authorized way. Modifications include writing, changing, deleting & creating.

ENCRYPTION PROCEDURE OF BEST:

The encryption process does a variety of binary operations like Shift Left Operation on the message for protecting it against unauthorized attacks.

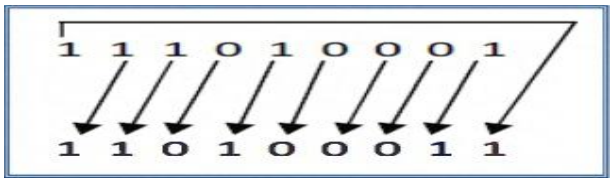


Fig 1: Shift Left operation

In this operation, bits are shifted left to one place and the Most Significant Bit (MSB) is placed to Least Significant Bit (LSB) as shown in the Figure 1.

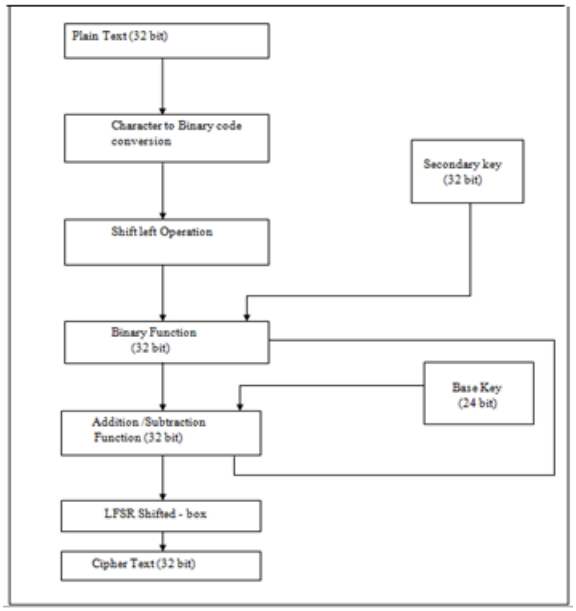


Figure: Block diagram of BEST Encryption Algorithm

The steps of encryption are given as follows:

1.The plain text in the block size of 32 bits is read from input file.

2.The plaintext is transformed into ASCII code and then modified into binary form.

3.Then shift-left operation is performed on this 32-bit data 10 times.

4.The modified plain text is then X-ORed with a secondary key of 32 bits and it is made sure the result is also of 32 bits.

5.A random number is chosen from a given range and converted into 16-bit binary number.

6.A sequence symbol is randomly selected from a preselected range.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

7.The selected symbol is converted into ASCII code and then finally into binary number of 8 bits.
8.The 8-bit binary code is then appended to the 16-bit binary number resulted from random number and the result is stored as the Base Key or Primary Key.
9.Then the key is applied on the modified plaintext with the help of a binary operation.
10. In the next step, a new key is generated from a different random number and different sequence symbol.
11.Every time a new key is generated, it is applied using a different binary operation on resulted cipher text of previous step and a modified cipher text is obtained.
12. These are Created LFSR shifted box for securing the algorithm.
13. The encryption process is continued for next characters of file until end of file is reached.

RESULTS:

MSE and PSNR:

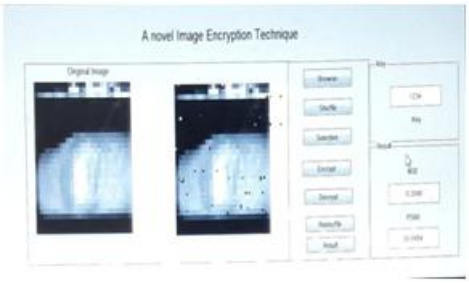
PSNR is used to measure the quality of reconstruction of lossy and lossless compression (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality.

PSNR is most easily defined via the mean squared error.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Mean Square Error

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$



CONCLUSION:

In conclusion, LFSR S-box is presented in this study. The proposed architecture is simple and compact in design. It has been successfully implemented on image . The average of A novel image encryption technique is faster and it offers the enhanced security features than the other symmetric key algorithem.These are proves to be a very efficient technique for image

REFERENCES:

1. D. canright , " A very compact Rijndael S-box," Naval Postgraduate school, tech.Rep. NPS-MA -04-001, 2005.
2. X. Zhang and k.k.parhi "on the optimum constructions of composite field for the AES Algorithm," IEEE Trans. Circuits syst. II, vol.53,no. 10, pp. 1153-1157, 2006.
3. M.M. wong, M.L.D. wong A.Nandi, and I.Hijazin," Construction of optimum composite field architecture for compact high –throughput aes s-boxes," very large scale integration (VLSI) system, IEEE Transactions on, vol.20, no. 6, pp. 1151-1155,2012.
4. M.M. wong M.L.D. wong "New Lightweight AES S-box Using LFSR," 2014 IEEE International symposium on Intelligent signal Processing & Communication System (ISPACS 2014), kuching Malaysia, December 2014.
5. S.Das." Halka : A lightweight ,software friendly block cipher using ultra-lightweight 8-bit s-boxes." Cryptology eprint Archive, Report 2014/110.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

6. S.Das.” Ultra-lightweight 8-bit multiplicative inverse based s-box using LFSR.” Cryptology eprintArchive ,Report 2014/022.
7. Wong Ming Ming and dennis Wong Mou Ling, “LFSR Based S-Box for Lightweight cryptographic implementation” 2015 International Conference on Consumer Electronics-Taiwan (ICCE-TW) IEEE 2015.
8. AkhilKaushik, ManojBarnela and Anant Kumar, “Block Encryption Standard for transfer of data”, 2010 international Conference on networking and Information technology,2010 IEEE.
9. D. canright , “ A very compact Rijndael S-box,” Naval Postgraduate school, tech.Rep. NPS-MA -04-001, 2005.
10. X. Zhang and k.k.parhi “on the optimum constructions of composite field for the AES Algorithm,” IEEE Trans. Circuits syst. II, vol.53, no. 10, pp. 1153-1157, 2006.
11. M.M. wong, M.L.D. wongA.Nandi, and I.Hijazin,”Construction of optimum composite field architecture for compact high –throughput aes s-boxes,” very large scale integration (VLSI) system,IEEE Transactions on, vol.20, no. 6, pp. 1151-1155,2012.
12. M.M. wong M.L.D. wong “New Lightweight AES S-box Using LFSR,” 2014 IEEE International symposium on Intelligent signal Processing & Communication System (ISPACS 2014), kuching Malaysia, December 2014.
13. S.Das.” Halka : A lightweight ,software friendly block cipher using ultra-lightweight 8-bit s-boxes.” Cryptology eprint Archive, Report 2014/110.
14. S.Das.” Ultra-lightweight 8-bit multiplicative inverse based s-box using LFSR.” Cryptology eprintArchive ,Report 2014/022.
15. FarnazKhani and ArashAhmadi, “Digital realization of Twisted Tent Map and Ship Map with LFSR as a Pseudo Chaos Generator”,#rd International Conference on Computer and Knowledge Engineering(ICCKE 2013), IEEE 2013.
16. MehranMozaffari Reza Azarderakhsh, Chiou-Yng Lee and SiavashBayat-Sarmadi, “Reliable Concurrent error Detection Architectures for Extended Euclidean-Based Division Over GF(2^m)”, IEEE Transactions on very large scale integration (VLSI) Systems, Vol. 22, No. 5 May 2014.