IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 3, March 2016.
www.ijiset.com
ISSN 2348 – 7968

Layer Based Image Encryption Using Kist Algorithm

Melbin Mathew[#1], Sushitha Susan Joseph[#2]

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

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

[1]mmelbin@rocketmail.com

[2]sushisusan64@gmail.com

Abstract *- Today encryption of multimedia files are getting tedious task. Most of the security algorithms have its own demerits. So a kind implementation is essential. Data encryption is a vital application term to enable security in open networks like internet and data sharing fields. Image and document files are widely used for various purposes and they are the most popular formats of data on the web. Different image encryption algorithms are proposed so far to generate encrypted image so that it is so difficult to find about the image and their pixel values and ratios. Mostly attackers find their own form to get into these algorithms. This paper proposes a new framework for image encryption, a layer based method for efficient image encryption using a newer and most efficient algorithm. 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. Here we discuss a layer based transformation algorithm in which image is divided into number of equal divisions. Then these blocks are being led to encryption process. At the receiver side after decryption, these blocks are re- transformed and joined into their original form. The main advantage of this method is that it reproduces the original image with no loss of pixel value during the encryption and decryption process in a feasible amount of time, and due to the efficiency, it becomes more secure and reliable over the network.*

Keywords- KIST**,** Segmentation, localization, permutation, encryption.

I. INTRODUCTION

Nowadays multimedia is one of the popular formats in data storage and transmission sessions. Due to the vital role of multimedia data in digital world, the security of multimedia data is becoming more important these days. Every day huge amount of multimedia data is transmitted through the World Wide Web which poses some real security issues, such as unauthorized access and intruder access. Data encryption comes to this field to overcome all these issues and improve the security level of data sharing field. Each kind of data has its own features and terms. Different representations of information like text, audio, video and images in any formats can be individually considered for encryption using suitable techniques basis on their specific features. Text encryption has longer story than any image encryption and there already exist several traditional methods for text encryption such as DES, AES, RSA and IDEA.

There are different types of image encryption algorithms to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types and conditions. Such that some encryption schemes have embedded facilities to encryption such as compression; region based selective, selective encryption, passive encryption and so on. In this paper, a systemized encryption system based on some layers is proposed to enhance the encryption proficiency. It was fully concern to consider all concerns about cryptography.

Different regions of image carry different importance, for instance edge area in image has more important information in comparison with smooth and normal area in that same image. Providing similar security level to data with varied significance implies more computational cost and effort. In this paper region based selective is exploited to provide different security level and protection for blocks of varied significance in image. Region based selective image encryption has lots of usages in time-critical applications and in world wide web wherein security is also a concern such as, internet banking transactions, resource fetching, military image database and communication and medical imaging systems. The image is decomposed into fixed predefined blocks, and then they will be classified as significant or in-significant using edge detection method and make it for a shuffle. Each of these two block groups are treated separately in every encryption phase.

In this paper, we implement a new image encryption algorithm called KIST (key insertion and splay tree encryption) which is basically used for searching. Some of the characteristics and advantages of KIST are as follows.

- An asynchronous key of sequence is used, which depends on the initial key and plaintext encrypted.

ISSN 2348 – 7968

- A splay tree is used such that the substitution is dynamic.
- The encryption is fast and uses less space.
- Cipher texts are compressed in every case.
- The block size of the plain text and key size are flexible and legible.
- It is good for massage integrity.

Splay trees were first described by Sleator and Tarjan in 1983 and the details were presented in end of 1985. Splay trees were originally intended as self-balancing binary search trees with the property that recently accessed nodes are very quick to access again. This property was applied to data compression by Jones loters. The di fference between a ordinary 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. An algorithm called semi-rotations was introduced and used in for data compression to eliminate the need of treating the zigzag cases and thus to simplify the algorithms, proved that on an n-node splay tree, the amortized cost of an access at distance d from the preceding accessible node is O(log(d + 1)). In addition, there is an O(n) initial cost. The accesses include searches, modification, insertions, and deletions. Using splay trees, the more frequent used bytes will be encoded into shorter codes. So the cipher text definitely will give some information to the attacker. However, the method using splay tree for encryption has some attractive characteristics. It is e fficient 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.

II.PRESENT WORK

In this section a novel layer based image encryption method is defined. Concerns and various facilities that the authors have treated are mentioned below:

- Exploit previous author's experiences to achieve lower correlation and higher entropy in new system
- Embed region selective encryption
- Embed block independent encryption
- introduce a new permutation algorithm called PP algorithm and define BBE measure
- Provide different security level and protection according to the block significance
- Achieve to both less processing time and more secure encryption coordination.

The proposed layer based image encryption can be decomposed into four layers (fig .1).

- Segmentation
- localization
- permutation
- Encryption .

Each of the layers is separately described in the rest.

Fig.1 layers based image encryption

A. Segmentation

This section deals with dividing the entire image into Nb number of non-overlapping blocks with variable size. Each block (region) is represented by a square matrix containing a particular number of pixels for each block size. This representative matrix form is used for performing the operations on every regions, each sectional part is considered separately individually for encryption (fig.2). Different block sizes are taken for region segmentation, block sizes defines as $B_S = 2q$, where corresponding block is contains of 2q×2q pixels where 1<q<6. Here four various sizes are considered for blocks of picture including 4×4, 8×8, 16×16, and 32×32. Input images are already defined as a 512×512 dimensions and all four block sizes contribute same (128×128 of 512×512) to decomposition of input image. So, system will have four set of blocks, comprise of 32 blocks of 4×4, 16 blocks of 8×8, 8 blocks of 16×16, and 4 blocks of 32×32. The work use random number of blocks while here, system will have fixed number of blocks for each image so that one of the four different sizes assigned to each block. Just as variable block size is more secure than fixed block size, having some large blocks reduce the encryption time.

ISSN 2348 – 7968

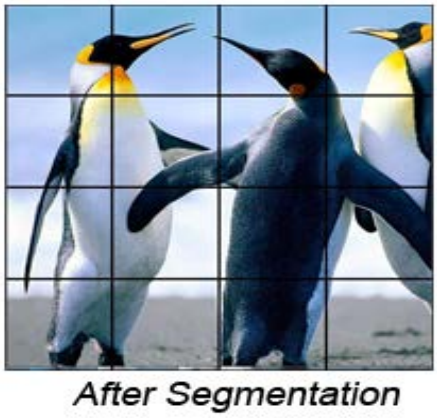
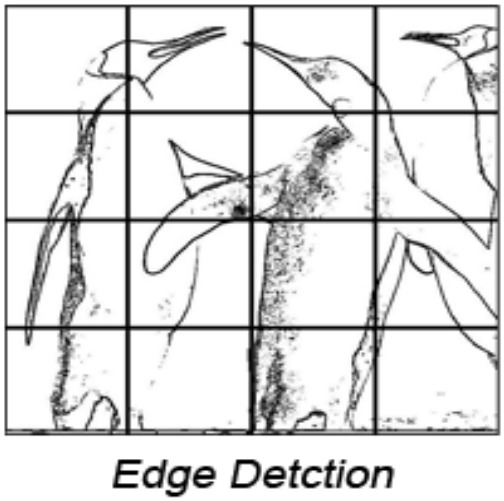


Fig.2 segmentation

B. LOCALIZATION

Image file has distinct regions which belong to different level of importance.. Encryption makes it possible to encrypt on all regions of the image. Featuring same security level to whole of image info which has varied relevance consumes more computational methods and appears unnecessary. Initially of all we ought to search the graphic to extract the features and identify important locations of image (fig. 3), the task just let user to mark some region important, while do the job do this automatically applying prewitt edge detector. In this paper, two techniques considered for identification of significant regions, First that can be done immediately by system, and second, manually by user.



An efficient encryption approach should be able to perturb edges condition and location to stand organization against various attacks. All of us choose Prewitt edge recognition technique as in, intended for three reasons, first that is accurate, second it includes easily implemented, and third it imposes low computational costs (fig. 4).

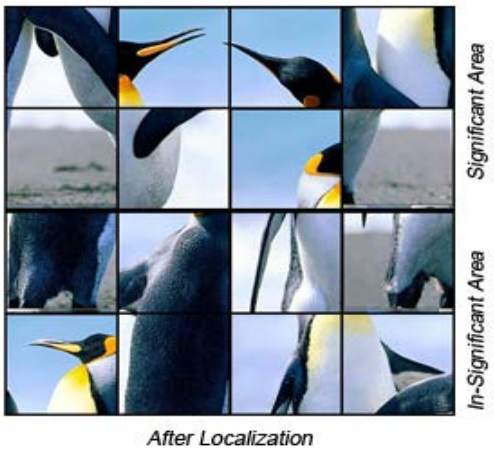


Fig.4 localization

C. PERMUTATION

Edge based permutation deals with interweaving the blocks of the image to generate a newly transformed image. The perceivable information associated with an image can be highly depended on the correlation among the picture elements in an offered arrangement. Decreasing the relation among the image factors using certain permutation approach can makes it extremely difficult to understand. Furthermore, the process of dividing and shuffling the positions of image blocks will produce difficult to predict the cost of any given pixel coming from the values of the neighbours in other palm, it confuses the alliance between the original image and the generated one. Random permutation algorithms are taken by including, RC Permutation, Permutation, Random Sequence, and Chaotic Reordering. The job have pointed out that all permutation-only image encryption are vulnerable to attacks. As a conclusion, they suggested that permutations have to be combined with other encryption techniques to design strongly secured images. Here a new simple and efficient algorithm is created by the developers to permutation of image blocks. We termed it as perspicacious permutation (PP) here, because this simple algorithm has a strategy exactly knowing where the current block should replace in. This algorithm calculates a measure value for each block. The PP algorithm efficiently permutes blocks with the help of Block Background Estimation (BBE) readings. BBE finds the average of pixel intensity ratios for every pixels of the block. This algorithm simply acts in such way that minimizes the bonding permuted image/picture.

ISSN 2348 – 7968

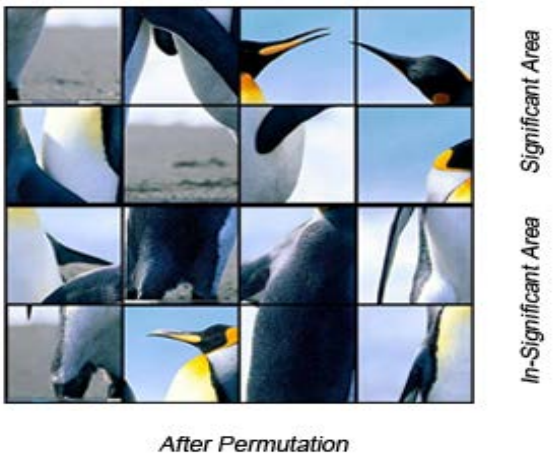


Fig.5 permutation

D. ENCRYPTION

As stated the second layer (localization), blocks are divided into insignificant and significant category positions. Binary significant vector of size 1× Nb is generated, in order that factor '0' indicate the corresponding block is |unimportant t, and '1' indicate the corresponding block is significant. Two procedures are created to treat with blocks according to whether it is labeled| as insignificant or significant. Each insignificant block which is included less essential information will encrypt using rescanning; a less complex methodology. Each significant block which has high possibility to include critical information will encrypt using one particular algorithm in golden set.

This method consists of three sub divisions which can be described as three algorithms:

1. Key generation algorithm.

2. Encryption algorithm.

3. Key injection algorithm.

A) KEY GENERATION ALGORITHM

The key generation algorithm is as follows.

KEY GENERATION(P,K)

comment: P is plain text and K is initial key

for $i = 1$ to 16
  do $key(i) \leftarrow K_i$
$c \leftarrow 17$
for $j = 1$ to m
  do $\begin{cases} key(c) = key(c) \oplus up[p_j + 255] \\ \text{output } (key(c)) \\ c \leftarrow c + 1 \end{cases}$

The *i*th key is generated from initial key and P_j, where P_j contains first *j* bytes of plain text.

B) ENCODE ALGORITHM

The encode is proceeded byte by byte. Since encoding is done by following a path from a leaf to the root of the tree, the code bits are produced in the reverse order from the order in which they should be transmitted. Therefore a local stack is used to temporarily store the bits. The algorithm of encode function encode(byte i) is as follows.

ENCODE(*i*)

comment: i is a byte from input

$j \leftarrow i$
$i \leftarrow i + 255$
while $(i \neq 0)$
$\begin{cases} \text{if } (i = left[up[i]]) \\ \quad \text{then push bit 0 to stack} \\ \quad \text{else push bit 1 to stack} \\ i \leftarrow up[i] \end{cases}$
while (stack is not empty) pop a bit and output it
$Splay(j)$

C) ENCRYPTION ALGORITHM

Now we give our encryption algorithm which is essentially the splay tree algorithm of plus key injection algorithm. First we need to define splay function. The algorithm of Splay function Splay(byte i) is as follows.

ISSN 2348 – 7968

ENCRYPTION(P,K)

```
comment: P is plain text and K is key sequence
for i = 1 to 16
  do injection(K_i, N)
key ← 17
for j = 1 to m
  do { encode(p_j)
     { injection(K_key, N)
     { key ← key + 1
```

D) KEY INJECTION ALGORITHM

The key injection defines to use a key to move inner nodes each other. On the other palm, we also need to compressthe cipher text a little bit. After doing some searches, we found that the random injection may cause the algorithm losing the compression property completely. Actually, in many cases of our test, the cipher text is larger than the plain text. To avoid this problem, we only move the inner nodes which are above to the layer n, where n are some parameter that we predefined. Since more frequent generated bytes are usually at higher layers in encryption, this method will keep some compression of the cipher text.

In this method, it exchanges the links of two separate nodes. So the injection is more efficient and responsive than splay.

INJECTION(i,N)

```
comment: i is a byte from input
j ← i
if (i = 0)
  then quit
s ← 1
N ← n
while (up[j] ≠ 0)
j ← up[j], s ← s + 1
if (s < N)
  then { if (j = right[0])
       {   then t ← left[0]
       {   else t ← right[0]
       { exchange links of i and t (swap up[i] and up
  else quit
```

III.CONCLUSION

This paper proposed a new framework for image encryption, a layer based method . This layer based method is comprised of four layers, segmentation, localization, permutation, and encryption. Author's innovations are applied in all the layers. In localization all blocks briefly are processed and identified as significant and in significant. In permutation layer which PP algorithm is designed to shuffle blocks using BBE measure. In encryption layer various security levels is provided according to importance of the block using combination strategy. It is tried to take all encryption concerns into consider. The proposed method provides different security level to blocks of varied significance in image to 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.

REFERENCE

[1] S. F. El-Zoghdy, Y. A. Nada and A. A. Abdo "How Good Is The DES Algorithm In Image Ciphering?", International Journal of Advanced Networking and Applications, vol. 1, Issue 7, **(2011)**.

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

[3] 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.

[4] M. A. El-Wahed, S. Mesbah and A. Shoukry, "Efficiency and Security of Some Image Encryption Algorithms", World Congress on Engineering 2008, vol. 1, WCE 2008, London, UK, **(2008)** July.

[5] 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.

[6] 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.

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

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