Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

SECRECY OF NOVEL ENCRYPTION ALGORITHMS FOR THE IMAGE CRYPTOSYSTEMS: A REVIEW ARTICLE

S. Karthikeyan
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: s.karthikeyan@jainuniversity.ac.in

Abstract

Straightforward encryption is an efficient way to keep transmitted messages secret. Taking efficiency into account, partial encryption for pictures, audio and video has recently been generally accepted. However, in cases where a large number of images are purposely transmitted to the same destination, a new and efficient method is required. Chang, Hwang and Chen proposed an encryption algorithm for images based on vector quantization, in which the encryption of a common codebook is suggested to be the better option of their two proposed schemes, since several images can be transmitted with only one corresponding codebook encrypted. However, in the present paper, if the popular codebook is used to encrypt a large number of images, the weakness of the CHC image cryptosystem is established according to the selected-plain image assault. And holding the index sets in a simple form is shown not to be a good idea, based on the cypher image-only attack. A way of protecting the transmitted images is also recommended.

Keywords: *Cryptosystem, Digital Images, Encryption, Medical Images, Data protection, Quantization.*

I. INTRODUCTION

Digital images can be shared more effectively and rapidly due to substantial improvements in networking. In certain applications, such as military photographs, medical images and commercial imaging goods, and other sensitive details that cannot be revealed, the transmission of classified images through an open computer network environment is often used. The topic of digital image protection has therefore become increasingly relevant [1].

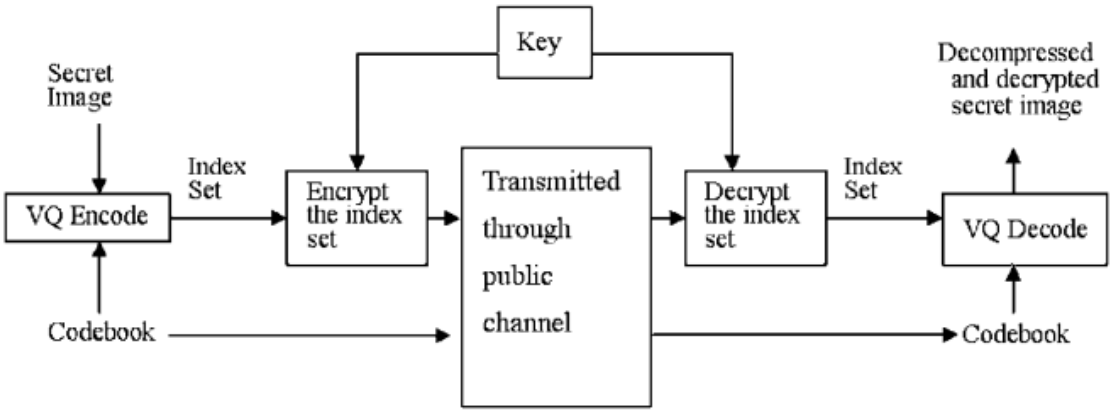

Fig. 1: Illustrates the procedures of encoding index set in CHC picture cryptosystem [2]

For image encryption, there are certain important properties that can be highlighted as critical, particularly overhead bandwidth and computational costs. Photos are typically transmitted in the form of compression nowadays. Therefore, by combining encryption with compression while keeping image communication secret, it is a good strategy to reduce bandwidth and compute load [4].

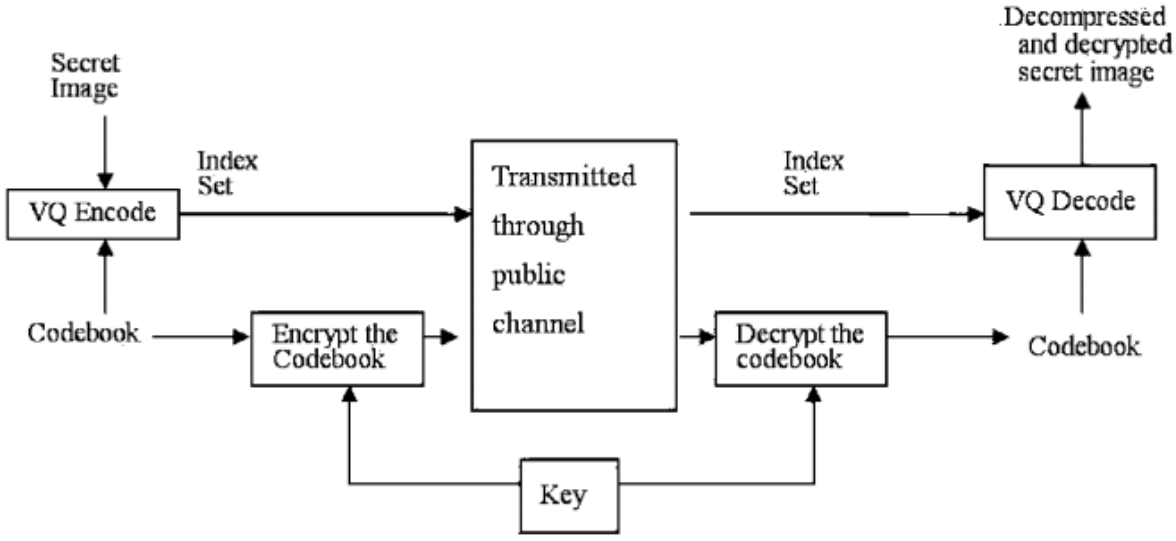

Fig. 2: Illustrates the procedures of decoding index set in CHC picture cryptosystem [3]

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\;(y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)}\; \neq 0, \sqrt{D(y)} \neq 0$$

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below [5].

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations [6]

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

II. LITERATURE REVIEW

A survey was carried out by Justin et al. on different encryption techniques. This paper focuses specifically on the various forms of current encryption techniques, and frames all the techniques

together as a literature survey. Aim for a thorough experimental analysis of implementations of different encryption techniques available. It also focuses on techniques for image encryption, information encryption techniques, double encryption, and encryption techniques based on Chaos. This research relates to the performance parameters used in encryption processes and their security problems are examined [7].

III. DISCUSSION AND CONCLUSION

In the present paper, the cases of the chosen plain image attack and the cipher image attack are discussed to show why it is not good to protect a large number of secret images by encrypting a common codebook and to leave an index set in a clear form, respectively. The ideal would be to encrypt both the codebook and the index set with distinct keys or to change the codebook every certain number of images. In particular, for VQ-based schemes, to encrypt the index set is the minimum requirement for security. In summary, it is not recommended to leave the index set in a simple form, taking into account the capability of HVS and the essence of the VQ technique. Instead, in the VQ-based image encryption methods, scrambling the index collection makes it difficult to figure out the relationship between different image blocks.

IV. REFERENCES

[1] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, 2010, doi: 10.1016/j.sigpro.2010.03.022.

[2] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method," *Multimed. Tools Appl.*, 2017, doi: 10.1007/s11042-016-3383-5.

[3] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," 2014, doi: 10.1109/ICSIP.2014.80.

[4] E. N. Kumar and E. S. Kumar, "A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach," 2013.

[5] S. Kumar, A. Gupta, and A. Arya, *Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio*. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[6] M. Khan and T. Shah, "A Literature Review on Image Encryption Techniques," *Autoimmunity Highlights*. 2014, doi: 10.1007/s13319-014-0029-0.

[7] J. M. Justin, "A Survey on Various Encryption Techniques," *Int. J. Soft Comput. Eng.*, 2012.

ISSN: 0374-8588
Volume 21 Issue 9, September 2019