ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 7, January 2016

Image Compression and Encryption using Vector Quantization(VQ)
Shifting of Contents in the Codebook

R.NishaanthKanna[1],A.Kathiresan[2], S.Abinaya[3]

(1),(2) Department of Computer Engineering , PSG Polytechnic College , Coimbatore,India

(3) Lecturer, Department of Computer Engineering, PSG Polytechnic College, Coimbatore, India

Email-Id:nishaanth1998@gmail.com, kathir22@live.com,abi.dce@psgpolytech.ac.in

Abstract—**The popularity of Internet usage increases exponentially as well as the risk involved in exchanging confidential data between the users. As a result, several algorithms for encryption of data and images have been developed for secured transmission over Internet. In this work, a scheme (Fig.1) for Image compression [1][2] and encryption [3] based on Vector Quantization [4][5] has been proposed that concurrently encodes the images for compression and shifts the contents of the codebook based on a key for encryption. The processing time of the proposed scheme is much less compared to other systems involving both compression and encryption, because it does not use any traditional cryptographic operations, and instead it shifts the contents in the codebook with respect to the key. It may be noted that the security of the proposed system depends on the size and the complexity of the key. Since the generation of truly random sequences are not practically feasible and not consistent in all systems, we use the key entered by the user to convert it into a sequence of numbers using a mathematical function and shift the position of the contents in the codebook which encrypts the image, by entering the same key and generating the same sequence we shift back the position of the contents in codebook which decrypts theimage.**

Keywords— Image Compression; Image Encryption; Vector Quantization

I. INTRODUCTION

The demand for new approaches for reducing the multimedia data which has a rapid growth in their usage, the overall size as well as secured transmission over public channel is also rapidly increasing. This has opened opportunity for extensive research for algorithm based on secured transmission and image compression of multimedia data. Digital image compression [1] and encryption technique [2]willbethesolutiontosolvetheproblemsstatedabove.

While compression technique reduces the size of an image file to be transferred or stored, encryption is widely used to ensure security. The overall processing performance will be slowed due to many computational involvements in these two techniques. Furthermore, one essential point before designing the image cryptosystem is that image must be compressed previous to encryption operation. The reason is that the compression of the encrypted images contributes to low compression ratio (CR) than the compression of unencrypted images as the redundancy of original images is broken on encryption. For this, a suitable and fast cryptography technique has been adopted on compressed image data. The other issue for designing image cryptosystem is that traditional data encryption techniques are not applicable on image data. An image requires more time during encryption/decryption process when a traditional data encryption/decryption techniques are used, because image data is huge in size. Besides, when the traditional data encryption is used on text data, the decrypted text must be identical to the plaintext. However, this requirement is not always necessary for image data. The decrypted image need not be faithful replication of the original image because human visual perception allows the loss of visual intimation to a considerable extent. Because of these differences between image data and text data as well as compressing data speeds-up the encryption/decryption process, in literature several image cryptosystems have been proposed on compressed image. For example, C-C Chang et al. [3] first applied vector quantization to compress the image. After that for enhancing security they diffused and confused the codebook and encrypted these parameters of the codebook by a symmetric cryptosystem like DES [2]. Tung-Shouet. al. [4] proposed scheme is known as virtual image cryptosystem. In their technique, the VQ-based secret image is embedded into the host image to form the stenographic-image. In [5],

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 7, January 2016

Chang et al. proposed scheme can achieve lossless compression using quadtree data structure as well as appreciate secure encoding through secret scanning sequences. In Chuanfeng et al. [6], proposed image cryptosystem is based on k-PCA based compressed image data. Then the compressed image is fed to RC4 algorithm for encryption. Maniccam et. al. [7] proposed scheme is based on different scan patterns, these patterns are used to compress the image in lossless fashion then the compressed image is encrypted by rearranging the bits of the compressed image using a set of scanning paths. In [8], Goh et. al. used DWT and EZW to compress the input secret image. After the compression, RC4 algorithm was applied on the compressed image to ensure confidentiality of image. But this technique does not provide any compression after applying encryption algorithm on compressed image. Among them, Vector Quantization (VQ) based image cryptosystems are attractive especially because it is a block-based quantization method with the benefits including simple architecture, efficient decoding process, and easyimplementation.

In this paper, we have proposed an image cryptosystem based on the VQ scheme. The conventional VQ-scheme compresses the input image to a codebook. Then the codebook is encrypted for secure transmission over public channel. Our proposed method can serve the following objectives: (i) we can achieve both the compression and the encryption of the input image simultaneously; (ii) the proposed method can be easily implemented and highly efficient for the fast encryption and decryption of the compressed image; (iii) the encryption mechanism makes the encrypted data more secure without using popular traditional cryptography technique such as DES, RSA and soon.

The rest of this paper is organized as follows: In section 2 we present a brief overview of VQ based image compression subsequently several approaches for designing of VQ based image cryptosystem. The proposed image cryptosystem is described in section 3. The experimental result and security analysis of the proposed image cryptosystem are presented in section 4 and 5 respectively. Finally, the conclusion is given in section 6.

II. PRELIMINARIES OFVQ

The proposed image cryptosystem, during VQ encoding time, simultaneously performs the compression and encryption of the input image for transmission over insecure communication channel. This section gives some basics of Vector Quantization for image compression. In addition, several existence approaches for designing VQ based image cryptosystem are described with their schematic diagram.

A. VQ Based ImageCompression

The VQ [9-12] is one of the popular lossy image compression techniques and it is based on the basic idea, according to the Shannon's rate-distortion theory, that the better compression is always achievable by coding image vectors not image scalars. It provides two advantages of reducing the required bit-rate for image transmission and requiring simple hardware structure for image decoding at the receiving end. Initially, the VQ encodes original images by decomposing into a set of vectors, and then it uses a suitable codebook to match and represent those vectors in the original images, where the size of each codeword of the codebook can be typically 4×4 pixels. The matching is obtained based on the smallest squared Euclidean distances between the image vectors and the codeword of the codebook; the indices of the matched codeword are then used to replace the image vectors for compression. In case of decoding, each index is used to search the same codebook and the corresponding codeword is placed in the position indicated by the index to get decompressed images. The algorithmic steps of VQ are given.

B. Algorithmic steps of VQCompression

Step 1: Initially, an input image X is divided into non-overlapping *n* blocks of typical size say *4×4* pixels. Then these blocks are converted into vectors of dimension *16* such that $X=\{X_1, X_2, X_3,..., X_{n-1}, X_n\}$, where $X_i$is the i-th training vector.

Step 2: A suitable codebook of m codewords say, $Y = \{Y_1, Y_2, Y_3,..., Y_{m-1}, Y_m\}$ is considered by using LBG [11-12] algorithm, where $n>m$. Then the image vectors formed in step-1 are scanned serially and they are represented with an index i corresponding to the elements Y_i, *for i = 1 to n*, in Y, that closely match with the input image vectors. The matching is done using a distance metric such as Euclidean distance technique.

Step 3: The indices and the selected codewords obtained in step-2 are transmitted separately to the destination, where they are decoded for the construction of original images as shown in *Fig.1*.

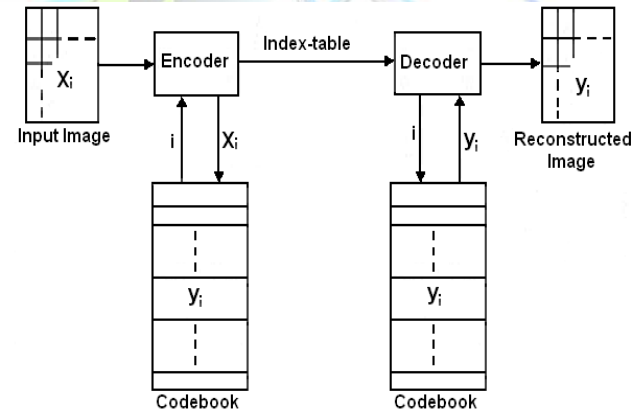

*Fig. 1.*The block diagram of encoding and decoding in VQ[11]

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ernational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
. 3, Special Issue 7, January 2016

C. VQ Based Image CryptosystemDesign

As stated earlier, conventional VQ compresses the input image into the combination of the codebook and the index-matrix. Now the codebook and/or the index-matrix are encrypted to make them confidential. This can be achieved in several ways and among them three major techniques which are adopted by different researcher are described in this section.

Mode 1: The codebook is encrypted before sending to the receiver. The index-matrix is sent as a plain text form. The schematic diagram of such image cryptosystem is shown in *Fig2.*

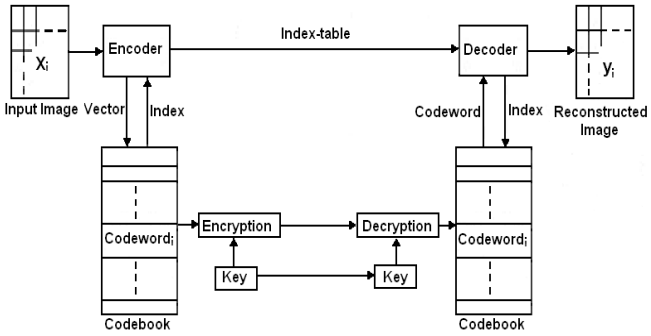

Fig. 2. The schematic diagram for enciphering the codebook in VQ [11]

Mode 2: In this mode the index-matrix is selected for encryption process and the codebook is transmitted through public channel without encryption. The block diagram of such image cryptosystem, where index-matrix is considered for encryption is shown in *Fig. 3.*

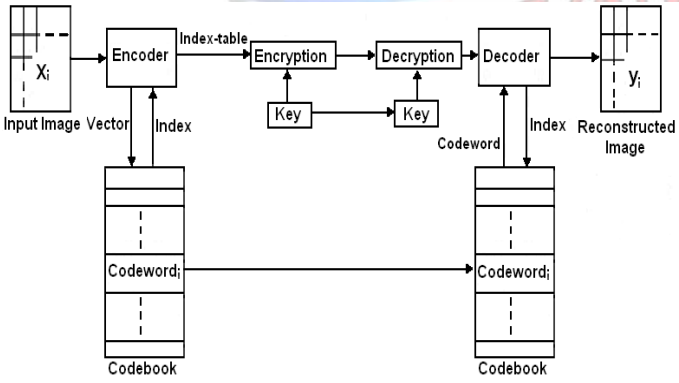

Fig. 3. The schematic diagram for enciphering the index-matrix in VQ [11]

In this paper, the proposed technique basically compresses and encrypts the input image during VQ encoding time. Also the proposed technique, which provides high degree of security, instead of using any conventional cryptography technique and its execution time is fast, is described in the subsequent section in detail. Christo Ananth et al. [14] proposed a work, in this work, a framework of feature distribution scheme is proposed for object matching. In this approach, information is distributed in such a way that each individual node maintains only a small amount of information about the objects seen by the network. Nevertheless, this amount is sufficient to efficiently route queries through the network without any degradation of the matching performance. Digital image processing approaches have been investigated to reconstruct a high resolution image from aliased low resolution images. The accurate registrations between low resolution images are very important to the reconstruction of a high resolution image. The proposed feature distribution scheme results in far lower network traffic load. To achieve the maximum performance as with the full distribution of feature vectors, a set of requirements regarding abstraction, storage space, similarity metric and convergence has been proposed to implement this work in C++ and QT.

III. THE PROPOSEDSCHEME

The process of representing a large— possibly infinite— set of values with a much smaller set is called *quantization* [10]. The detail description of the proposed scheme for image compression and encryption are given in this section. Approaches like shuffling the codevectors using the help of pseudo random numbers [17] is difficult because the generation of pseudo random numbers in an efficient manner is not practically feasible in all platforms so in the proposed approach only the contents of the code book is shifted based on the key given by the user to encrypt the image which makes the approach practically feasible in many platforms. The objective of the proposed technique is that if the codevectors in the codebook are shifted, after VQ compression, based on the key provided by the user before transmitting, then the decryption is not possible without knowing the key used to shift back the codevectors in reverse order. The proposed technique starts with getting an integer key which is then converted into a sequence using a mathematical function. The image is first compressed using Vector Quantization. After compression, the position of the codevectors in the codebook is multiplied with this number to obtain its new position and so on to get a series of numbers then the codevectors are shifted based on the sequence. If this generated codebook is transmitted to the receiver, then the receiver is not able to reconstruct the original image without knowing the key.The Algorithm for the Proposed Scheme is givenbelow:

A. Algorithm for the ProposedScheme

Step 1: The image is compressed using Vector Quantization and the codebook with the codevectors are produced
Step 2: The key is received from the user
Step 3: A sequence is produced based on the number where the sequences have no recurringnumbers.
Step 4: The codevectors are shifted based on the sequence.
Step 5: During final Decryption, the same key is entered and the same sequence is generated and the codevectors are shifted back based on the sequence. The overall process of the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ıternational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
'ol. 3, Special Issue 7, January 2016

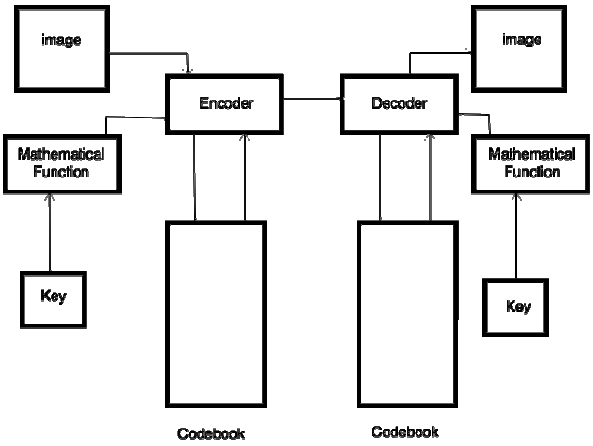

Fig 4. Block diagram of proposed system

B. CODE TO IMPLEMENT PROPOSEDALGORITHM

The Python programming language is used to implement the proposed scheme is an application using Python libraries such as *WxPython* for Graphical User Interface design and *OpenCV* for image compression and parsing the data as individualvalues.

```
while subloop<len(finalImage):
    positionChanger = positionChanger * keyF
    while positionChanger >= len(finalImage):
      positionChanger = positionChanger - len(finalImage)
    if changed.count(positionChanger) == 0:
        changed.append(positionChanger)
        subloop = subloop + 1
        positionChanger = subloop
```

```
while loop < len(finalImage):
    img[loop] = dummy[changed[loop]]
    loop = loop + 1
```

C. SCREENSHOTS

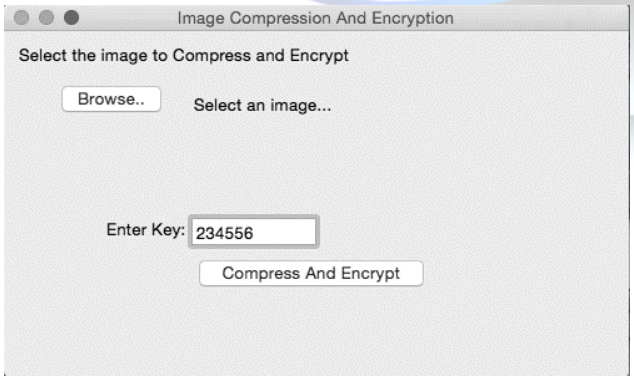

Fig.5.1.The above application is used to compress and encrypt using the key

Fig.5.2.The above application is used to decompress and decrypt using the key

D. EXPERIMENTALRESULTS

To evaluate the performance of the proposed image cryptosystems are described here. Several image codebook generation algorithms [14-16] are available in literature. The result of a 5K image (5120x2880) after encryption is shown in Fig 6.2. The original image is presented in Fig. 6.1.

Fig.6.1 Original5K Image

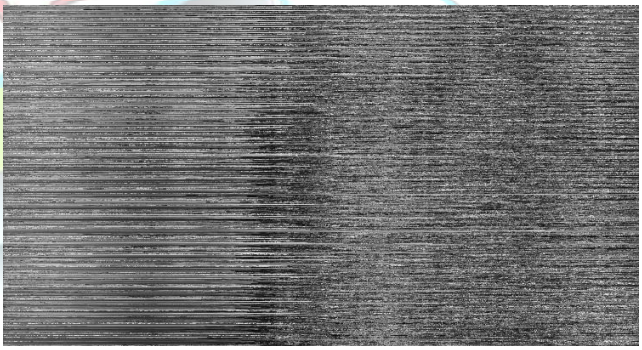

Fig.6.2- Encrypted 5k Image under considering proposed compression and encryption algorithm

E. SECURITYANALYSIS

In our proposed technique compressed image components are not directly encrypted by any existing cryptographic technique like DES, RSA, RC4 and so on. The proposed technique generates shifted codebook as described in section 4 to achieve the confidentiality of the input image. To prove the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 7, January 2016

feasibility of our image cryptosystem if the opponent tries to guess the key by brute force technique. If the key size is 64 bits then it has 2^{64} possible combinations. If the opponent uses a 1000 MIPS (Million Instructions Per Second) computer to guess the key, the computational cost is large enough that no one image can be closed-door after 500 years.

$(2^{64})/(1000*10^{6}*3600*24*365) = 584$ Years

Under a known-plainimage attack, the opponent is assumed to have obtained several plainimage and cipher components pairs. In this case, the cryptanalysts intend to obtain the secret key by analyzing these pairs. After recovering the secret key, the opponent can correctly decrypt the next cipher image component if the original image is encrypted by same key. To stop such type of attack, if we choose key in such a way that the key is changed for every image, then the scheme is wellsecured.

CONCLUSION

An efficient image cryptosystem based on simultaneous VQ compression and shifting of codevectors in the codebook is. It needs the mathematical function to generate the sequence from the key. Although it is considered to be publicly known, the overall secrecy is maintained by keeping the corresponding key as secret to the opponents. The proposed scheme is tested in some several test images and satisfactory results have been found. It is secured also as evident from the security analysis of the proposedscheme.

REFERENCES

[1] David Salomon, " Data Compression: The Complete Reference", *Springer international Edition*, 2005

[2] William Stallings, "Cryptography and Network Security: Principles and Practices", *Pearson Education, Inc.,* Fourth Edition, 2007.

[3] Chin-Chen Chang, Min-Shian Hwang and Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58: pp. 83-91, 2001.

[4] Tung-Shou Chen, Chin-Chen Chang and Min-Shiang Hwang, " A virtual image cryptosystem based on vector quantization", IEEE Transactions on Image Processing, Vol. 7, No 10, October 1998.

[5] Chang H. K. and Liu J. L, " A linear quadtree compression scheme for image encryption", Signal Processing: Image Communication, vol 10, no. 4, pp. 279-290, 1997.

[6] ChuanfengLv and Qiangfu Zhao, "Integration of Data Compression and Cryptography: Another Way to Increase the Information Security", in: 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.

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

[8] Goh H. K., Azman S. and Zurinahni Z., "Enhance Performance of Secure Image using Wavelet Compression", in Proceedings of World Academy of Science, Engineering and Technology, Vol. 1, January 2005.

[9] R. M. Gray, "Vector quantization", IEEE ASSP Magazine, Vol. 1, no. 2, pp. 4-29, April 1984.

[10] KhalidSayood, "Introduction to Data Compression", Morgan Kaufmann Publishers, Second Edition, 2000

[11]A. Greso, R. M. Gray, " Vector Quantization and Signal Compression", Kluwer Academic Publishers, Boston, MA; 1991.

[12]Y.Linde, A. Buzo and R. M. Gray, "An algorithm forvectorquantizer design",IEEETransactionsonCommunications,1980,28:84-95.

[13] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. on Information Theory, IT-22(6):644-654, 1976.

[14] Christo Ananth, R.Nikitha, C.K.Sankavi, H.Mehnaz, N.Rajalakshmi, "High Resolution Image Reconstruction with Smart Camera Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015, pp:1-5

[15]Jim Z.C. Lai, Yi-ChingLiaw and Julie Liu, "A fast VQ codebook generation algorithm using codeword displacement", Pattern Recognition, Vol 41, pp. 315-319, 2008.

[16]H. B. Kekre and Tanuja K. Sarode, "An Efficient Fast Algorithm to Generate Codebook for Vector Quantization", IEEE Trans. On ICETET, 2008.

[17] Arup Kumar Pal, G.P. Biswas and S. Mukhopadhyay "Design of image cryptosystem by simultaneous vq-compression and shuffling of codebook and index matrix "