RESEARCH REVIEW JOURNALS
Volume-04
Issue-04
April -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Implementation of Star-Lock Encryption Algorithm for Secure Image Transformation

Persia A

Assistant Professor, Department of Computer Science, Vidhya Sagar Women's College, Chengalpattu, Tamilnadu (India)

ARTICLE DETAILS

Article History
Published Online: 15 April 2019

Keywords
Star-Lock, Public Key, Arduino board, Encryption, Decryption

***Corresponding Author**
Email: persia.sampan17[at]gmail.com

ABSTRACT

The encryption techniques nowadays play a very important role in securing sensitive data in all means of communication. As the rate of electronic crimes has been increased, the process of capturing and transferring images through network should be secured with low cost method. The secured image transformation provides authentication of user's integrity and safety of images over a network. Our main objective focuses on improving public key cryptographic algorithm that involves robust encryption and decryption techniques. In this project, STAR-LOCK encryption algorithm is proposed based on a new permutation technique for image encryption with embedded platforms using Arduino board. Arduino board is a microcontroller, supported with image capturing tool and external memory. It is used under Arduino IDE. From the captured image, the binary value blocks are calculated which will reorganize into a permuted image. Finally, the generated image will be encrypted/ decrypted using STAR-LOCK algorithm.

1. Introduction

Image capture has become an integral part of the security of any premises and organization. In this paper an OV7670 VGA cMOS Image sensor is interfaced with an Arduino Board for capturing still images. The process of assessing the threat involves transmitting the images to the consumer. The data delivery and sharing process, usually based on CD/DVD-ROM or on shared network environment (LAN, Internet, WAN etc), offers the user with digital version of the remote sensing images and data. In the same method as for multimedia system contents, the digital set-up implies an intrinsic risk of illegal copy or utilization of the product. The speedy development of Internet in the digital world today, the protection of digital images has become more and more important. The occurrence of multimedia technology in our people has endorsed digital images to play a more considerable role, which demands a serious guard of users' privacy. Similarly, many digital services, such as Medical, Military, and Space imaging systems require reliable protection in transmission and storage of digital images. To achieve such privacy and security needs in different applications, encryption of images is most important to reduce malicious attacks from illegal parties [4].

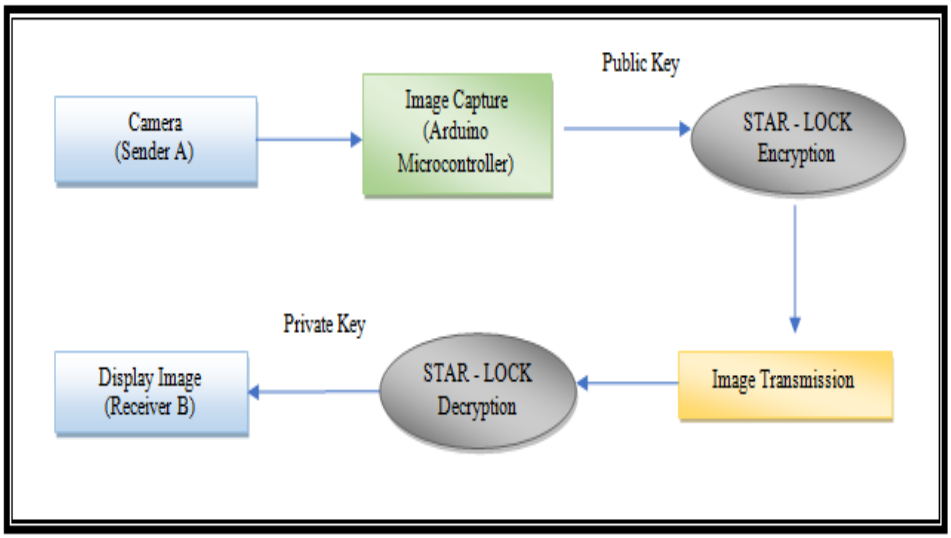

Fig.1 Secure Image Transmission Using STAR-LOCK Algorithm

In order to provide unobtrusive transmission of data, suitable encryption and decryption is provided and the scheme is shown in Fig.1.In this context, there are a number of Algorithms proposed and implemented so far for the encryption and decryption of images. Earlier, based on Magic Rectangle (MR), new image encryption algorithm was proposed. In this work a plain-image is changed into block of single bytes and then the block is substituted as the value of MR [1]. Hiral Rathod et al. had proposed permutation technique for image encryption [2]. Baidaa A. Atya et al. also employed permutation technique using Arduino Board for encryption and decryption. This paper focus on combining two algorithms to make a more efficient algorithm known as STAR-LOCK.

2. Proposed STAR-LOCK Algorithm

STAR-LOCK algorithm is hybrid algorithm derived from a synchronous public key cryptography algorithm as well as asynchronous RSA algorithm. The advantages of this hybrid algorithm are to make a faster encryption and a much-secured key model. The STAR-LOCK algorithm uses a highly advanced permutation technique to encrypt an image and decrypt it to a specified device using the private key. Proposed algorithm improved version of the existing RSA and Block Cipher-Based Transformation Algorithm (AES, DES, 3DES) algorithms. From the selected image, the binary value blocks are calculated, which will be reorganize into a permuted image using a permutation process, and then encrypted using STAR-LOCK algorithm. The encrypt component is used to hide visual information such as bmp or jpeg image. The encrypted image is known as Cipher. The decrypt component is used to get the original image from hidden visual information.

2.1 Description of the STAR-LOCK algorithm

Choose two large distinct primes p and g and then form the public modulus n = pq.

- Choose public exponent e to be co-prime to (p − 1) (g − 1), with 1< e < (p − 1) (g − 1). The pair (n, e) is the public key.
- The private key is the distinctive integer 1 < d < (p − 1) (g − 1) such that ed = 1 mod (p − 1) (g − 1).

Encryption: Divide a Image M into a series of blocks M1, M2, Mt where each Mi satisfies 0 ≤ Mi < n. Then encrypt these blocks as follows.

2.2 Decryption

- Given the cipher text C and the private key d, the decryption is the inverse process with different key(d).
- Encryption does not enlarge the size of a message. Both the cipher text and the message are integers in the range 0 to n - 1.
- The encryption key is the twosome of positive integers (e; n).
- Similarly, the decryption key is the couple of positive integers (d; n). In STAR-LOCK algorithm encryption key is public and keeps the corresponding decryption key private.

Step 1: Initialize the state array with the block data (encryption for a 128-bit block). Input is considered as image (.jpeg) is being converted to 128-bit plain text.

Step 2: Calculate Image Pixels Value of M
Horizontal Value of Pixel =PixelWidth/10
Vertical Value of Pixel = PixelHeight/10

Step 3: Further 128-bit text is being splitted into two sets of 64-bit plain text data.

Step 4: Next this 64-bit plain text is being specified as input to block cipher algorithm which encrypts to offer encrypted 64-bit text.

Step 5: Enciphering a 64-bit data block and key using the STAR-LOCK algorithm consists of: An initial permutation (IP). The permuted plaintext is divide into two halves, right and left. Right half text moves to the left with no manipulation, and left half is XORed with the output of a function F that acquire round key and right half as inputs 16 rounds of a complex key dependent calculation (f)

Step 6: A final permutation, being the inverse of (IP): The output is treated as 8 blocks of 1 byte each. The 8 blocks are then shuffled and passed through 8 different STAR-LOCK like substitution boxes (S1 to S8). The outcome of the 8 Substitution boxes are combined again to 64 bits, and then passed to a second permutation P2, which directed to the final output of the F function.

Step 7: Repeat the same for all m blocks.

3. STAR-LOCK Algorithm Implementation

The STAR-LOCK Algorithm is implemented in java programming language using windows operating system. For network image transmission using Arduino system, Java supports Socket Programming in LAN environment. For this it includes a special package called ava.net. JAVA supports GUI environment through which a user can interact with the system dynamically (at run time). The STAR-LOCK algorithm encryption is not limited to the file size, but depending on this, the key length varies i.e. 128, 192, 256 bits. Whenever we want to encrypt a particular file, the algorithm divides the file contents into blocks of 128 bits. Now these bits are stored in an array of bytes. From this array, the bytes are transformed into a state. The state is divided into rows and columns. In this algorithm, the number of rows is constant i.e. 4 and the number of Columns depend on the key lengths i.e. If the key length is n, the number of columns are n/32. Here, each cell in the state is of 1 byte i.e. equivalent to 8bits and 4 bytes in a Column will form one word i.e. equivalent to 4 * 8 = 32 bits and this entire state is of 128 bits i.e. 4 * 4 =16 * 8 =128 bits. The similar procedure is followed in the Cipher key also. Now, the state is ready for encryption process and the cipher key for key scheduling. Now, by using the matrix, the Algorithm will calculate 10 round keys, each being Utilized in 10 rounds. Thus, to calculate Wi word, the algorithm will consider Wi-1 word and perform Root Word, calculates the Sub Bytes for this and Selects Wi-4 word to perform XOR operation. To this XORed result, the Algorithm will select a column from STAR-LOCK Graph, which is a standard table, performs XOR addition and result is placed in the Wi word. Now, to calculate

the next word, the algorithm considers Wi word and performs XOR addition with Wi-4 word and result is placed in the Wi word. The similar procedure continues for the remaining Columns also. For our experiment, we use a laptop Pentium® 32-bit Operating System and Dual-Core CPU T4400 @2.20Ghz. The algorithm was applied on a JPEG image that has the size of 300 pixels x 300 pixels with 256 colors. In order to assess the impact of the number of blocks on entropy, and here entropy is calculated using following equation Entropy defined as [5]

$$He = -\sum_{K=0}^{G-1} P(K) \log 2(P(K)) \ldots\ldots\ldots (1)$$

Where: *He*: entropy., *G*: gray value of input image (0... 255), *P(k)*: is the probability of the occurrence of symbol *k*.

4. Conclusion

This paper focuses on creating a *STAR-LOCK* algorithm for transformation and permutation of image data. *STAR-LOCK*, which is a hybrid algorithm, is derived from RSA public key generation and AES (Block Cipher cryptographic algorithm). The algorithm uses the Public key encryption method and for decryption keeps the key in private to ensure security. The proposed hybrid technique provides high protection level, a reduced amount of computational time and power in efficient and reliable way to deal with difficult and intractable data, particularly for images.

References

1. D.I. George Amalarethinam and J. Sai Geetha (2015) 'Image encryption and decryption in public key cryptography based on MR' International Conference on Computing and Communications Technologies (ICCCT).
2. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, 'Design and Implementation of Image Encryption Algorithmby using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)', International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, Issue 3, pp 7-13.
3. Baidaa A. Atya et al. (2016) 'Encryption of Video Images Using Arduino Card', International Journal of Scientific & Engineering Research, Volume 7, Issue 7, pp 539-549.
4. Prof. Dr. Sudan Jha et al., (2016) 'Chaotic Image Encryption Technique'" International Journal of New Innovations in Engineering and Technology, ISSN 2319-6319, Volume 6 Issue 1.
5. D. Feldman, 'A brief introduction to: information theory, excess entropy and computational mechanics,'college of the atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/

