An Optimized Encryption Method for Improving Image Security

[1] Dr. Jitendra Singh Chauhan, [2] Nimisha Khetan

[1] Associate Professor and Head, [2] Research Scholar
[1, 2]Department of Computer Science and Engineering, Aravali Institute of Technical Studies, Udaipur, Rajasthan, India
Email – [1] chauhan.jitendra@live.com, [2] nimishakhetan94@gmail.com

Abstract: *Latin square image cipher is a bit level encryption method. It is a non - chaotic image cipher and directly defined on finite numbers. It can be effectively implemented with accuracy in software as well as hardware. For encryption and decryption process to generate keyed Latin squares a 256 bit key is used by LSIC, which resist brute force attacks due to larger key space. LSIC contains 3 Latin Square based encryption primitives, namely Latin square Whitening (XOR operation with Key), Latin Square Substitution and Latin Square Permutation, all of which are dependent on keyed 256 x 256 Latin square. Hence LSIC sensitive to key changes.*

In this paper we propose a method to enhance security of an image and its results are compared with previous ones. The LSIC in substitution permutation network achieve many desired properties of secure cipher including a large key space, high key sensitivities, uniformly distributed cipher text, excellent confusion and diffusion properties, semantically secure, robustness against channel noise. This encryption primitives construct LSIC in SPN, a structure proven to be effective and efficient to encrypt images with good confusion and diffusion properties. Encrypting a plaintext image multiple times will generate distinctive cipher text images even through the encryption key is unchanged, this property helps LSICs to a achieve a higher level of security and it completely prevents an adversary to sense identical plaintext images by observing identical cipher text images.

Key Words: *Encryption, Latin square, Key, Image, Substitution-permutation network.*

1. INTRODUCTION:

Due to the rapid growth of computer networks and advances in information technology, a huge amount of digital data is being exchanged over unsecured channels. Mainly information which is transmitted requires various security mechanisms for protecting valuable data. There are various applications of multimedia encryption in our day to day life. Colored images are communicated in a large amount over the network which, is the main basis of continues development in multimedia and network technologies.

Image data have strong correlation among adjacent pixels forming intelligible information. Three different ways to protect digital image data from unauthorized eavesdropping are cryptography, steganography and watermarking. Cryptography provides high level of security by development of various new technologies for transforming information between intelligible and unintelligible forms. It deals with the content confidentiality and access control. In secure communications using cryptography, which is the main focus of the present work, the encryption and decryption operations are guided by one or more keys.

2. CRYPTOGRAPHY:

Cryptography provides the various techniques for secure communication of data over networks. It generally, construct and analyze various protocols that deals with the various aspects of information security like confidentiality, integrity, etc. Modern cryptography combines various disciplines of engineering and sciences. There are various applications of cryptography in day to day like ATM cards, computer passwords, and electronic commerce, etc. Cryptography is the technique which we called as a synonymous of encryption, which convert the readable and under stable form of information into some other unknown form, which is decoded at the other end to get the desired information using decoding technique provided by the originator of the message, thereby secure data from unwanted persons.

3. THE NEED FOR CRYPTOGRAPHY:

The main emphasis of defence is based on physical security. Physical security is always not an appropriate option. Computers are mostly interconnected via appropriate communication channels for transferring data.

The five major principles of security are:
1. Confidentiality: assuring that private data remains private.
2. Authentication: Assuring the identity of all parties attempting access.
3. Authorization: assuring that a certain party attempting to perform a function has the permissions to do so.
4. Data integrity: assuring that an object is not altered illegally.
5. Non-Repudiation: assuring against a party denying a data of a communication that was initiated by them.

4. OBJECTIVE:

To overcome the drawbacks of chaotic systems we use symmetric Latin square image cipher in bit level image encryption. LSIC contains three Latin square based encryption primitives, namely Latin Square Whitening, Latin Square Substitution and Latin Square Permutation, all of which are dependent on a keyed 256×256 Latin square. Hence LSIC is sensitive to key changes. Further, these encryption primitives construct LSIC in a SPN, a structure proven to be effective and efficient to encrypt images with good confusing and diffusion properties. In plus, we integrate the probabilistic encryption in LSIC by embedding random noise in the least significant bit plane of a plaintext image. Consequently, encrypting a plaintext image multiple times will generate distinctive cipher text images even though the encryption key is unchanged. This property helps LSIC to achieve a higher level of security and it completely prevents an adversary to sense identical plaintext images by observing identical cipher text images. LSIC provide demonstrate the robustness and effectiveness using extensive theoretical analysis simulation results and comparisons to peer algorithms.

5. LATIN SQUARES:

A Latin square of order N is N ×N array filled with a symbol set of n distinctive elements, with each symbol appearing exactly once in each row and each column. The name Latin Square is developed by the mathematician Leonhard Euler, who used Latin characters as symbols. Mathematically, we can define a Latin square L of order N via a tri-tuple function fL of (r,c,i) as follows:

$$f_L(r,c,i) = \begin{cases} 1, & L(r,c)=S_i \\ 0, & \text{Otherwise} \end{cases}$$

Where r denotes the row index of an element in L with r € N {0, 1,…….N-1};c denote the column index of an element in L with c € N; I Denotes the symbol index of an element in L with i € N; and Si is the ith symbol in the symbol set S={S0, S1……SN-1}.

If, L is a Latin Square of order N,

- for arbitrary c, i € N, we have

$$\sum_{r=0}^{N-1} f_L(r,c,i)=1$$

- for arbitrary r, i € N, we have

$$\sum_{c=0}^{N-1} f_L(r,c,i)=1$$

6. SUBSTITUTION – PERMUTATION NETWORK

In cryptography, an input message and its corresponding output message of a cryptosystem are referred to as plaintext and ciphertext, respectively. A substitution- permutation network is a cipher structure composed of a number of substitution and permutation ciphers with multiple iterations. This structure is widely used in many well-known block ciphers, e.g. Rijndael i.e. AES [5], and ensures good confusion and diffusion properties [12].

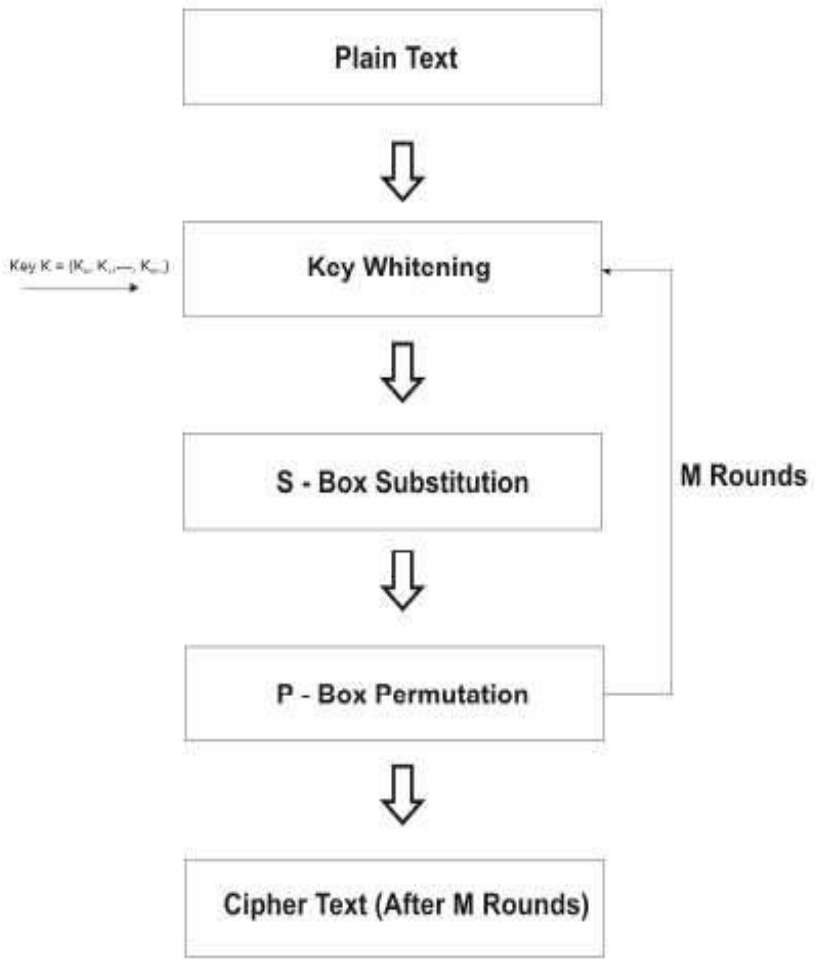

Figure 1 M- Round SPN with key whitening for Block Ciphers

A typical M – round SPN for block ciphers has a structure shown in above figure. Conventionally in a SPN. Plaintext, commonly in the form of a bit stream and denoted as P, is the original message to be encrypted. Key Whitening denotes an operation to mix the plaintext P with a round key: S Box denotes a substitution – box which maps one input byte to another in a deterministic way: P Box denotes a permutation- box, which shuffles bit positions within the input bit stream in deterministic way; and cipher text denotes the output bit stream C, which is an encrypted message by the SPN. The decryption process of SPN cipher is simply to reverse the arrow directions of all processing and to use inverse S-Box and inverse P-Box instead.

The classic SPN ciphers are able to obtain good Shannon's confusion and diffusion properties [27]. For the diffusion property: if one changes one bit in plaintext P, the corresponding cipher text C changes in many bits. This one-bit change result in a different byte after passing through S-Box, then leads more byte changes after passing through a P-Box, so on and so forth in each cipher round. Finally, one- bit change leads to significant changes in ciphertext C. The confusion property is the same as the diffusion property. One bit change in encryption key K, will spread over all bits and result significant changes in ciphertext C.

7. LSB NOISE EMBEDDING:

Probabilistic encryption [8], [9] means to use randomness in a cipher, so that this cipher is able to encrypt one plaintext with the exact same encryption key to distinctive cipher texts. It is well known that such randomness is crucial to achieve semantic security [4]. We introduce such randomness by embedding noise in the least significant bit-plane of an image. More specifically, we XOR a randomly generated 256×256 bit-plane with the least significant bit plane of the plaintext image where the generation of this random bit plane is completely independent of the encryption key.

Fig 2 shows an example of LSB noise embedding. These, introduced noise in LSB does not affect any image visual quality from the point view of human visual perceptibility. However any slight change in plaintext here will lead to significant changes in cipher text after it is encrypted by the SPN.

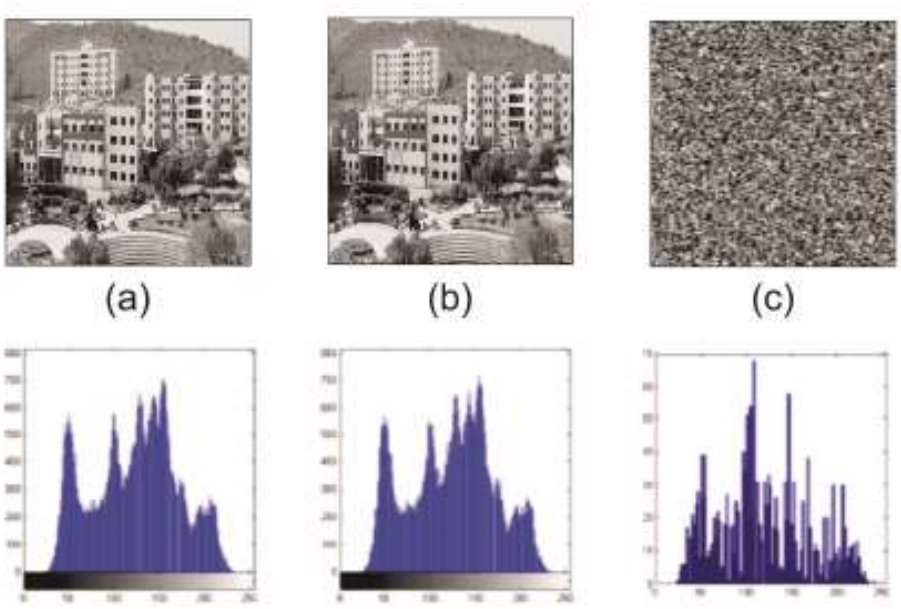

Figure 2 Noise Embedding at LSB (a) Plaintext image (P) and corresponding Histogram (b) Noise Embedded image (P') and corresponding Histogram (c) |P – P'| image and corresponding Histogram.

8. Encryption Algorithm:

Latin Square Image Cipher-Encryption C=(P.K)

Require: K is a 256 bit key.
Require: P is a 256 × 256 8-bit grayscale image block.
Ensure: C is a 256 × 256 8-bit grayscale image block.
(Q1. Q2) = KDSG (K,8)

```
for n=0:1:7 do
if n== 0 then
CLSP=LSBNoiseEmbedding(P)4
end if
Ln=LSG(Q1n. Q2n)
Dn=Ln(0,0)
CLSW=Ecrw(Ln,CLSP,Dn)
If mod(n,2)≠0 then
CLSS=Ecr8
col (Ln,CLSW)
else
CLSS=Ecr8
row(Ln,CLSW)
end if
CLSP=EcrP(Ln,CLSS)
end for
L8=LSG(Q18. Q28)
D8=L8(0,0)
C=ECrw(L8,CLSP,Dn)
```

9. Noise Robustness Analysis:

A good cipher should also be capable of tolerating a certain amount of noise e.g. noise in a channel or decoding errors. As discussed previously, the proposed Latin square image cipher adopts an asymmetric structure for encryption and decryption, and one noisy pixel in ciphertext image will only propagate in a factor of two in each round Fig. 3 shows the results of the decryption robustness of the Latin square image cipher against various noise ratio in ciphertext images. After decryption, noise concentrating in the center square of a ciphertext image now distributed almost evenly over the deciphered image. Human vision system is still able to recognize the deciphered image contents as long as it is not fully unintelligible, due to the psychovisual redundancy within an image.

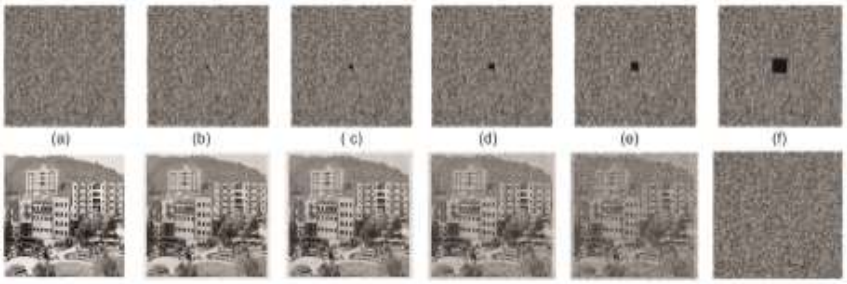

Figure 3 Sample results of noise robustness in decryption (having different percentage of noise embedded)

10. CONCLUSION & FUTURE WORK:

In this paper, we have suggested a symmetric key Latin Square Image Cipher with probabilistic encryption for grayscale and color images. This new image cipher has distinctive characteristics:

1. LSIC is purely defined on integers. It can be executed in hardware and software without causing any accuracy problems.
2. LSIC generates all encryption ciphers based on one keyed Latin square, including XORing (whitening), substitution and permutation. Therefore it attains high sensitivities to any key change;
3. LSIC encrypts and image pixels in the unit of byte instead of bit and processes a 256 x 256 plaintext image at one time.
4. LSIC arranges all these encryption primitives in the framework of substitution permutation network (SPN) and thus it attains good confusion and diffusion properties [10];
5. LSIC integrates probabilistic encryption in a pre-processing stage and thus is allows to encrypt a plaintext image into different ciphertext images when the same encryption key is used.

The effectiveness and robustness of LSIC have been demonstrated by extensive simulation results using the complete USC – SIPI Miscellaneous image dataset. Theoretical security analysis shows that LSIC has good resistances to brute-force attacks, ciphertext only attacks, known-plaintext attacks and chosen-plaintext attacks. Experimental security analysis with comparisons to peer algorithms indicates that LSIC reaches state of the art. The LSIC is very suitable for digital image encryption demonstrate by all these analysis and results.

REFERENCES:

1. A. Sinha and K. Singh, “A technique for image encryption using digital signature”, source: Optics Communications, vol. 218, no. 4, (2003), pp. 229-234.
2. N.K. Pareek, Vinod Patidar and K.K. Sud, (2011) “A symmetric encryption scheme for colour BMP images”, International Journal on Computer Applications, NSC (2), pp. 42-46.
3. Yue Wu, Joseph P, Noonan and Sos Again, (2011) “NPCR and UACI Randomness Tests Image Encryption”, Journal of selected Areas in Telecommunications, pp.31- 38.
4. Yue Wu. Y. Zhou, J. P. Noonan, K. Panetta, and S. Agaian, “Image encryption using the LSIC symmetric key patterns,” S. S. Agaian and S. A. Jassim Eds., vol 7708, no. 1. SPIE, 2012.
5. GulQuiuang Hu, Di Xio, yongwang, Xinyan Li “Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion” Springer Edition, vol88, no. 2., April, 2017**,** pp. 1305-1316.
6. Padampriya Praveen Kumar, R. Amirtharaja, John Bosco “Fusion of confusion and diffusion: a novel image encryption approach”Springer Edition, vol65, no. 1, May, 2017**,** pp. 65-78.
7. X.Liao, S.Lai, and Q.Zhou, “A novel image encryption algorithm based on self-adaptive wave transmission”. Signal Processing vol. 90, no. 9, pp. 2714-2722, 2010.
8. A. Awad, “A new chaos-based cryptosystem for secure transmitted images”, Computers, IEEE Transactions on, vol. PP, no. 99, p. 1,2011.
9. A.Kumar and M.K.Ghose, “Extended substitution-diffusion based image cipher using chaotic standard map, “Communications in Nonlinear Science and Numerical Simulation, vol. 16, no. 1, pp. 372-382, 2011, doi: DOI: 10.1016/j.cnsns. 2010.04.010.
10. E.Solak and C.C, okal “Comment on “encryption and decryption of images with chaotic map lattices “,” vol. 18, no. 3, p. 038101,2008.
11. S.Li, X. Mou. Y. Cai, Z. ji, and J.Zhang, “On the security of a chaotic encryption scheme: problems with computerized chaos infinite computing precision”. Computer Physics Communications, vol. 153, no. 1, pp. 52-58, 2003.
12. G.Alvarez, S.Li, and L.Hernandez, “Analysis of security problems in a medical image encryption system,“ Computers in Biology and Medicine, vol. 37. No. 3, pp. 424-427, 2007.