IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ........
Email: editoriijcs@ipasj.org
Volume 5, Issue 2, February 2017
ISSN 2321-5992

# SECURING IMAGE TRANSMISSION VICTIMISATION IN- COMPRESSION CRYPTOGRAPHY TECHNIQUE

**Mr. Jai dev Kaushwah**

Pune Institute of Computer Technology, Pune

## ABSTRACT

***To enhance the embedding capacity of image steganography and provide an imperceptible stego-image for human vision, a novel adaptive number of least significant bits substitution method with private stego-key based on gray-level ranges are proposed in this paper. The new technique embeds binary bit stream in 24-bits color image (Blue channel) or in 8-bits gray-scale image. The method also verifies that whether the attacker has tried to modify the secret hidden (or stego-image also) information in the steno-image. The technique embeds the hidden information in the spatial domain of the cover image and uses simple (Exert operation based) digital signature using 140-bit key to verify the integrity from the stego-image. Besides, the embedded confidential information can be extracted from steno-images without the assistance of original images. The proposed method can embed 4.20 bits in each pixel of gray-scale image and 4.15 bits in each pixel of color image. The presented method gives better results than the existing methods.***

## 1. INTRODUCTION

With the fast development of multimedia system and network technologies, the protection of multimedia system becomes a lot of and a lot of vital, since multimedia system knowledge area unit transmitted over open networks a lot of and a lot of of times. Typically, reliable security is important to content protection of digital pictures and videos. cryptography schemes for multimedia system knowledge ought to be specifically designed to safeguard multimedia system content and fulfill the protection needs for a selected multimedia system application. for instance, time period cryptography of a complete video stream victimisation classical ciphers needs serious computation attributable to the big amounts of knowledge concerned, however several multimedia system applications need security on a far lower level, this may be achieved victimisation selective cryptography that leaves some sensory activity info when cryptography. As a vital method of coming up with a secure video cryptography schemes, secret Multiple Huffman Tables (MHT) are prompt in some styles. the most important advantage by using this type of joint compression-encryption approach is that top compression ratio and high encryption degree are often achieved in one single step, which simplifies the system design and makes it flexible for some advanced multimedia processing [1] in addition to the reduction of time required to perform compression followed by encryption. After re-studies the security of multimedia encryption scheme based on secret Huffman tables, the present cryptanalysis shows presence of drawbacks in MHT technique. To overcome the drawbacks of MHT technique, a new scheme for more general and efficient secure multimedia transmission, OMHT, is proposed. OMHT depends on using statistical-modelbased compression method to generate different tables from a training set has the same data type as images or videos to be encrypted leading to increase compression efficiency and security of the used tables. Using known fixed tables in MHT technique generated by mutation (a method introduced in [1]) for compressing and encrypting images causes degradation in both compression ratio and security. We focus our research attention to enhancing multiple Huffman tables coding techniques. It is a challenging problem to verify joint consideration of security, bitrate overhead, and friendliness to delegate processing. Performance analysis of the newly proposed scheme OMHT shows that it can provide superior performance over both generic encryption and MHT in the security and compression. This paper is organized as follows: Section 2 shows an overview of multimedia encryption techniques. A new proposed scheme, Optimized Multiple Huffman tables coding technique (OMHT) is described in section 3 with a detailed description for proposed adaptive quantization technique. Section 4 presents a performance analysis of the proposed scheme OMHT technique. The computational cost of the proposed technique is analyzed in section 5. Conclusion is given in section 6.

## 2. OVERVIEW OF MULTIMEDIA ENCRYPTION TECHNIQUES

When dealing with still images, the security is often achieved by using the naïve (traditional) approach to completely encrypt the entire image, traditional encryption, with a standard cipher [2] (DES, AES, IDEA, etc.). As shown in Fig. (1), assuming that the plaintext and the cipher text are denoted by P and C, severally, the encryption procedure in a cipher can be described , wherever Ke is the cryptography key and E(•) is the cryptography perform. Similarly, the decipherment procedure is P =DKd (C), wherever Kd is that the decipherment key and D(•) is that the decipherment perform once, the cipher is termed a private-key cipher or a rhombohedra cipher For private-key ciphers, the encryption-decryption key should be transmitted from the sender to the receiver via a separate secret channel. once Ke ≠ Kd, the cipher is termed a public-key cipher or AN uneven cipher. For public-key ciphers, the cryptography key Ke is printed, and therefore the decipherment key Kd is unbroken non-public, that no further secret channel is required for key transfer. Ciphering the entire compressed file could end in excessive process burden and power consumption at the decoder and maybe even the server/ encoder. However, there area unit range of applications that the naive primarily based cryptography and decipherment represents a significant bottleneck in communication and process. Some recent works explored a replacement method of securing the content, named, partial cryptography or selective cryptography, soft cryptography, sensory activity cryptography, by applying cryptography to a set of a bitstream. the most goal of selective cryptography is to cut back the quantity of knowledge to cypher whereas achieving a needed level of security [3].

According to Fig. 2, there area unit 2 undemanding places to use generic cryptography to multimedia system. the primary chance is to cypher multimedia system samples before any compression, stages one and a pair of, Qiao et al. [4] and Uehara and Safavi-Naini [5] area unit samples of pre-compression selective cryptography. the most downside with this approach is that the cryptography typically considerably changes the applied mathematics characteristics of the initial multimedia system supply, leading to abundant reduced squeezability. Cheng and Li, 2000. The wavelet-based compression formula SPIHT [6] is AN example of post-compression cryptography theme, stage four and five. Wu et al proposed encryption scheme based on encoding with multiple Huffman tables (MHT) used alternately in a secret order [1]; is an example of in-compression selective encryption stages 3, and 4. The encryption with reasonably high level of security and unaffected compression can be achieved simultaneously, requiring almost negligible additional overhead. One of the major advantages by using this kind of joint encryption-compression approach is that encryption and compression can be achieved in one single step, which simplifies the system design an makes it flexible for some advanced multimedia processing such as scalability and rate shaping.

## 3. OPTIMIZED MULTIPLE HUFFMAN TABLES (OMHT)

OMHT compression-encryption technique is a modification to the MHT scheme; it generates different Huffman tables for each type of images instead of using fixed Huffman tables for all images as in MHT technique. The main advantage of using OMHT technique over other lossy compression technique is that it produces a much smaller compressed file than any compression method, while still meeting the advantage of encryption. Remove small, invisible parts, of the picture is based on an accurate understanding of how the human brain and eyes work together to form a complex visual system. As a result of these subtle reductions, a significant reduction in the resultant file size for the image sequences is achievable with little or no adverse effect in their visual quality. As shown in Fig. 3 OMHT process takes two parallel paths A, and B, so it takes no additional time to add encryption to the compressed bitstream as both traditional and selective encryption techniques.

### 3.1. THE PROCEDURE OF COMPRESSING THE

Original Image As shown in Fig. 3 (path A), The input NxM image is first converted into single vector by concatenating successive rows beside each other to form a long row that contains all the image pixels using matrix to vector converter. This vector is exposed to DCT to transform the image from spatial domain into frequency domain in which energy of the image information is concentrated in a few number of coefficients. The output of the DCT process is a vector that has the same length of the image (number of pixels in the image), but with many values approximated to zeros. After applying the DCT the output coefficients are arranged in a descending order according to its energy content. The energy content of the coefficients is summed from the beginning of the vector and toward the end till a specific energy percentage (EP) of the image energy is reached. Those coefficients that carry EP energy percent are chosen to be transmitted and the rest coefficients are neglected since they carry only very small energy that will not affect the visual quality of the recovered image. This EP price depends on image characteristics and it will be varied to bring home the bacon the desired compression quantitative relation and the signal to noise quantitative relation according the application: As we have a tendency to decrease the EP price, a better compression quantitative relation is obtained with slightly lower signal to noise quantitative relation. currently the amount of the transmitted coefficients (Tc) becomes terribly tiny.

The reduced coefficients vector came back to the spatial domain victimisation IDCT to be processed by AN economical quantizer. The planned Least Probable Coefficients Approximation (LPCA) reduces the output values of the IDCT by conniving their prevalence chances. The IDCT coefficients area unit organized in a very downward order consistent with their chances in a very vector. The fascinating division levels area unit taken because the most probable coefficients from the start of the organized vector; if the desired metal and SNR area unit achieved by transmission solely four division levels, those division levels area unit the primary four coefficients within the organized vector. The likelihood of the last QL is termed neglecting likelihood (NP).

## 5. PROCESS ANALYSIS

The analysis of the process speed of ciphers sometimes consists of the analysis of the keysetup value, the cryptography value and therefore the decipherment value [16]. The cryptography and therefore the decipherment prices area unit sometimes similar, and that they area unit a lot of vital than the key-setup value as a result of one single key-setup will typically be followed by thousands of encryption/decryption operations. within the following, we have a tendency to analyze these prices of our OMHT cryptography theme, and compare them with those of MHT and trendy ciphers.

a) Key-Setup cost: The key-setup method includes all the computation and memory allocation operations before actual cryptography of the primary bit within the plaintext. The process value of OMHT key-setup is dominated by the development of optimized multiple Huffman tables, generation of the key order by that those tables area unit used, and scrutiny the check image with datasets. OMHT takes concerning ten operation per table generation, single operation for secret key generation, and L operation for comparison. the overall range of operations equal 10XMXL+1+L, where L, M is range of datasets and range of subsets severally. For L=4, M=20, world wide web Key-Setup value =805 operations. For MHT technique it takes twenty operations per table entry, the overall value would be 20xtxm, wherever t and m area unit the table size and therefore the range of chosen tables, respectively. For the instance of JPEG dc constant cryptography as shown within the previous subdivision, the key-setup value would be around 2000 operations ( t=13 and m=8 ).Compared with the ciphers listed in Table half dozen,the key-setup value of OMHT cryptography is way smaller than MHT and alternative ciphers.

b) Encryption/Decryption value: world wide web process cost of the OMHT is that the same because the basic MHT-encryption theme [1] is a smaller amount than one C.P.U. operation per encrypted bit as explained below. once an emblem is to be encoded with a traditional Huffman computer user, the shift quantity is supplementary to the bottom address of the table to get the address of the specified Huffman code. This method is illustrated in Fig.13 (a). within the basic MHT system, we have a tendency to store the bottom addresses of the tables in a very cyclic queue consistent with the order that they're used. once an emblem is to be encoded/encrypted, the bottom address is initial loaded from the memory, so the shift-amount is supplementary thereto. Afterwards, the index to the cyclic queue of base addresses ought to be inflated by one. Then, the index ought to be compared with the top of the queue so as to make a decision whether or not it ought to be reset to the start of the queue. Therefore, the process distinction between our cipher/encoder and a traditional Huffman computer user is one memory-load, one addition and one comparison operation for every image encoded. The coding method of the planned cipher/encoder is shown in Fig.13 (b). Since each symbol within the original data usually corresponds to quite 3 bits within the Huffman bitstream, then encryption cost of our algorithm is less than one CPU operation per encrypted bit, which is around 20 times smaller than the well-known AES as listed in Table 6.

## REFERANCES

[1]. C.-P. Wu and C.-C. J. K. Kuo. “Design of integrated multimedia compression and encryption systems”. IEEE Transactions in Multimedia, vol. 7, no. 5, pp. 828–839, 2005.

[2]. W. Stallings. "Cryptography and Network Security Principles and Practices", Upper Saddle River, NJ: Prentice Hall, 2003.

[3]. M. Van Droogenbroeck and R. Benedett. “Techniques for a selective encryption of uncompressed and compressed images”. In Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS '02), pp. 90–97, Ghent, Belgium, September 2002.

[4]. L. Qiao, K. Nahrstedt, and M.-C. Tam.“Is MPEG encryption by using random list instead of zigzag order secure?”. in Proceedings of the IEEE International Symposium on Consumer Electronics (ISCE '97), pp. 226–229, Singapore, December 1997.

[5]. T. Uehara and R. Safavi-Naini.“Chosen DCT coefficients attack on MPEG encryption scheme”. in Proceedings of IEEE Pacific Rim Conference on Multimedia, pp. 316–319, Sydney, Australia, December 2000.

[6]. H. Cheng and X. Li. “Partial encryption of compressed images and videos”. IEEE Transactions on Signal Processing, vol. 48, no. 8, pp. 2439–2451, 2000.

[7]. C.-P. Wu and C.-C. Kuo. “Efficient multimedia encryption via entropy codec design”. Proc. SPIE, vol. 4314, Jan. 2001.

[8]. D. Xie and C. J. Kuo. “Enhanced Multiple Huffman Table (MHT) Encryption Scheme Using Key Hoping”. In Proceedings of IEEE International Symposium on Circuits and Systems, pp.568–571, May2004.

[9]. D. Xie and C. J. Kuo. “Multimedia Data Encryption via Random Rotation in Partitioned Bit Stream”. In Proceedings of IEEE International Symposium on Circuits and Systems, pp.568– 571, May2004.

[10]. D. W. Gillman and R. L. Rivest. “On breaking a Huffman code”. IEEE Transactions on scientific theory, vol. 42, no. 3, pp. 972–976, 1996.