IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016.
www.ijiset.com

ISSN 2348 – 7968

Image Encryption Using KIST-A Case Study

Anandhu M Kovoor[#1], Vijin Kurian Varghese[#2], Sushitha Susan Joseph[#3]

[1]*Student B.Tech, Computer Science & Engineering, MBCCET, Peermade, Kerala, India*

[2]*Student B.Tech, Computer Science & Engineering , MBCCET, Peermade, Kerala, India*

[3]*Assistant Professor, Computer Science & Engineering, MBCCET, Peermade, Kerala, India*

[1]*anandhum1994@gmail.com*

[2]*vijin76@gmail.com*

[3]*sushisusan64@gmail.com*

Abstract: *Image encryption algorithms are used to generate encrypted image so that it is so difficult make prediction of pixels value by attackers. There are many algorithms are founded until now for partial as well as complete image encryption and decryption process and thereby providing much security for images for communication purposes. This paper proposes a new method for image encryption, a layer based method combining some most efficient image encryption algorithms .Now a days there are many vital applications are performing on the basis of image encryption methods. This paper provides a different image encryption based on KIST algorithm. KIST algorithms are mainly used for searching purposes .And we uses it for encryption of images.*

Keywords: Splay tree, Edge detection, permutation, significant and insignificant image spaces

I. INTRODUCTION

First of all we need to know what is meant by encryption. Encryption is the most commonly used method to achieve possible security for data's. The data may be of any formats like images, videos, audios, documents etc. A data that is not encrypted is called as a plain text and that is encrypted is called as a cipher text. To read an encrypted data, we need to decrypt it. For this purpose, we need a password or a key. This key is known by the sender and receiver.

There are two types of encryptions are there, Symmetric and asymmetric encryptions. In Symmetric encryption method, same key is used by both sender and receiver. But in asymmetric encryption, the keys are used by sender and reciever are different.

In this paper, we propose a new encryption algorithm called KIST (key insertion and splay tree encryption). The characteristics of this KIST are:

• A splay tree is used so that the substitution is dynamic.

• The encryption is fast and uses small space.

• Cipher texts are compressed in most cases.

Splay trees were first proposed in 1983 by Sleator and Tarjan in and the details were presented in 1985. Splay trees were originally intended as self-balancing binary search trees with the property that recently accessed nodes are quick to access again. This property was applied to data compression by Jones . The difference between a compression splay tree and a search splay tree is that the compression tree does not require a lexicographic ordering of the nodes, that simplifies the algorithm.

In general, the method suggested in is not secure. Using splay trees, the more frequent used bytes will be encoded into shorter codes. So the ciphertext definitely will give some information to the attacker. However, the method using splay tree for encryption has some attractive characteristics. It is efficient in regarding both time and space. The splay tree compression operation needs only 2 KB to 4 KB memory. Also the cipher text is compressed under this method. In this paper, we will propose a new encryption algorithm which applies some techniques of splay trees.

ISSN 2348 – 7968

Every day huge amount of multimedia data is transmitted through the World Wide Web which poses some real security issues, such as unauthorized access. Data encryption comes to field to overcome these issues and improve the security level of digital world. Each kind of data has its own features. Different representations of information like text, voice, video and image can be individually considered for encryption using appropriate techniques basis on their inherent specific features.

There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Furthermore some encryption schemas have embedded facilities into their own techniques such as compression; region based selective, independent encryption and so on.

I. EXISTING SYSTEM

In the paper, Combinational domain encryption for still visual data, proposes a new framework of combinational domain encryption that encrypts significant data in spatial domain and insignificant data in wavelet domain. Experiments have been performed to analyze the effect of proposed framework as compared to encryption technique in a single domain. Significant reduction in computational time has been observed without compromising on the security. Medical applications or security applications requiring fast computation would be benefitted by implementation of the proposed technique.

This paper, thus, proposes a combinational domain based encryption technique that considers data significance while encrypting the entire image data. The proposed combinational domain encryption framework contemplates data significance in spatial domain and provides corresponding security level to data of different significance. The significant part of image data is totally encrypted in spatial domain while the insignificant part is partially encrypted in wavelet domain.

In the Paper, Selective Image Encryption Using JBIG, they propose a selective encryption scheme with extremely low encryption demand focussed onto listlessly encoded imagery which is based on the hierarchical progressive coding mode of JBIG. In order to be able to process gray scale images with this JBIG based approach, we use a biplane representation which has been discussed before in the context of selective bitplane encryption. The JBIG based approach improves the latter techniques significantly.

Joint Binary Image Experts Group is an ITU standard (ITU recommendation T.82) finalized in 1993 for compressing binary images and was meant to improve the fax compression standards of that time especially with respect to the coding of halftones images. JBIGs corecoding engineis a binary context-based adaptive arithmetic ccoder similar to the IBM Q-coder. In this section we will mainly focus on the hierarchical progressive coding mode of JBIG since the understanding of the associated techniques is crucial for the selective encryption technique described subsequently. As a first step a binary multiresoltion hierarchy is being constructed.

Additionally, two strategies bypass the arithmetic coder if pixel values may be determined without encoding the actual values:

Deterministicprediction(DP): Basedonknowledgea boutneighbouringpixel values of the current resolution layer, neighbouring pixel values of the layer with lower resolution, and the rule how the multiresolution hierarchy has been built, some pixel values are known without explicitely encoding them, the values may be derived from the other data.

Typical prediction(TP): In the lowest resolution layer this means that identical lines are coded only once. A following identical line is labelled as being “typical” by setting a corresponding flag and the content is not fed into the coder. In the remaining layers, for a “typical” pixel being surrounded by pixels of the same colour follows that the corresponding four pixels in the next higher resolution layer have the same colour.

When using the JBIG hierarchy for selective encryption only the lowest resolution of 5 layers may be encrypted, in this case for all bit planes. This results in encrypting 0.5% of the original data only. These two principles may be mixed additionally: it is possible to limit encryption to a subset of resolution layers of a selected set of bitplanes only.

ISSN 2348 – 7968

In the paper, Scan Based Lossless Image Compression And Encryption, they presents 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 a formal language based two dimensional spatial accessing methodology which can efficiently spec& and generate a wide range of scanning paths or space filling curves. This paper presents compression specific SCAN language, compression and decompression algorithms, encryption and decryption algorithms, and test results of the methodology.

The proposed compression - encryption method compresses a given binary image, by specifying a scanning path of the image using a SCAN pattern, and by specifying the bit sequence along the scanning path. For a given binary image, the compression algorithm determines a near optimal or a good scanning path which minimizes the total number of bits needed to encode the SCAN pattern and the bit sequence. After the binary image is compressed, the bits of the compressed image are rearranged using a set of SCAN patterns, which forms the encryption key, to obtain the compressed and encrypted image. A gray scale image is compressed and encrypted by applying the binary methodology to each bit plane of the gray scale image.

In the paper, Image Encryption and Decryption Using SCAN Methodology, they proposes an encryption method is based on SCAN patterns generated by the SCAN methodology. The SCAN is a language-based two-dimension spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths. Then scanning paths sequence fill in original image. Note that the scanning paths with random code generating procedure, which produces the encryption keys in a very many ways; so come to the quite secret system.

Each SCAN language is defined by a grammar and each language has a set of basic scan patterns, a set of transformation of scan patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns.

Above mentioned algorithm has its strength and weakness in terms of security level, speed, and resulting stream size metrics.

In the paper, image encryption using block-based transformation algorithm, we introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images Image encryption techniques try to convert an image to another one that is hard to understand . On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. The transformation technique works as follows: the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement.

In the paper, region based selective image encryption, a region based selective image encryption technique is proposed which provides the facilities of selective encryption and selective reconstruction of images. The concept of region based selective image encryption finds use in time-critical applications wherein security is also a

ISSN 2348 – 7968

concern such as, internet banking transactions, military image database and communication and medical imaging systems. Special and reliable security in transmission of digital images is needed in many applications, such as pay-TV, confidential video conferencing and corporate communications. Looking at the requirements of the hour and the existing techniques, the idea of region based selective image encryption finds a prominent place in the field of image Security. In this technique, the entire image is encrypted and decrypted each time, which is a big overhead in case of storage and retrieval of a large set of image sin an image database or transmission of images over an insecure channel. Also the loss of even a small part of the encrypted image results in greater distortion in the decrypted image.

II. PROPOSED SYSTEM

In our proposed system,Layer Based Image Encryption Using KIST Algorithm,we are using a layer based method combining some most efficient image encryption algorithms.

It is tried to take all encryption concerns into consider, achieve highest possible level of security while cost is already acceptable. The proposed method provides different security level to blocks of varied significance in image to consume less computational resources.

The layer based methods are focused on mainly 4 implementations and they are Segmentation, Localization, Permutation and finally Encryption.

Segmentation

This step deals with dividing the whole image into *N* number of non-overlapping blocks with variable size. Each block (region) is represented using a square matrix containing a specific number of pixels for each block size. This representative matrix is used for performing the operations on regions, each region is considered separately for encryption.

Localization

Image file has distinct regions which belong to different level of importance. Recently researchers exploit this feature of image file and develop a new approach which refers as partial encryption or selective encryption. Selective Encryption makes it possible to encrypt only some regions of the image. First we should search the image to extract the features and identify important regions of image, the work just let user to mark some region as important.

Permutation

Region permutation deals with interweaving the blocks of the image to build a newly transformed image. The perceivable information of an image is highly depended on the correlation among the image elements in a given arrangement. The PP algorithm efficiently permutes blocks with the help of Block Background Estimation (BBE) measure. BBE is the average of pixel intensity value for all pixels of the block. This algorithm simply acts in such way that minimizes the correlation in permuted image.

Encryption

Two procedures are designed to treat with blocks according to whether it is classified as insignificant or significant. Each insignificant block which is included less important information will encrypt using rescanning; a less complex methodology which introduced. Each significant block which has high potential to include critical information will encrypt using KISTalgorithm.

III. CONCLUSION

This paper proposed a new framework for image encryption, a layer based method combining some most efficient image encryption algorithms. In localization all blocks briefly are processed and identified as significant and in significant.In encryption layer various security levels is provided according to importance of the block using combination strategy.

The proposed method provides different security level to blocks of varied significance in image to

ISSN 2348 – 7968

consume less computational resources.Various analysis and experiments such as histogram, correlation coefficient, entropy, and computational time revealed that significant promotion in security has been achieved without compromising on the computational time.

IV. REFERENCES

1. "A Comprehensive Layer Based Encryption Method for Visual Data" Reza Moradi Rad, Abdolrahman Attar and Reza Ebrahimi Atani.

2. M. A. B. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG, International Journal of Computer Science, vol. 35, no. 1, **(2008)** February.

3. C. S. Chen and R. J. Chen, "Image Encryption and Decryption Using SCAN Methodology", Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taipei, Taiwan, **(2006)** December.

4. K. C. Ravishankar and M. G. Venkateshmurthy, "Region based selective image encryption Region based selective image encryption", International Conference on Computing and Informatic (ICOCI'06), Kuala Lumpur, Malaysia, **(2006)** June**.**

5. R. Pfarrhofer and A. Uhl, "Selective Image Encryption Using JBIG", Conference on Communications and Multimedia Security, **(2005)**, pp. 98-107.

6. S. S. Maniccam and N. G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption", International Conference on Information Intelligence and Systems, **(1999)**.

7. N. Taneja, B. Raman and I. Gupta, "Combinational domain encryption for still visual data", Journal of Multimedia Tools and Applications, **(2011)** March.