Secure Image Data by Double encryption

Jayant Kushwaha
Department of Computer Science and Engineering,
Maulana Azad National Institute of
Technology (MANIT), Bhopal, India

Bhola Nath Roy
Department of Computer Science and Engineering
Maulana Azad National Institute of
Technology (MANIT), Bhopal, India

ABSTRACT
Security is the main concern in today's world and securing data from unauthorized access is very important. Different techniques should be used to protect confidential image data from unauthorized access as each type of data has its own features. In the natural images the values of the neighboring pixels are strongly correlated. Correlation means that the value of any given pixel can be reasonably predicted from the values of its neighbors. The proposed technique "secure image data by double encryption" provides image data security using cryptographic technique. The proposed method breaks the correlation among neighboring pixel by dividing original image into blocks of size of n pixels*n pixels (n is provided by user) and then encrypt each pixel by their position (x, y) and then encrypt each block by AES Encryption algorithm by using public key of the receiver. The result shows that the correlation between image pixels is decreased and higher entropy is achieved by using this technique.

Keywords
Cryptography, public key encryption, Image Correlation, Image encryption, Image entropy.

1. INTRODUCTION
Government, military, financial institution, hospitals. And private business amass great deal of confidential images about their patient (in Hospitals) , geographical areas(in research) , enemy positions (in defence), product , financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer, if these confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands, than such a breach of security could lead to lost of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is word wide accepted fact that securing file data is very important, in today's computing environment [3].

There are n numbers of approaches available to persuade image file data security, but due to large data size and real time Constrains, algorithms that are good for textual data may not be suitable for multimedia data. There are various approaches available to ensure file data security, such as encryption tool like "aescrypt" for text[3] and other chaos based encryption application for image, but each one has its own disadvantage, rendering them being less frequently used [1, 2].
In this paper we are introducing a new algorithm of image data security, Secure Image Data by the encryption of image data double, first encrypt is of pixel by their position (x, y) and second encryption is of each block. There is a world of difference between digital images data and texts data in many aspects and thus required different encryption technique. In the natural images, the values of the two neighbor pixels are strongly related to each other. I.e. if we have the value of any one of the pixel than we can easily predict the value of other one pixel (called correlation among pixels). With the aim to reduce this high correlation between pixels and to increase the entropy value, we are proposing a Secure Image Data by using a combination of double encryption process based on the combination of the encryption by pixel position (x, y) and another encryption for the blocks. We are using public key cryptography which is a world wide known encryption algorithm. The transformation process that we are using is used to divide the original image into a number of blocks that are then encrypted by their pixel position with one other within the image. The resultant image is then become the input to the public key encryption algorithm. By tacking the correlation and entropy as a parameter of security, the encryption process by their pixel position will be expected to result in a lower correlation and a higher entropy value when compared to using the An Image encryption approach using a combination of permutation Technique followed by encryption and thus improving the security level of the encrypted images. We are using the concept of public key encryption, for the encryption and decryption of image. In this public key's of sender and receiver is known to both but private key's are kept secret [2].

2. RELATED WORK

2.1A Technique for Image Encryption Using Digital Signature
Alok Sinha and Kehar Singh [4] have presented a new ttechnique to encrypt an image for secure image transmission. The digital signature of the original image is added to the Encoded version of the original image. Image encoding is Done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver End, after the decryption of the image, the digital signature can be used to verify the authenticity of the image. In the first step of encryption technique, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image.

2.2 Lossless Image Compression and Encryption Using SCAN
S.S. Maniccam and N.G. Bourbakis [5] 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 a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The drawback of the methodology is that compression-encryption takes longer time.

2.3 A New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture

Jiun-In Guo and Jui-Cheng Yen [6] have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step-1 determines a 1-D chaotic system and its initial point $x(0)$ and sets $k = 0$. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system. Steps-4, 5, 6, and 7 rearrange image pixels using swap function according to the binary
Sequence. But this algorithm does not have any compression scheme and authenticity verification.

2.4 A New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo [7] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point $x(0)$, row size M and column size N of the
Image f, iteration number no, and constants α, β, and μ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels. But this algorithm does not have any compression scheme and authenticity verification.

2.5 Double image encryption by using iterative Random binary encoding in gyrator domains

Muhammad Ashfaq Ahmad3 and Shutian Liu have a double image encryption by using random binary encoding and gyrator transform. Two secret images are first regarded as the real part and imaginary part of complex function. Chaotic map is used for obtaining random binary matrix. The real part and imaginary part of complex function are exchanged under the control of random binary data. An iterative structure composed of the random binary encoding method is designed and employed for enhancing the security of encryption algorithm. The parameters in chaotic map and gyrator transform serve as the keys of this encryption scheme. But the encryption method is safer in the comparison with double random phase encoding.
But these approaches are generally cumbersome and inconvenient to the user and system. Therefore, there is a need for mechanism/system which can ensure reliable and efficient data security in a convenient way. We focused on these issue and proposing secure image data by using a combination of permutation and encryption technique that solve the image data security problem.

2.6 Image Encryption Using Block-Based Transformation Algorithm

Mohammad Ali Bani Younes and Aman Jantan an Image Encryption Approach presented in February 2008 combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks of variable size, 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[1].

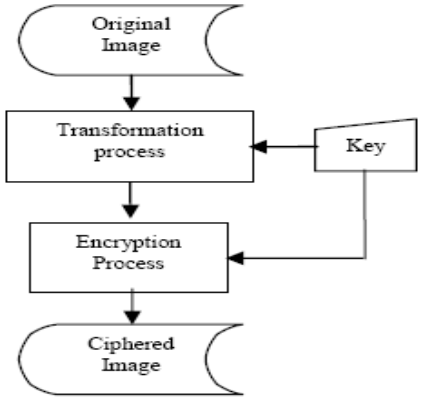

Fig. 1. General block diagram of the transformation algorithm

But this method has few drawbacks. Like first one , they did not mention the decryption process , second one is , if we are using permutation on block of image than , while sending image to an authorized receiver ,we have to send permutation key too , which is a deep security concern.

2.7 An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption

Mohammad Ali Bani Younes and Aman Jantan an Image Encryption Approach presented in aprail 2008 is the combination of permutation technique followed by encryption. They introduced a new permutation Technique based on the combination of image permutation and a Well known encryption algorithm called RijnDael. The original Image was divided into size of 4 pixels × 4 pixels blocks, which were Rearranged into a permuted image using a permutation process Presented here, and then the generated image was encrypted Using the RijnDael algorithm. The results showed that the Correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved[2].

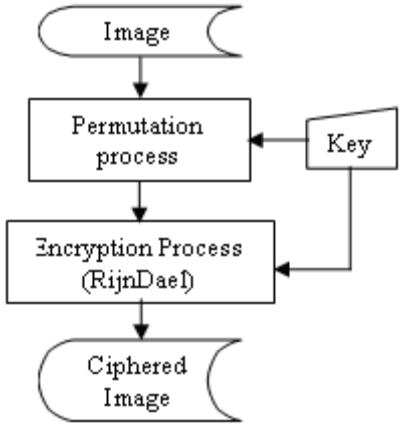

Fig. 2 General block diagram of the permutation technique

But this method has few drawbacks. Like first one , they did not mention the decryption process , second one is , if we are using permutation on block of image than , while sending image to an authorized receiver ,we have to send permutation key too , which is a deep security concern.

3. PROPOSED SECURE IMAGE DATA BY DOUBLE ENCRYPTION

3.1 Design Goals

We have designed proposed secure image data by using a combination of permutation and encryption technique, the aim that image data security should be provided as the top priority of the system. The encryption and decryption of image file data are performed in such a way that making it convenient for the users. The proposed secure image system is designed with the following objective:

- Security: confidentiality of data is ensured by use of strong encryption. Image is divided into blocks than permuted and at last gets encrypted then saved to the disk or send onto the network
- Strong Access Control: we are using Public-Key Cryptographic Technique, to control the access of the file. This approach enhances the security of file by avoiding unwarranted access.
- Transparent Performance: Encrypted file should behave no different from some other files.
- Convenience: the system should be convenient to users.

3.2 Design of proposed Secure image System

The proposed secure image system is free from the type of the image type (i.e. jpg, imp, etc.) designed to provide the above mentioned goals. The secure image system works as follows:
Very first step of this algorithm is, every user who is the part of system has to generate a pair of public – private key, through any key generating algorithm (RSA – key generating algorithm). After this sender and receiver have to do following steps :-

3.2.1) At the sender side

- Convert given image into blocks of nxn
- Encrypt each pixel using their position (i, j).
- Encrypt each block using the public key.
- Calculate the entropy and correlation for analysis purpose.
- Transfer the Image

ALGORITHM ENCRYPT_ IMAGE

Image (image, n, pub_rec, **)**
1: Load the plain Image
3: calculate the Width and Height of the image
3.1: Lower Horizontal Number of Blocks = Integer (Image Width / n)
3.2: Lower Vertical Number of Blocks = Integer (Image Height /n)
4: Number of Blocks = Horizontal Number of Blocks × Vertical Number of Blocks
5: For N = 0 to Number of Blocks -1
5.1: for I=0 to n-1
5.2: for j=0 to n-1
5.3: Encrypt each pixel using their position (I, j),
END PERFORM_ENCRYPTION BY THEIR PIXEL POSITION
SRAT PERFORM_ENCRYTPION BY BLOCK
Input: Image blocks, Receiver public key
6: For N = 0 to Number of Blocks – 1
6.1: Encrypt each block with the public key of receiver,
7: Calculate correlation and entropy
Output: Encrypted image with decrease correlation and increase entropy.

3.2.2 At the Receiver side

- Divide the received Image in nxn blocks. Value of n to be provided by sender.
- Decrypt each block using his private key.
- Decrypt each pixel using its position (i, j).
- Image is decrypted.
- Use image according to the use.

ALGORITHM DECRYPT_ IMAGE

Image (image, n, pub_rec,)
1: Load the plain Image
2: calculate the Width and Height of the image
3.1: Lower Horizontal Number of Blocks = Integer (Image Width / n)
3.2: Lower Vertical Number of Blocks = Integer (Image Height /n)
4: Number of Blocks = Horizontal Number of Blocks × Vertical Number of Blocks

5: For N = 0 to Number of Blocks -1
5.1 Decrypt each block with the private key of receiver,

END PERFORM_ENCRYPTION BY THEIR PIXEL POSITION
STRAT PERFORM_ENCRYTPION BY BLOCK NUMBER

Input: Image blocks, Receiver private key
6: For N = 0 to Number of Blocks – 1
6.1: for I=0 to n-1
6.2: for j=0 to n-1
6.3 decrypt each pixel using their position (I, j),
Output: Encrypted image with decrease correlation and increase entropy.

Above encryption method, which result decrease in the correlation and increase in the entropy, produces three types of output image, (a) Block divide image which is the output of the third and fourth steps of the encryption process, (b) encrypted image which is the output of the fifth step of the encryption process, (c) final ciphered image which is the output of the sixth step of the encryption process, formula for the calculation of the correlation and entropy is as follows:-

3.2.3 Equation for correlation and entropy

Correlation defines as:-

$$r=\frac{n\sum(xy)-\sum x\sum y}{\sqrt{\left[n\sum(x^2)-(\sum x)^2\right]\left[n\sum(y^2)-(\sum y)^2\right]}}$$

Where
r: correlation value
n: the number of pairs of data
Σxy: sum of the products of paired data
Σx: sum of *x* data
Σy: sum of *y* data
Σx^2: sum of squared *x* data
Σy^2: sum of squared *y* data

Entropy defined as follows [18], [19]:-

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k))$$

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

4. ARCHITECTURE OF SECURE IMAGE DATA BY DOUBLE ENCRYPTION

Figure 3 shows the architecture of proposed secure image system in detail. Architecture mainly has four components:-

- Key Management Unit (KMU)
- Block Divider (BD)
- Crypt Engine (CE)
- File Header Extractor (FHE)

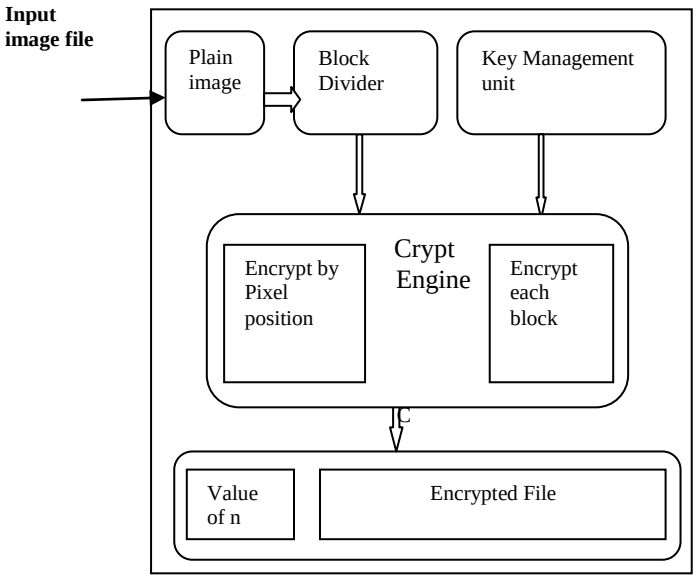

Figure 3 Encryption architecture

4.1 Key Management Unit (KMU)

Key management unit is a very crucial task and is responsible for generation and management of key pair, it generate the key pair (private, public). Key management unit provide one of this key to crypt engine (public key to sender and private key to receiver) for the encryption and decryption of the image at the sender and receiver side.

4.2 Block divider (BD)

Block divider is very important part of the secure image file by double encryption of image, it divide the image into block of size n. Block size n is supply by the user through keyboard or other input device. Divide an image into block of size n is the basic part of the system.

4.3 Crypt Engine (CE)

Crypt engine is the hard part of the secure image data by double encryption of the image. Crypt engine receive the public or private key (public for the sender side and private for the receiver side) from the KMU. With the help of thee key pair crypt engine encrypt the image data by pixel position (x, y) and by block in order at sender side and decrypt the image data by block and by pixel position (x, y) in order at the receiver side. Encrypt or decrypt by pixel position and encrypt or decrypt each block are the eternal part of the Crypt Engine which are use to encrypt or decrypt image by pixel position (x, y) and encrypt or decrypt image each block.

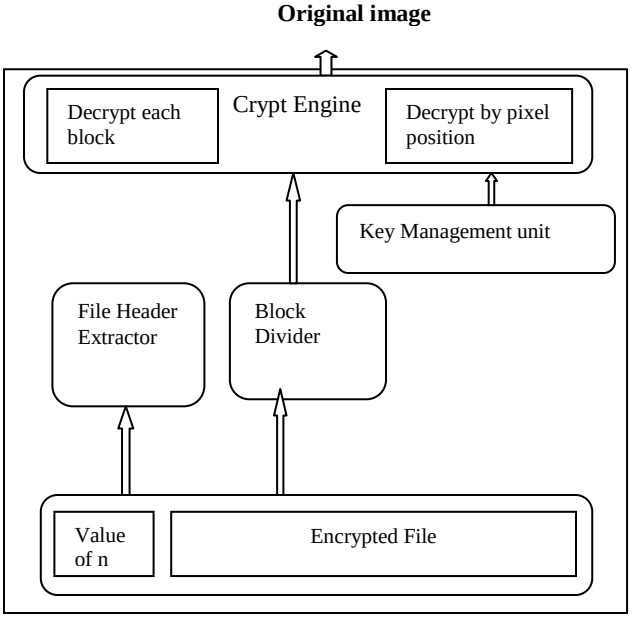

Fig. 4 Decryption architecture

4.4 File Header Extractor (FHE)

FHE comes into play when image is being decrypted at the receiver side. FHE extract the value of n, which is used to divide the image into blocks of size n.

4.5 Operation of the secure image data by double encryption of the image

In this section we will cover the sequence of events which take place while file is being encrypted and decrypted.

4.5.1 While Encryption

For the encryption sender need to enter the value of n through the key board or other input device this value n is used to divide the image into blocks. As shown in the figure 3, following action will take place while encryption:-

- Key management unit will generate the pair of private – public key.
- Block divider will use the value n and divide the image into blocks of size n.
- Crypt engine will encrypt the each pixel by position (x, y) and each block using RijnDael algorithm.
- This encrypted file and the value of n are transferred on the network to the receiver.

4.5.2While Decryption

For the decryption of the encrypted image, receiver uses the value of n which is attached with the encrypted image:-

- File header Extractor extract the value of n, which is used by the block divider to divide the image into blocks.
- Block divider will divide the image into blocks of size n which is extract by the file header extractor.
- De-crypt engine will decrypt the each block and each pixel by position (x, y) using RijnDael algorithm.

5. CONCLUSION

This paper presents a technique "*Secure Image Data by Double Encryption*" for image encryption and decryption. This will provide a valuable tool for secure image transfer. It is very unsecure to transfer an image without breaking the correlation among adjacent pixels, due to strong correlation among neighbouring pixels; the proposed encryption technique will decrease the correlation and increase the entropy of the image. To make a secure image system, the proposed technique divides an image into blocks of n*n size and then perform double encryption process, this will decrease the correlation among neighbouring pixels and increase the entropy and transform the block into encrypted form.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[2] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, vol 3 no 4, April 2008

[3] Rajesh Kumar Pal and Indranil Sengupta, "Enhancing File Data Security In Linux Operating System by Integrating Secure File System" June 2009.

[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

[6] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encr-yption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China

[7] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm" Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China,*E-mail:* jcyen@mail.lctc.edu.tw

Jayant Kushwaha, research scholar in Dept. Of Computer Science and Engineering, National Institute of Technology, Bhopal, India-462003

Bhola Nath Roy, Asst. Professor of Computer Science and Engineering Dept., National Institute of Technology, Bhopal, India-462003.