Image Encryption using Key Matrix Generation and Lossless Compression

Natasha D'Costa
Assistant Professor,
Padre Conceicao College of Engineering
Verna, Goa INDIA 403 722

Anusha Pai
Assistant Professor,
Padre Conceicao College of Engineering
Verna, Goa, INDIA 403 722

ABSTRACT

Most of the existing encryption algorithms are best suited for textual data and cannot directly be applied on images since image data have special features such as bulk capacity, high redundancy and high correlation among pixels that imposes special requirements on the encryption technique used. Therefore, image security has its own special requirements that lead to different thoughts to protect digital data.In this paper, the proposed system would overcome the problem of security and storage by encrypting and compressing the image.The image would be encrypted using a key matrix and then compressed using the proposed algorithms for encryption and compression on the sender side. Similarly on the receiver side the received image would be decompressed and decrypted using the same key. The proposed encryption algorithm encrypts the pixel values by exoring these values with the key generated by the key generation algorithm and then compresses these encrypted pixel values using a specific encoding scheme. This system can be used in any application where image needs to be sent over an insecure channel.

Keywords

Image Encryption, Compression, Decryption, Decompression, Security Analysis

1. INTRODUCTION

Today, in the Information Age, as the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-TV, ecommerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, electronic commerce and touches on many aspects of our daily lives. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.

Communication security is an application layer technology to guard any transmitted information (starting from speech, image to computer messages) against unwanted disclosure as well as to protect the data from unauthorized modification while in transit. Image Encryption can become an integral part of the image delivery process if encryption is the process of transforming the information to insure its security with the huge growth of computer networks and the latest advances in digital technologies. As a result, different security techniques have been used to provide the required protection. Each type of data has its own characteristics include high correlation among pixels, bulk data capacity and high redundancy. Hence, many different techniques should be used to protect confidential image data from unauthorized access.

Data compression is the process of eliminating or reducing the redundancy in data representation in order to achieve savings in storage and communication costs. However image compression is different from data compression. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in file size allows more images to be stored in a given amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages.

The security level of digital images over network has attracted much attention recently, and many different image encryption methods have been proposed to enhance the security of these images. According to the image encryption scheme try to convert an image to another one that is hard to understand only. On the other side, image decryption retrieves the original image from the encrypted one.

Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain. Nevertheless, these approaches have extremely low security levels due to the lack of security keys or the small key space. Furthermore, the permutation-only based encryption schemes are known to be vulnerable for plaintext attacks.Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations. The security level of this method is much lower because the results of its decomposition process and logic operations are predictable. It is not immune to plaintext attacks.Another approach is to use a key image. A key image is another image with the same size as the original image.This image is used to encrypt the original image by using the logical operators. The disadvantage in this case is the large key image needs to be send from sender to receiver through a network. This is not a secure approach of sending a key and is also time consuming and costly.

Lossless data compression makes use of data compression algorithms that allows the exact original data to be reconstructed from the compressed data. This can be contrasted to lossy data compression, which does not allow the exact original data to be reconstructed from the compressed data. Lossy data compression method is one where compressing data and then decompressing it retrieves data that may well be different from the original, but is "close enough" to be useful in some way. Since image data is large and a lot of bandwidth is utilized while transferring images, image compression is being used and while transferring the data it needs to be secured. Hence in this paper we try to develop a system which would overcome these two problems of security and storage.

2. LITERATURE SURVEY

Lot of research has been carried out by researchers in the area of image encryption and compression. Authors in [1] developed twolossless image encryption algorithms. Here they try to change the values of the image pixels by exoring the values of image pixels with a key-image. The key image is derived from another image having the same size as the original image. Authors in [2] applied both lossless compression and encryption on binary and gray-scale images. Here using scanning path each pixel of the image is accessed only once. The scanning path and the values of pixel read during scanning are specified in an encoded form. The algorithm specified then searches for the best optimal scanning path and compresses the pixel values read and then encrypts it. Authors in [3] discussed an improvement of the Hill cipher algorithm. Since finding the inverse of the matrix in certain cases is not possible the concept of invertible matrix is used so that it is always possible to find the inverse of the matrix. Also the solution to overcome the problem of weak security present in hill cipher has been proposed. Authors in [4]discussed lossless compression of encrypted gray scale images. They found that Markov properties in Slepian-Wolf decoder do not work well for gray scale images hence a new resolution progressive compression scheme has been proposed to overcome this problem. Authors in [5] developed a new image encryption approach using block based transformation algorithm. Here the image is divided into blocks and the blocks are transformed during encryption and then retransformed during decryption. For the encryption and decryption process blowfish algorithm is used. Authors in [6] discussed compressing encrypted data. The traditional way of sending image data is first compressing and then encrypting it. In this paper the order is reversed and is proved that in certain cases this scheme would be better than the original scheme.Author in [7] developed a novel scheme for lossy compression of an encrypted image. The original image is encrypted using a pseudorandom permutation, and the encrypted data are efficiently compressed by discarding fine and rough information. A receiver then iteratively reconstructs the content of the original image by updating the values of coefficients. Authors in [8] explained a novel scheme of scalable coding for encrypted images. Here the original data has been masked with pseudorandom numbers that are derived from a secret key. The encrypted data is downsampled into a subimage and is quantized and Handamard coefficient is used to reduce the data amount. Similarly on the receiver side the quantized coefficients of the data are used to reconstruct the original image. Authors in [9] showed that the quality factoring a JPEG image can be an embedding space, and can be used to embed a message. This can be used as a tool for secret communication. Authors in [10] discussed a shared key encryption algorithm that works in the JPEG domain. Hence the conversion of the images into a spatial domain is not required. The algorithms works directly on the quantized DCT coefficients and the decryption process is lossless preserving the original data.Authors in [11] proposed a design in image security by making use of arithmetic coding and advanced encryption standard. Both these methods are used to compress and encrypt the image.Authors in [12] proposed a method to secure image data by double encryption. First the correlation among the pixels is broken by dividing the image into blocks and encrypting them with the pixel position and the blocks are encrypted using AES encryption algorithm.Authors in [13] introduced a new permutation technique which is used to rearrange the blocks of the image and a new encryption algorithm called Hyper Image Encryption Algorithm has been introduced to encrypt the image.

In all the papers mentioned we can see that different methods are used to encrypt and compress the image. But in most of the cases the storage is a problem and sending over a network utilizing a lot of bandwidth becomes a threat to the system. Hence we make an attempt to combine both encryption and compression and perform compression of the encrypted data so that even if the encoding scheme is known the data would be secure since it is encrypted. This would solve the problem of security and storage.

3. PROPOSED SYSTEM

The proposed system encrypts and compresses the image.The image would be encrypted using a novel encryption algorithm making use of a key matrix and then compressed using the algorithm [2] for compression which has been modified, on the sender side. Similarly, on the receiver side the received image would be decompressed [2] first and then decrypted using a novel decryption algorithm using the key matrix which is generated on the receiver side. The block diagram of the proposed system is shown in Figure 1. It consists of Encryption, Compression Decompression, Decryption and Key Generation modules.

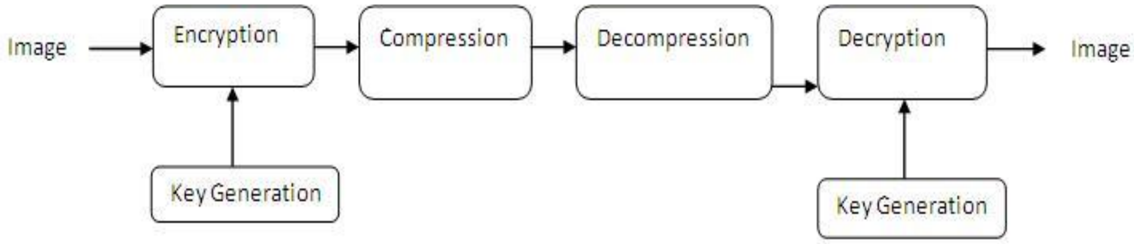


Figure 1.Proposed System

Key generation: In this module, depending on the seed value entered by the user the key generation algorithm would produce a key matrix whose size is equal to a single block size of the image. The key generation algorithm works in this module. Depending on the size of the nxn matrix, the matrix is divided into four parts of n/2xn/2 matrix. Then each block is formed by the formulas specified in the algorithm. Since the block size used is a 64x64 matrix, n=64 and hence the key generation algorithm generates a matrix of this size.

Encryption: In this module the key generated by the key generation algorithm would be used for encryption. The image is first pre-processed and then divided into blocks. Then the key generated is EXORed with each block of the image to get the encrypted image. The encryption algorithm works in this module. After Exoring the key matrix with each block of image we get the encrypted image.

Compression: In this module the pixel values of the encrypted image are read and stored into a file. The data stored in the file are used by the compression algorithm to compress the image.Here the bit sequences are read. The compression algorithm works in this module

Example:Let1111111100000001100000000000000000000101 010101010 be the bit sequence..

The first segment has 11111111 8 bits. From the encoding table 1, the lower limit is 5 and three bits are used to encode the segment preceded by the prefix 10. Therefore the encoded form of it would be 10011. Similarly the next sequence 11 is encoded as 001. Similarly the next bit sequence which is 00000000000000000000 for which the lower limit is 13 and 4 bits are used to encode the segment with the prefix 110. So the encoded form is 1100111. In the last sequence we have consecutive number of 1's and 0's. So we see the total length of the sequence. In this case its 12. So we map it with J. So we get the sequence as J2101010101010.After using the encoding scheme we get a compressed text file having size smaller to the original file.

Decompression: In this module the pixel values of the compressed image are read and stored into a file. The data stored in the file are used by the decompression algorithm to decompress the image. Here the prefix is read and the current bit is stored. Depending on the prefix, the next corresponding bits are read as N. N is then convertedto binary. N is then added to the lower limit of that prefix. Those many current bits give the decoded form. The decompression algorithm works in this module.In case the prefix is an alphabet, it is mapped with its corresponding number, that number is multiplied by 10 and added with the next bit. Those many bits are read from the sequence.The compressed file is read and decompressed using the decoding scheme and the data is stored back in a text file. The data from this file is then converted into image and is used by the decompression algorithm.

Decryption: In this module the key generation algorithm is used to generate the key. Depending on the seed value the key matrix would be exored with the blocks of the encrypted image to get the final decrypted image. The decryption algorithm works in this module. After exoring each block of the encrypted image with the key matrix the final original image is obtained.

4. ALGORITHMS USED FOR IMPLEMENTING THE PROPOSED SYSTEM

4.1 Encryption Algorithm

Here the input is an image which is preprocessed and after the exor operation performed with key, the pixel values of this image are changed. Hence we get an encrypted image which is different from the original image. The steps for performing this process are as follows:

1. Perform the preprocessing steps on the image.

   This preprocessing step involves resizing the image so that the image is of size 512x512 pixels.

2. Divide the image into blocks. Each block contains 64x64 pixels of image.
3. Generate the key matrix of size 64x64 by using the key generation algorithm.
4. Perform the exor operation between the key matrix and each block of image

Result is the encrypted image.

4.2 Key Generation Algorithm

The key matrix is generated [3] using a seed value 's' which is chosen by the user. Since each block size is 64x64, n=64 hence the key matrix is formed using the following steps:
The first element of the matrix which is A11has n/2 x n/2 elements as
a_{11}=s

a_{12}=st

.

.

.

a_{21}=stn/2

.

.

.

$a_{2n/2}$=stn-1

Thus a_{ij}=stm

where m=(i-1) n/2 + j-1, 1<=i<=n/2 and 1<=j<=n/2

Then form A_{22}= - A_{11}

Set $a_{i+n/2,\ j+n/2}$=- a_{ij} for i, j=1 to n/2

Then form A_{12} as A_{12}=k(I- A_{11})

$a_{i,\ j+n/2}$ =k (I- a_{ij}) for i=j=-k a_{ij} for i!=j with i,j =1 to n/2

Form A_{21} as A_{21}=1/k (I + A_{11})

Thus $a_{i+n/2,\ j}$ =1/k (I- a_{ij}) for i=j= a_{ij}/k for i!=j with i,j =1 to n/2

Thus A is formulated.

4.3 Compression Algorithm

The pixel values of the encrypted image are stored in a file. The bit sequences are then read from the file to perform compression.
The encoding[2] is performed as shown in table 1.

Table 1: Scheme of encoding bit sequence

Segment size	Lower limit	Prefix	Bits used to encode segment size	Total bits
2-4	1	0	2	3
5-12	5	10	3	5
13-28	13	110	4	7
29-60	29	1110	5	9
61-316	61	11110	8	13
317-1340	317	111110	10	16

In case there is a long sequence of consecutive 0 and 1 the following mapping is used to encode this sequence
The length of the sequence is divided by 10. Let the quotient obtained be q and remainder be r.
Depending on the value of q the following mapping is used.
q->value

1->J	
2->K	
3->L	
4->M	
5->N	
6->O	
7->P	
8->Q	
9->R	

The mapped value is concatenated with the remainder r and the entire sequence.

4.4 Decompression Algorithm

In this case also the compressed data is stored in the file and the bit sequences are read and the following steps are performed to get the original data. In case the prefix is not an alphabet the following algorithm [2] is used.

```
Inputs: Encoded bit sequence J,First bit F.
Output: Decoded bit sequence
DecodeBitSequence (J, M, F)
{
BitSequence = Empty
CurrentBit=F
For i=1 to M
{
Read prefix P. if P is 0, 10, 110, 1110, 11110, 111110, 11111 then read next
2, 3, 4, 5, 8, 10, 18 bits, respectively.  Let N be the number of bits read.
Convert the binary strings of N bits to decimal value L. Add lower limit of L to
L using table 1.
Append L number of CurrentBit bits to BitSequence
If (CurrentBit is 0)
CurrentBit=1
Else
CurrentBit=0
}
Return BitSequence
}
```

If the first bit read is an alphabet then the reverse of the mapping done in compression is obtained and concatenated with the second bit.

The number of bits read gives the consecutive sequence of 0’s and 1’s .

4.5 Decryption Algorithm

In this case the input is the encrypted image and after the exoring performed with key, we get the original image back. The steps are as follows:

1. Generate the key matrix of size 64x64 by using the key generation algorithm.
2. Divide the image into blocks. Each block contains 64x64 pixels of image.
3. Perform the Exor operation between the key matrix and each block of image
4. Result is the decrypted image.

5. SECURITY ANALYSIS

Security analysis is the process of analyzing how secure a system could be. A system is analyzed against the different cryptographic attacks to check its level of security. The system is analyzed against the following cryptographic attacks:
Brute Force Attack: The Brute force attack is an attack model in which the attacker tries to guess the security keys by conducting an exhaustive search of all the possible combinations of security keys of the encryption algorithms. Theoretically, this approach is feasible if the key space of the encryption algorithm is limited and the attacker knows the encryption algorithm.

The key size is chosen by the sender and receiver. This could be any infinite number. This number is then used to generate the key matrix. The encryption algorithm also has a large avalanche effect so brute force attack is almost impossible.

Ciphertext-only Attack: In cryptography, the plaintext is the original information to be encrypted. The cipher text is the encrypted plaintext. The cipher text-only attack is an attack model in which an attacker tries to deduce the security keys by only studying the cipher text. This attack can be used to recover the original data by studying the encrypted data.

Here the compressed text file is sent on the network. Even if the attacker gets this file and has knowledge of the compression and encryption algorithm the key to be generated is too large. Thismakes it impossible to generate the key due to the large key space as well as the large size of the image.

Even if the attacker tries to get the encrypted image, the encrypted image is visually unrecognizable and totally different from the original image. They contain almost no visual information of the original images.

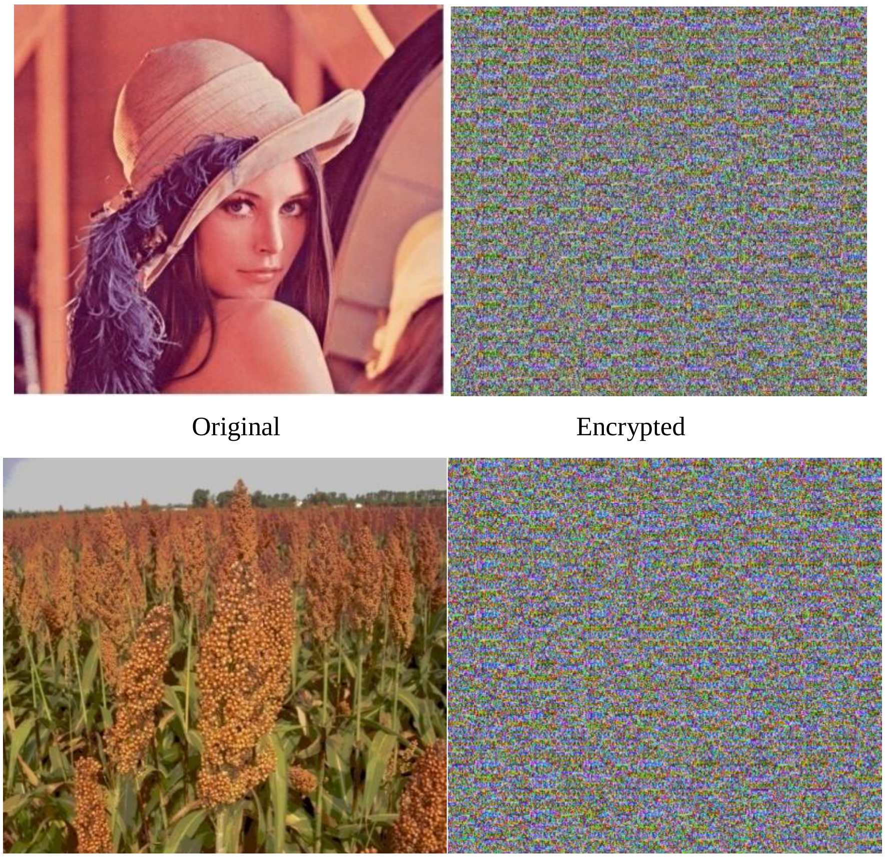
Known-Plaintext Attack: The known-plaintext attack is an attack model in which an attacker tries to obtain the security keys of encryption algorithm by studying a number of plaintexts and the corresponding cipher texts. The condition of this attack is that the attacker should have some plaintexts and the corresponding cipher text.

The EXOR operation in the encryption algorithm is used to change the image data. This data is then compressed in a text file. The text file contains data that cannot be understood until the compression algorithm is known. Even if the compression algorithm is known the image data is protected with the key. Due to the large key space and large size of the image this attack is not possible.

6. RESULTS

The system is implemented in java where two clients establish a connection and the sender selects a seed value from which the key matrix is generated. The key matrix is then used to encrypt the image. After encryption, the pixel values of encrypted image are stored in a file. The data from the file is used by the compression algorithm thus reducing the file size. The seed value selected by the sender is sent to the receiver using Diffie-Hellman key exchange algorithm. The data received by the receiver is first decompressed and the decompressed data is then decrypted using the key matrix generated by the seed value sent by the sender.

Figure 2 shows the images of the original image and the encrypted image. On decryption the same original image is obtained.



Original Encrypted

Original Encrypted

Figure 2: Snapshots of Original and its Encrypted Image

Table 2: Execution time taken by proposed algorithms and comparison with standard implemented algorithm

Image	Encryption-Compression	Decompression-Decryption
Lena	$O(n^2)$	$O(n^2)$
Field	$O(n^2)$	$O(n^2)$
Mandrill	$O(n^2)$	$O(n^2)$

Table 3: Compression ratios of text files

Image size	Uncompressed text file	Compressed text file	Compression ratio
512x512	16,384KB	9060KB	1.8083

Table 2 shows that the encryption and decryption algorithm together have an execution time complexity of $O(n^2)$ similarly the decompression and decryption algorithm has a execution time complexity of $O(n^2)$.

Similarly the compression ratio calculated is 1.8083 as shown in table 3.

7. CONCLUSION

In this paper the concept of both encrypting and compressing the image was accomplished. Here we use both these processes to overcome the problem of security and storage. The encryption algorithm has a good avalanche effect. The compression algorithm is also able to reduce the file size to a considerable amount.Table 2 shows that the time taken to encrypt-compress the image is less than that of an already existing algorithm used [2].The compression is compared with the original and compressed text file. Here the compression ratio comes as 1.8083. The encryption algorithm with the key generation algorithm worked very well for the large image size of 512x512. The key generation algorithm reduces the computation of inverse of the matrix.The future work would include an additional module to encrypt-compress and send more than one image at a time.Improving the image quality of the decrypted image, improving the encoding used in the compression algorithm so that the compressed data can be converted back to the image.

8. REFERENCES

[1] Yicong Z., Panetta K, Agaian S, Senior Member, "Image Encryption Using Binary Key- images" ,Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009

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

[3] Acharya B, Patra S. K., Panda G., "A Novel Cryptosystem Using Matrix Transformation", Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India, Vol. 4, 92

[4] Liu W, Zeng W, Dong L, and Yao Q, "Efficient Compression Of Encrypted Grayscale Images", IEEE Transactions on Image Processing, Vol. 19, No. 4, April 2010

[5] Gautam A, Panwar M, Gupta P. R., "A New Image Encryption Approach Using Block Based Transformation Algorithm", International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 8, Issue No. 1, 090 – 096

[6] Johnson M, Ishwar P, Prabhakaran V, Schonberg D, and Ramchandran K, "On Compressing Encrypted Data", IEEE Transactions On Signal Processing, Vol. 52, No. 10, October 2004

[7] Zhang X, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011

[8] Zhang X, Feng G, Ren Y, and Qian Z. , "Scalable Coding of Encrypted Images", IEEE Transactions On Image Processing, Vol. 21, No.6, June 2012

[9] Guo J M and Le T N, "Secret Communication Using JPEG Double Compression", IEEE Signal Processing Letters, Vol. 17, No. 10, October 2010

[10] Sudharsanan S, "Shared Key Encryption of JPEG Color Images", IEEE Transactions On Consumer Electronics, Vol. 51, No. 4, November 2005

[11] Reddy P V, Sharma K. V, Mallesham P. , Radhadevi P., "Secure Image Transmission Through Unreliable Channels", International Journal on Computer Science and Engineering, Vol. 02, No. 06, 2010, 2053-2058

[12] Kushwaha J, Roy B., "Secure Image Data by Double encryption", International Journal of Computer Applications (0975 – 8887), Volume 5– No.10, August 2010

[13] Rathod H., Sisodia M. S., Sharma S. K., "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)",International Journal of Computer Technology and Electronics Engineering (IJCTEE),Volume 1, Issue 3

[14] Stallings W, Cryptography and Network Security: Principles andPractice, 3rded. Upper Saddle River, NJ: Prentice-Hall, 2003.

[15] Pratt W. K., Burge M. J., Digital Image Processing, 4th edition , A John Wiley & Sons, Inc., Publication.