IMAGE ENCRYPTION USING SCAN PATTERN

[1]SAISUBHA V, [2]PRIYANKA U, [3]REMYA K R & [4]REENU R

First year M.Tech students, Department of Computer Science and Engineering, Mohandas College of Engineering and Technology, Thiruvananthapuram, Anad Thiruvananthapuram
Email: saisubhav@gmail.com, priyankayou@yahoo.in, remykr@gmail.com, reenu.rahman@gmail.com

Abstract—With rapid growth in communication and computer technologies, there is a huge datatransaction in mobile, internet, TV, teleconferencing, telemedicine and military applications. Data security is important.Encryption is one of way to give security for data,in this regard this paper proposed a scanpattern technique for image encryption.It involves rearranging of mapping image based on scanpattern. Decryption is also done for reconstruction of original image.

Keywords—Scanpattern,Mapping,Encryption,Decryption.

I. INTRODUCTION

Image encryption schemes have been increasingly developed to meet the requirements for secure transmission over the communication channels. In the digital world today, the security of digital images becomes more and more important, since the communications of digital products over networks occur more and more frequently. reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image database and communications as well as confidential video conferencing, etc. In recent years, some consumer electronic devices, especially mobile phones and hand-held devices have also started to provide the function of saving and exchanging digital images via the support of multimedia messaging services over wireless networks. There are several image encryption methods, each of them having their own strength and weakness. Ismet Ozturk and Ibrahim Sogukpinaar have discussed the analysis and comparison of image encryption algorithms. And they classify the image encryption methods in to three major types: position permutation, value transformation and visual transformation. A Mitra have presented a new approach for image encryption using combination of different permutation techniques. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. S. R. M. Prasanna have presented an image encryption method. with magnitude and phase manipulation using carrier images. N. K. Pareek and Xiaojun Tong have used chaotic sequence for image encryption.

It used the concept of carrier images and one dimensional Discrete Fourier Transform for encryption purpose and it deals with private key cryptosystem, works in the frequency domain. S.S. Maniccam and N.G. Bourbakis have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based two-dimensional spatial accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. C. Kachris have designed a detailed architecture for SCAN algorithms. N. K. Pareek and Xiaojun Tong have used chaotic sequence for image encryption. Said E. El-Khamy proposed a paper on partial encryption system based on chaotic system. Bibhudendra proposed a novel advanced ill encryption technique .

II. PROPOSED SYSTEM

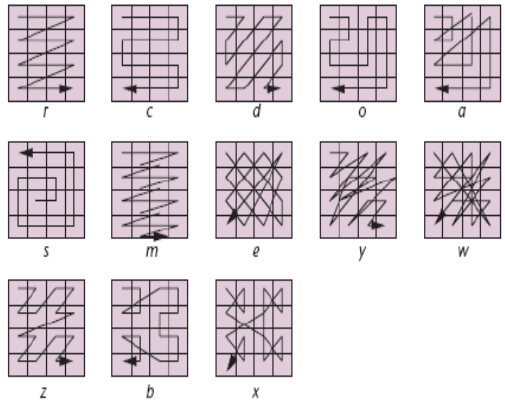
This method converts a 2D image into a 1D list, and employs a SCAN language to describe the converted result. In this language, there are several SCAN letters. Each SCAN letter represents one kind of scan order. Different kinds of combinations of SCAN letters may generate different kinds of secret images. After determining the combination of SCAN letters, scan letters then generates a SCAN string. This string defines the scan order of the original image. Next, this method scans the original image in the determined order and, moreover, encrypts the SCAN string by using commercial cryptosystems. Since the illegal users cannot obtain the correct SCAN string, the original image is therefore secure. No image compression is used in this method. Therefore, the size of the image is very large, and thus it is inefficient to encrypt or decrypt the image directly.
The SCAN represents a family of formal languages based on two-dimensional spatial accessing methodologies, which can represent and generate a large number of scanning paths easily. The SCAN family of formal languages includes several versions such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. Each SCAN language is defined by a grammar rules to compose

simple scan patterns, which in turn are used to obtain complex scan patterns from simple scan patterns production rules of the grammar of each specific language. The basic idea of the proposed encryption method is to rearrange the pixels of the image and change the pixel values. The rearrangement is done by a set of scanning patterns(encryption keys) generated by an encryptionspecific SCAN language, which is formally defined by the grammar *G*.
The basic idea of this image encryption method is to rearrange the pixels of the image and change the pixel values. The pixel rearrangement is done by scan keys. The pixel values are changed by a simple substitution mechanism, which adds confusion and diffusion properties to the encryption method. The permutation and substitution operations are applied in intertwined and iterative manner. First, the encryption algorithm is described in detail. Next, the confusion and diffusion properties of the algorithm are presented in detail, and experimental results are shown to demonstrate properties of the encryption method, as well as pixel rearrangement. Finally, various extensions of the encryption method and the size of the encryption key space are discussed.
The SCAN algorithm is a block cipher algorithm are the RSA, the DES, and AES algorithms. The SCAN algorithm is a block cipher that uses large blocks and not just 56-bit or 256-bit blocks. The main advantage of the SCAN algorithm is its strong encryption rather than its high throughput. The encryption key actually consists of four components, namely, the two scan keys $k1$and $k2$, the random seed integer p, and the number of encryption iterations m. These four encryption key components are known to both the sender and the receiver before the communication of encrypted image. The random numbers needed by *Encrypt*() can be obtained by any method such as a linear congruential generator with seed p. The encryption algorithm uses four scan keys to increase the complexity of pixel rearrangement.

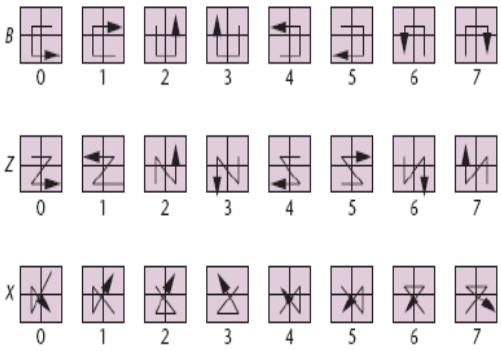
The keys $k1$ and $k2$ are specified by the user as part encryption key. The other two keys spiral $s0$ and diagonal $d0$ are fixed as part of encryption algorithm. These two keys $s0$ and $d0$ are chosen because they have opposite directions of scanning and hence increase the complexity of pixel rearrangement caused by the user specified keys $k1$ and $k2$. Note that the user generates keys $k1$ and $k2$ using the SCAN grammar. The secure encryption method satisfy the properties of confusion and diffusion. The confusion property which require that cipher text having random appearence. The diffusion property with respect to plaintexts (original data) and keys, which requires that similar plain texts produce completely different cipher texts when encrypted with the same key, and similar keys produce completely different cipher texts when encrypting the same plaintext. A single change in encryption scan key also changes all pixels in iteration, because a change in scan key causes at least one pixel to be changed, which causes all pixels to be changed.

The properties of the SCAN image encryption method, which include pixel rearrangement, confusion, and diffusion. The Simple Scan Patterns are algorithm that calculates the Scan address using some iterative loops. The software implementation of the C Scan algorithm consists of two nested loops. The boundaries of these loops depend on the transformation number. The diffusion and the confusion property is based on a formula that alters the pixel's value using a random number. The Substitution Units are used to change these pixels. The SCAN image and video encryption algorithm and an architecture for its efficient implementation in reconfigurable logic. The SCAN algorithm can be used for information hiding. The SCAN architecture can be used to encrypt data transmitted over a network.

Image is a multimedia component sensed by human. The smallest element of a digital image is pixel. In a 32 bit digital image each pixel consists of 32 bits, which is divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. If all bits of Alpha part are '0', then the image is fully transparent. This paper proposed an encryption algorithm for encryption of image. Algorithm to divide a digital color image into n number of shares where minimum n numbers of shares are sufficient to reconstruct the image. An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image is also taken as input from user. The encryption, i.e. division of the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the encryption algorithm. The basic idea of the proposed encryption method is to rearrange the pixels of the image and change the pixel values. The rearrangement is done by a set of scanning patterns(encryption keys) generated by an encryption-specific SCAN language, which is formally defined by the grammar *G*. and an architecture for its efficient implementation in reconfigurable logic. The SCAN algorithm is a block cipher algorithm are the RSA, the DES, and AES algorithms. The SCAN algorithm is a block cipher that uses large blocks and not just 56-bit or 256-bit blocks The main advantage of the SCAN algorithm is its strong encryption rather than its high throughput. The basic idea of the proposed encryption method is to rearrange the pixels of the image and change the pixel values. The rearrangement is done by a set of scanning patterns(encryption keys) generated by an encryptions specific SCAN language, which is formally defined by the grammar *G*



(a)



(b)

Fig 1: (a) Basic scan pattern (b) Partition patterns and transformation

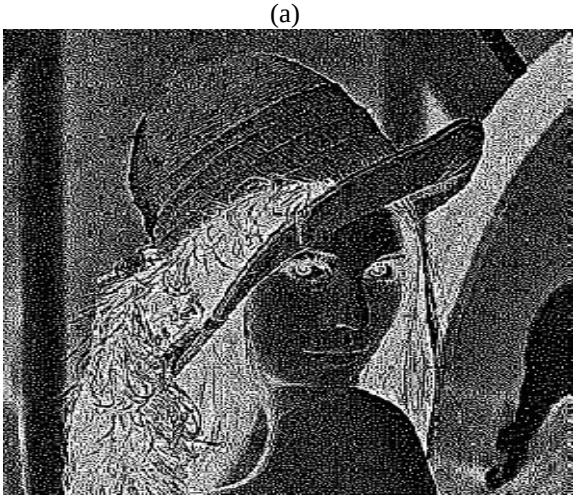
In this method, selecting the mapping image based on scan pattern. It will convert every pixel of mapping image and then it should be converted into its equivalent 8-bit binary number. In the next step, rearrange these 8-bit binaryinto 4-bit higher and lower nibble number. Convert these two 4-bit nibbles into its equivalent decimal value. With the help of these two decimal values pickup the gray pixel from the mapping image. Where higher nibble equivalent decimal value acts as row indicator and lower nibble equivalent decimal value acts as column indicator for mapping image.

Decryption is the reverse process of the encryption.It is implemented by using decryption algorithm. In the case of decryption, for computer generated program; OR function can be used. Here the numbers of shares are taken as input from user. As the shares are created from the image taken as input in encryption algorithm, each share must be of equal height and width as the source image. Then bitwise OR operation is performed among pixels of the shares, and final pixel values are stored in an array.

III. EXPERIMENTAL RESULT

This section shows the experimental result of image being encrypted by using technique of scan pattern. Encrypted image is transmitted from sender. It also show the decryption of this secret image by applying decryption at the receiver side.

(a)

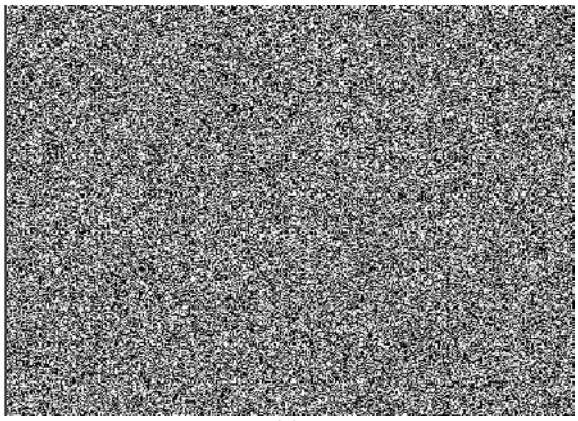


(b)

Fig 2:(a) Input image(b) Halftoning of input image

The above figure shows the input image. The next step involves the halftoning of input image. It is done by filtering the image. The filters are used to eliminate the noise. Halftone is applied on image. Image is treated as gray-scale image and transformed into binary image.

Halftoning is achieved by the input image is decomposed into three channels of Cyan, Magenta and yellow. Filtering of image is to eliminate noise and for sharpening the image. Image is filtered and decomposed into three channels.



(a)

(b)

Fig 3:(a) Encrypted image(b) Decrypted image

The above figure shows the encryption of the input image. After halftoning the decomposed channels of cyan, mangenta and yellow were encoded to form an encrypted image. The next step involves decryption of image by applying decryption algorithm and finally reconstruct the original image at the receiver side.

CONCLUSION

In this paper, I proposed a combined and effective method of scan pattern and partial image encryption method for encryption of data.

It also reconstruct the original image by using decryption technique. From the experimental results. It can confirm that scan pattern is more efficient for image encryption.

REFERENCES

[1] Ismet ozturk and Ibrahim sogukpinaar," Analysis and comparison of image encryption algorithms,"Transaction on engineering computer and t Technology, 2004, vol.3, pp.38-42.

[2] Mitra et.el., "A new Image Encryption Approach using combinational Permutation Techniques",IJCS,2006 vol.1,No.2,pp.127-131.

[3] S.R.M.Prasanna et.el., "An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images",IJCS,2006,vol.1,No.2,pp.132-17.

[4] S.S.Maniccam and N.G.Bourbakis, "Image and Video encryption using SCAN patterns",Pattern Recognition,2004,vol.37,pp.725-757.

[5] Chao Shen Chen and Rong Jian Chen, "Image Encryption and Decryption using SCAN Methodology",Proc.PDCAT,2006.

[6] N.K.Pareek et.el.,"Image encryption using Chaotic logistic map,"Image and Vision Computing,24,2006,pp.926-934.

[7] Xiaojun Tong and Minggen cui, "Image Encryption with Composed Chaotic Sequence Cipher Shifting Dynamically",Image and Vision Computing,28,2008,pp.843-850.

[8] C.Kachris et.el.,"A reconfigurable logic based processor for the scan image and video encryption algorithm",IJPP,vol.31,No.6,Dec 2003,pp.489-506.

[9] Bibhundendra Acharya et .el. ,"Image encryption using advanced hill cipher algorithm",International Journal of recent trends in engineering,ACEEE,vol.1,o.1,May2009.

[10] Said E.El-Khamy, "A partial image encryption sheme based on the DWT and ELKNZ chaotic stream cipher",MASAUM Journal of basic and applied science,vol.1,No.3,October2009.

★★★