Efficient Cryptographic Image Compression by Pixel Reorganizing

Leena Roslin Jenifer.M[#1], G.Sudha[*2]

[#] *PG Scholar, Department of ECE, Sri SaiRam Engineering College,*
Chennai-44,India.
[1]jenifer.leenaroslin@gmail.com
[*]*Assistant Professor, Department of ECE, Sri SaiRam Engineering College,*
Chennai-44,India.
[2]sudha.ece@sairam.edu.in

Abstract— **Wireless multimedia sensor networks (WMSN) have drawn the attention of the research community in the last few years over the field of civil and military applications. For such multimedia sensor nodes, the security requirement is usually low and so, the intruder can modify the appearance of the adequate data. Therefore it is necessary to protect the value of the total weight of the information during transmission. These sensor nodes are resource limited with low storage capacity. Hence both data compression and security are the essential tools for WMSNs. By implementing both the security and compression in a single step enhances the properties of the images in processing algorithm. For that Burrow wheeler compression algorithm is used with SPIHT and key transpose by which the secured and compressed image is obtained. Thus, the output with security and better compression with increased throughput is achieved and the subjective metrics of images can be retrieved by the BWT.**

***Keywords*— Burrow Wheeler compression algorithm, Compression and Encryption, Decompression and Decryption, SPIHT, BWT, Transposition.**

Introduction

This Wireless multimedia sensor networks (WMSN) consist of the image sensor, with a number of potential applications, ranging from security to monitoring. The major task of WMSN is image communication, which is really a challenge for resource constraint wireless sensors. Objective of this paper is to compress the image and adding security into the image which gives a secured and efficient format which saves the storage space and provides an efficient transmission through telecommunication channels. In order to prevent the image from the intruder, security is ensured by key transposition. The main advantage of proposed system is inserting security into the compression technique which ensure the compression encryption is carried out in a single step instead of two step process of compression and encryption. As well as the subjective metrics of the original image can be easily recovered without any distortion. The effective compression is achieved through Set partitioning in hierarchical Trees (SPIHT) compression technique. The SPIHT technique provides less complex algorithm for the sensor nodes. Thus the output after compression and encryption is in the secured and compressed format and so the intruder gain no data from the output during transmission.

I. RELATED WORKS

In the existing system, BWT is used along with the oldest compression method of entropy coding such as arithmetic coding and Huffman coding [1]. For providing security during compression keyed scrambling is used which is similar to AES technique by shifting of rows. However, the attacker or an unauthorized user can easily understand the content [6].For analog image path scanning should be implemented before going into the compression process in order to convert the image into pixel sequence. Hence, the zigzag scanning is prescribed before compression. However, Zigzag is applied only before DCT and there is necessity for DCT coding in after the zigzag scanning method [3].And the Images usually have the high redundancy while introducing security, the perceptual ability is disguised in case of both subjective and objective metrics [7].

II. CURRENT APPROACH

In the proposed method the image results of using the BWCA (Burrow Wheeler Compression Algorithm) with keyed transposition and SPIHT on images are enhanced.

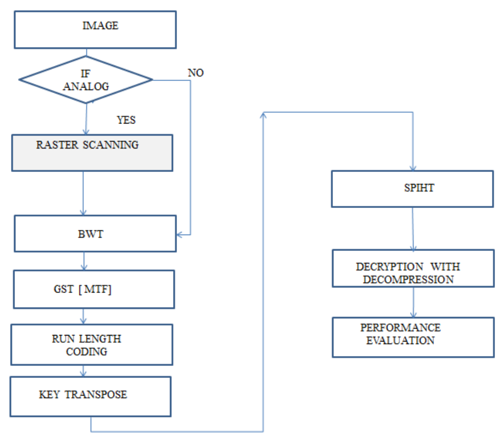

Fig. 1. Modules involved in process

By this way key based compression algorithm is achieved. The unification of compression and security carried out in a single step. This BWCA is consisting of five modules. Fig.1 represents the encryption compression and decompression, decryption in an image. During decompression decryption operation reverse transformation and inverse operation are performed to retrieve the original image.

A. *Burrow Wheeler Transform(BWT)*

It is the method which does not compress data, but modifies the input image and makes the image format which is helpful for further effective compression. The main idea of BWT is block sorting which groups the pixel sequence of repeated values. And it produces the output as lot of clusters with repeated values. The BWT operates by two sorting level. First is the cyclic sorting which cyclically sort the pixel sequence and from the output of cyclic sorting lexicographic sorting is applied on the pixel sequence. After the lexicographic sorting the last column of the matrix is taken as output along with its index. This BWT is bijective, because the original image can be easily recovered from the index values. Hence the bijective compressor which is present in the sink node can be fastly recovering the original sequence. The main reason for implementing BWT is it produces the output which in confusional perception which cannot be identified by the intruder.

B. *Move To Front Transformation(MTF)*

BWT is used along with MTF. Move to Front transformation is also known as Global structure Transformation (GST) or List Update Algorithm (LUA). Because, it ranks the values according to their relative frequency. And moves the most recent read items to the first place. And it is used to improve performance of entropy encoding techniques of compression. Hence the output of MTF produces the pixel values with many number of zero runs.

C. *Zero Run Length Coding(0RLE)*

As the output of MTF consist of many number of zero runs, in order to reduce the number of zero runs in data sequence, zero run length coding is implemented. It is a lossless compression coding technique used to reduce the repeated runs. It is more efficient for sequence of data that are duplicated. It encode the repeated pixel values with two integer pairs such as the value and the number of times it is getting repeated.

D. *Key Transposition*

In order to ensure security in compression conditional transposition is used. The transposition depends on secret key value. The weight of the algorithm is depending upon the strength of the key. The consideration of conditional transposition after run length coding is due to the nature of the entropy coding which is not affected by the position of the value. First of all the pixel sequence is written in row by row and then the permutation takes place. In permutation the pixel values and key values are bit Exor-ed. After permutation the pixel sequence are read column by column .Likewise, in the receiver node the inverse key transposition is applied in permutation process in order to obtain the run length coded sequence.

In the receiver side the pixel sequence is written in column by column in after that inverse key transposition is applied then it is read row by row. Since, it is a symmetric key transposition the sequence can be recovered easily by taking inverse key transposition. The inverse transposition is done by the knowledge of symmetric key value. The key values are generated according to the pixel sequence.

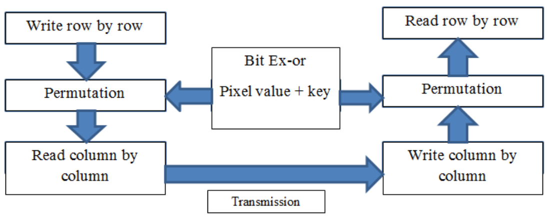

Fig. 2. Process of Key transposition.

E. *Set Partitiong In Hierarchical Trees(SPIHT)*

After key transposition SPIHT compression technique is applied on the pixel value. However, SPIHT represents a very effective form of entropy-coding,and it operates by using three lists such as LIP, LIS, LSP. The pixel values are added in these three list by using threshold value. The threshold value is calculated from 'n' which is given by following equation.

$$n=[log_2(\max_{(i,j)}|c_{i,j}|)] \quad (1)$$

where $c_{(i,j)}$ is the root pixel value. The threshold value is calculated as 2^n. At each stage, n is getting reduced by one. Thus the greater magnitude pixel values are coded first then the least magnitude values are coded. Thus at the receiver node from the greater magnitude value the image can be decompressed.

The memory requirement for SPIHT compression is given by the following equations. Let,

I: an image size of M*N pixels.
N_{LIP}: Number of entries in LIP
N_{LIS}: Number of entries in LIS
N_{LSP}: Number of entries in LSP

b: Number of bits needed to store addressing information of a coefficient.

$$b = [\log_2 (M) + \log_2 (N)] \qquad (2)$$

The total memory requirement in SPIHT,

$$M_{SPIHT} = b\,(N_{LIP} + N_{LIS} + N_{LSP}) \qquad (3)$$

In the worst case,

$$N_{LIP} = N_{LSP} = M*N$$
$$N_{LIS} = (M*N)/4$$

Thus the maximum working memory required for SPIHT is,

$$M_{SPIHT}^{max} = b\,(\frac{9MN}{4}) \qquad (4)$$

The equation.4 represents the working memory of SPIHT which will be suitable for sensor nodes.

III. IMPLEMENTATION RESULTS

Initially these operations are taken place in the sink node in the WMSN. The network consist of either analog or digital CMOS cameras. If the analog image is taken then in order to obtain the pixel sequence raster scanning is applied on the image else if digital image is considered then there is no need for raster scanning because it is already in raster format. In practical, now a days digital CMOS cameras are mostly deployed to obtain the image and there, is rare usage of analog image. So this paper focuses only the digital image which in the uncompressed bmp format. Then the process of modules are applied on the image and the output obtained is compressed and encrypted format in the transmitter. At the receiver side the original image can be obtained by applying decompression and decryption.

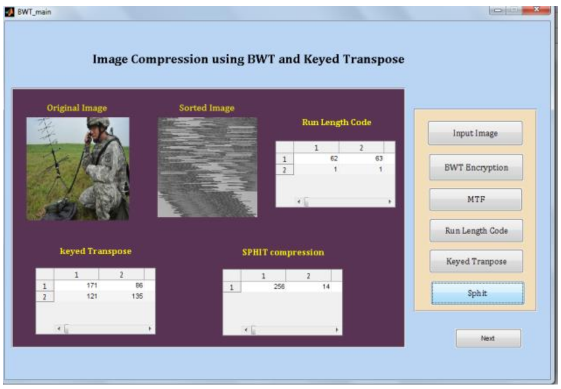

Fig. 3. Representation of Encryption and Compression Process.

For the compatibility in this paper the image with 255*255 image is considered. Then the color image is converted to grey scale image in order to obtain the intensity pixel values ranges from 0 to 255. The Fig.3 shows the output is in the encrypted and compressed format. Before applying the SPIHT the pixel sequence is written in DWT format in order to get the pixel sequence as root value, children pixel value, grandchildren and great grandchildren. Hence from the greater value which is in the root value, the threshold values are calculated and then the greater magnitude values are coded first because at the receiver side from the greater magnitude the image sequence can be easily recovered. And the time to decode is equal to time to encode which makes the operation faster. From the Fig.4 it is confirmed that the intruder gain no data because of the confusional perception at the output. These operations do not affect the image pixel values because the operations are applied on the index values generated at the BWT. Likewise in the receiver side the original image can be recovered from the index values.

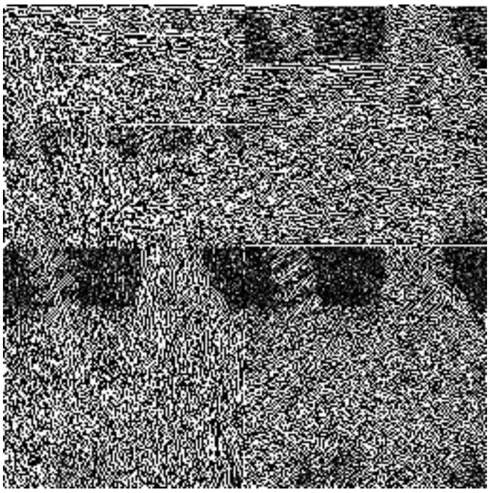

Fig. 4. Encrypted and Compressed Output.

There is no need for additional steps for decryption and decompression because from the index values both decryption and decompression is carried out in a single step.

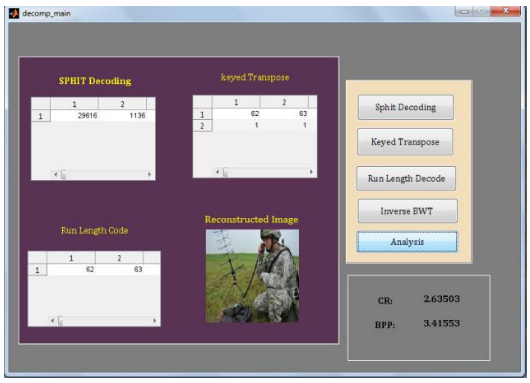

Fig. 5. Representation of Decrypted and Decompressed output.

The Fig.5 shows the decrypted and decompressed output from the compressed output. The decryption and decompression is done based on the reverse transposition and inverse operations. And due to the bijective nature of the

BWT the original image can be easily recovered without any distortion.

IV. CONCLUSION

Thus the security and effective compression in WMSN is achieved by intruding the security in compression onto the images. The process of converting the image into scalar along with encryption and compression is achieved with the help of Burrow Wheeler Compression algorithm using SPIHT and key transposition. This results the image to be compressed into a format which saves the storage space and provides an efficient secured format for transmission. Also, the intruder cannot retrieve the original sequence.

As well as more images can be transmitted with in a limited bandwidth. And the objective and subjective metric quality of the image is retrieved without any changes by the properties of BWT and key transposition.

ACKNOWLEDGEMENT

The authors like to express their thanks to the management of Sri SaiRam Engineering College and the department of Electronics and Communication for their encouragement and support during this work. Special thanks to Dr.A.R.Rajini, HOD of ECE department for their continuous help in pursuing our work.

REFERENCES

[1] J.H.Kong, K.P.Seng, L.S.Yeong, L.M.Ang, "Image Compression with Short term visual Encryption using the Burrows Wheeler Transformation and Keyed Transpose" presented at the proceedings of International Conference on Wireless Communications 2012.

[2] J.Abel,"A fast and efficient post BWT stage for the Burrows-Wheeler compression algorithm" published in IEEE conference publication in data compression conference,DCC proceeding in 2005.

[3] N.R.Jalumuri,"A Study of scanning paths for BWT-based image compression"M.S.C.S. Masters, Computer science, West Virginia University, 2004.

[4] E.Syahrul,J.Dubois, V.Vajnovszki, T.Saidani, and M.Atri, "Lossless Image Compression using Burrows Wheeler Transform (Methods and Techniques)" presented at IEEE conference on Signal Image Technology and Internet based Systems, 2008.

[5] V.S. Van,"Image Compression using Burrows-wheeler Transform",Master of Science in technology. Master's thesis, Department of Signal processing and acoustics,Helsinki University of Technology, Faculty of Electronics, Communications and Automation,2009.

[6] M.O.g.Kulekci,"On Scrambling the burrows Wheeler Transform to provide privacy in Lossless Compression",procl.in Computers & security, October 2011.

[7] M. Stanek," Attacking Scrambled Burrows-Wheeler Transform" procl in IACR Cryptography ePrint Archieve,vol.2012,p.149,2012.

[8] Effros.M,"PPM performance with BWT complexity: a fast and effective data compression algorithm"proceedings of the IEEE.vol.88,Nov 2000

[9] Arnavut.Z,"ECG Signal Compression Based on Burrows-Wheeler Ranks of Linear Prediction", IEEE Transactions on Engineering in Medicine and Biology society vol.54, March 2007.

