Slepian-Wolf Coding for Intrusion Identification System of Digital Images

Megha Jain
Assistant Professor
Vns Institute Of Technology, Bhopal

Anamika Jain
M.Tech Scholar
Vns Institute Of Technology Bhopal

ABSTRACT:
With the rapid growing of the internet technology it has been observed that the use of digital image has become the essential part in many applications. The digital image is used in various field like medical, defense, historical applications etc. While transmitting the image on internet which is such an unsafe communication medium because of the number of unauthenticated users present on the internet the image can be distorted easily with the help of several editing tools and its availability to all the users. Therefore it is essential to authenticate the image before transmitting and on the receiving side check the integrity of the image as well. Several authentication techniques have been used for image authentication. In this work non-regular Low density Parity Check (LDPC) are used for encoding the image and simultaneously encryption is done for authenticating the image on the sender side and check the authenticity of the image on the receiver side as well.

Keywords:
Distributed Source Coding, Linear Block Codes, Non Regular LDPC, Parity Check Matrix Source Coding.

1. INTRODUCTION
Nowadays, user authentication is one of the important topics in information security. Strong text-based password schemes could provide with certain degree of security. However, the fact that strong passwords are difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. In recent years, many networks, computer systems and Internet based environments try to use graphical authentication technique for their user's authentication. All graphical passwords have two different aspects which are usability and security.

Digital images become an important part of our daily lives due to the exponential growth of Internet, the increasing demand of multimedia and rapid advancement of computer technology contents from people. The up soaring number of image applications facilitates image processing. With the overwhelming diffusion of multimedia contents in every-day life, protecting the authenticity and the integrity of these contents from undesired manipulations has become an increasingly important.

Image authentication techniques have recently gained great attention due to their importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. Therefore, military, medical and quality control images must be protected against attempts to manipulate them; such manipulations could tamper the decisions based on these images. The risks for security are further exacerbated by the improved possibilities of tampering with media contents such as photos, an ability that would have traditionally required many hours of cumbersome work in a darkroom and that has become now a simple practice using a computer and some commercial software tools. In the case of images, different versions of the same file might differ from the original because of processing due, for instance, to Trans coding or bit stream truncation. Other legitimate, content preserving alterations of the original picture are also possible, when the image is enhanced by means of photo editing tools. This kind of modifications includes, for instance, moderate geometrical transformations or slight brightness/contrast adjustments. In other cases, however, one could tamper with part of the image and possibly affect its semantic content in order to illegally abuse it, e.g. to manipulate public opinion or to influence the verdict of the jury in a criminal trial. Given these premises, it is not surprising that a great deal of attention has been turned to methods able to offer proof of authenticity of an image , in the case of detected tampering, to identify which kind of attack has been carried out.

The purpose of image authentication is used to ensure the integrity of the contents of the digital image. Therefore, efficient and automatic techniques are desired to identify and verify the contents of digital images. Image authentication is such a promising technique to automatically identify whether a query image is a different one, or a fabrication, or a simple copy of an anchor image. Here, the anchor image is the ground truth image or the original image as an authentication reference, and the query image is the one under suspicion. In this work an image authentication technique is imposed which is based on using non regular LDPC codes for encoding and decoding the image with encryption and decryption.

2. NEED FOR SOURCE CODING
Source coding seeks to minimize the bit rate of a signal without an objectionable loss of signal quality in the process. High quality is attained at low bit rates by exploiting the source characteristics, the signal redundancy as well as the knowledge that certain types of coding distortion are discernible because they are masked by the signal. Techniques exploiting the source characteristics, such as signal redundancy and distortion masking are becoming increasingly more sophisticated, leading to the continuing improvement of low bit rate signals. The capability of signal compression has been central to the technologies of robust long distance communications, high quality information storage and information encryption. Compression continues to be a key in communications in spite of the promise of optical transmission media of relatively unlimited bandwidth due to the continued and increasing need to use band limited media such as radio and satellite links. Achieving a low bit rate is a key factor in meeting the demands of the new digital wireless communication systems. Impressive progress has been made

in this area in recent years. Distributed source coding (DSC) is one such technology.

2.1 Distributed Source Coding (DSC):

Source coding is a way to remove the naturally occurring redundancy in the input signal so as to reduce the bandwidth of the signal for it to be accommodated in the channel. Source coding methods can be classified into, lossless or lossy source coding. Lossless source coding is the compression of a signal where in the decompression gives back the original signal. Slepian Wolf coding is a case of lossless source coding. Lossy source coding on the other hand achieves greater compression by throwing away some parts of the signal that really don't matter. Wyner-Ziv coding is an example of lossy source coding. The source statistics play an important role in successful source coding. Shannon showed that there is a limit to which a source can be compressed without introducing errors at the decoder. Rate distortion theory gives a tradeoff between compression and quality in lossy source coding. Images, video and audio are often compressed using lossy source coding to achieve better compression techniques, however the compressors will have a lossless mode. Moreover, a lossless algorithm can be used as a building block in designing a lossy compressor.

DSC of correlated sources, is the compression of correlated sources that send their outputs to a common decoder without communicating with each other. It has evolved out of the need for removal of redundancy of data in networks involving applications using dense sensor networks. Applications involving distributed source coding are data compression for network communications, sensor networks, upgrading of existing schemes and video compression. In video compression the aim is to reduce the complexity of the encoder at the expense of increased complexity at the decoder. Practical solutions for the design of encoders for the sources are then obtained based on channel codes like block codes; convolution codes, turbo codes and LDPC codes.

2.2 LDPC codes

An (N,K) block code $C^{\perp}$ is a mapping of a message vector of length K to a codeword $C^{\perp}$ of length N. The code $C^{\perp}$ is linear if it is a K dimensional subspace of an N dimensional binary vector space VN , it can also be viewed as a mapping of K-space to N-space by a K. N generator matrix G, where $C^{\perp}$=mG. The rows of G constitute a basis of the code subspace. The dual space, $C^{\perp}$ consists of all those vectors in VN orthogonal to C so for all c$\in$ $C^{\perp}$ and all d$\in$ $C^{\perp}$ then <c, d>=0. The rows of the N-K×N parity check matrix H constitute the basis for $C^{\perp}$ so for each c$\in$ $C^{\perp}$, c$H^{\perp}$=0. Therefore a linear code is completely specified by either G or H matrix.

Low-density parity-check (LDPC) code, a linear block code defined by a very sparse parity check matrix, was first invented by Gallager in 1960's However; it has been ignored for about thirty years. The rediscovery of LDPC codes was done by MacKay and Neal a LDPC code with long block length shows good capacity-approached capability under iterative decoding algorithm, so it attracts much research interests in recent years. In practical applications, construction of good LDPC codes at short to intermediate block length is of great importance. A structured LDPC code reduces both encoder and decoder complexity and is suitable for hardware implementation. The recently proposed communication standard adopts structured LDPC codes as error-correcting codes.

3. PROPOSED WORK AND PROPOSED ALGORITHM

The image authentication system is proposed in which an authentication is done at the one side and authenticity of the image is checked on the other side. In this work conversion, mean projection and quantization, LDPC codes and a data encryption scheme is used for the process. A Non Regular LDPC Matrix is used for both encoding and decoding the image. The propose algorithm is as follows:-

4. ALGORITHM

At the sender end

- Take the image of any format, size or type for authentication. Let the image be X as shown in the figure 4.1 the input Image X goes into the system at the sender side.
- In the next step a transformation of the Image X is done. In this process the size of the image is compressed to a fix size of 336×336 which is called to a transformed image X_t.
- Than to the transformed image X_t Mean Projection and Quantization is done through which a projected data X_d is obtained which is of size 60×60.
- In the next step the projected data X_d is used for two purposes in the first part a Non regular Low density parity
- Check codes is applied to the projected data X_d through which Ldpc Encoded data $L_{(xd)}$ is yield and a conversion is done simultaneously on the projected data X_d to form a projected image I_{xd} which is again of the size 336×336.
- The next part is encrypting the projected image I_{xd} .the encryption is done using a key (k) which is generated according to the size of the original image X. The encryption is done while using the key (k) and Encrypted Projected Image X_E is generated.
- The system than sends the Original image X, Ldpc Encoded data $L_{(xd)}$, Encrypted Projected Image X_E by using a Two Way State Channel.

At the receiver end

- Let the image received through the two way channel be Image Y. the image is transformed and transformed image Y_t is formed.
- The mean projection and Quantization is done on the transformed image Y_t of 336×336 through which a projected data Y_d is generated which is of the size 60×60.
- Than with the help of Ldpc Encoded data $L_{(xd)}$ which is received by the receiver and projected data

Y_d a non linear LDPC decoding is applied which gives decoded projected data Y'_d.

- Then again conversion is done on the decoded projected data Y'_d on which decoded projected image $I_{Y'd}$ is the outcome.
- After this decryption is done using the key (k) on the Encrypted Projected Image X_E forming Decrypted Projected Image X_D.

5. THE COMPARISON

On the basis of Decoded projected image $I_{Y'd}$ and Decrypted Projected Image X_D comparison is done and if there is not a single bit error than the message will be generated that the image is the authenticated one otherwise if the system calculate even a single bit error than it will generate the message the image is tempered image.

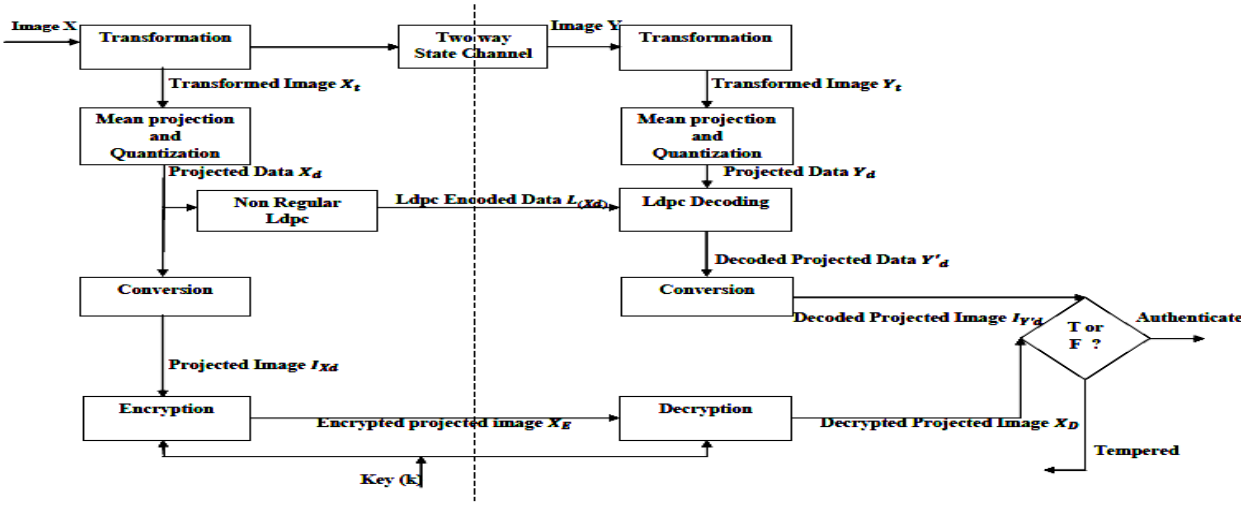

Fig 1: Flowchart Of The System

6. RESULTS

Fig 2: Original Image

Fig 3: Tempered Image

7. ANALYSIS

The original image is taken for authentication is of size 512×512 pixel. The results have been compared on the basis of statistical analysis and graphical analysis has been done.

As it is seen in figure 4.1 that when the original image is taken for ldpc intrusion identification system at both the ends that is at the sender and receiver side. When the comparative results on the basis of the statistical analysis that is on the number of pixel matching ends that is at the sender and receiver side is 3600 pixels matched out of 3600 pixels that we have taken for the authentication purpose that means the matching is 100% of pixel. And when the tempered image is taken for ldpc intrusion identification system at both the ends that is at the sender and receiver side the comparative results on the basis of the statistical analysis the pixel matching at ends from the decoded data and the decrypted data is 1872 out of 3600 about 52% respectively so it is clear from the analysis that the digital image is corrupted.

The graphical analysis has also done for the original image and the tempered image. The graph has been plotted for the size of the image which refers x-axis and the y-axis refers the gray value of the image. The comparison has been done of the image which was outputted after ldpc decoding that is $I_{Y'd}$ and the image which is decrypted that is X_D. The graph quite clearly shows the difference in the value of the pixels of the image when the comparative graph has been drawn. When the original image is authenticated the graph from decoded data and the decrypted data overlaps each other which shows the image is original as shown in figure 4.5. On the other hand when image is tempered the comparative results are shown in figure 4.6.

8. CONCLUSION AND FUTURE WORK

The results for different image are compared and it is seen that if the image is original without any single bit or single pixel distortion the system checks the authenticity of the image and gives the result as the image is validate. The system takes the image of any type, kind and size respectively. The use of non regular LDPC codes and the encryption methodology makes sure the authenticity of the image. And if the image is found to be unauthenticated it will

give the result accordingly. So the system is useful in many applications such as defense, medical, scientific etc. purposes.

On the other hand consider the image of a person in winter season when a picture of that person is taken and in

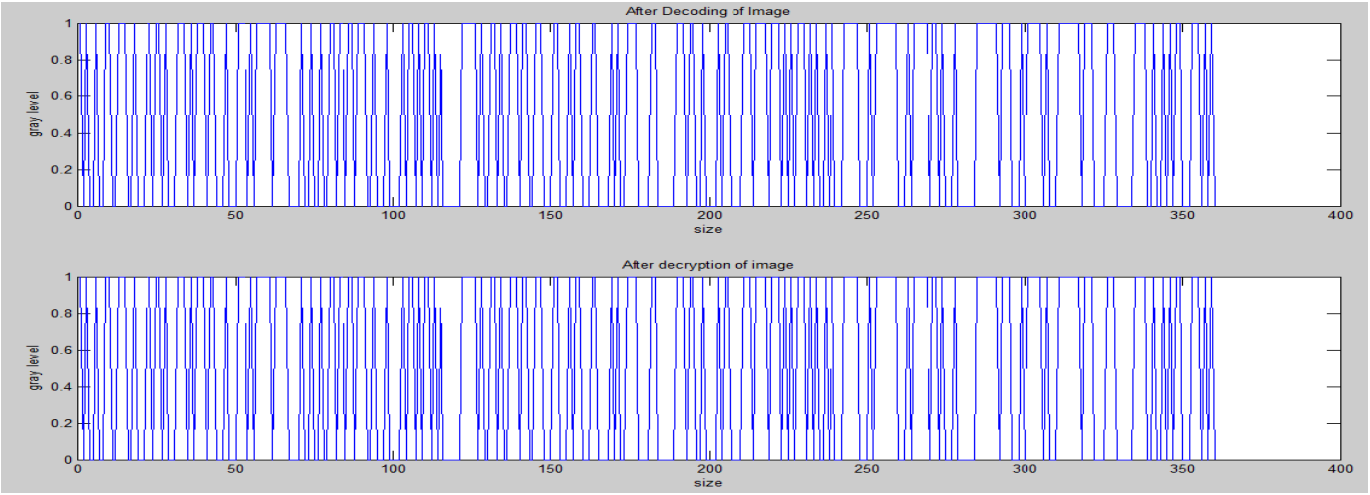

Fig 4: Graph for Original Image

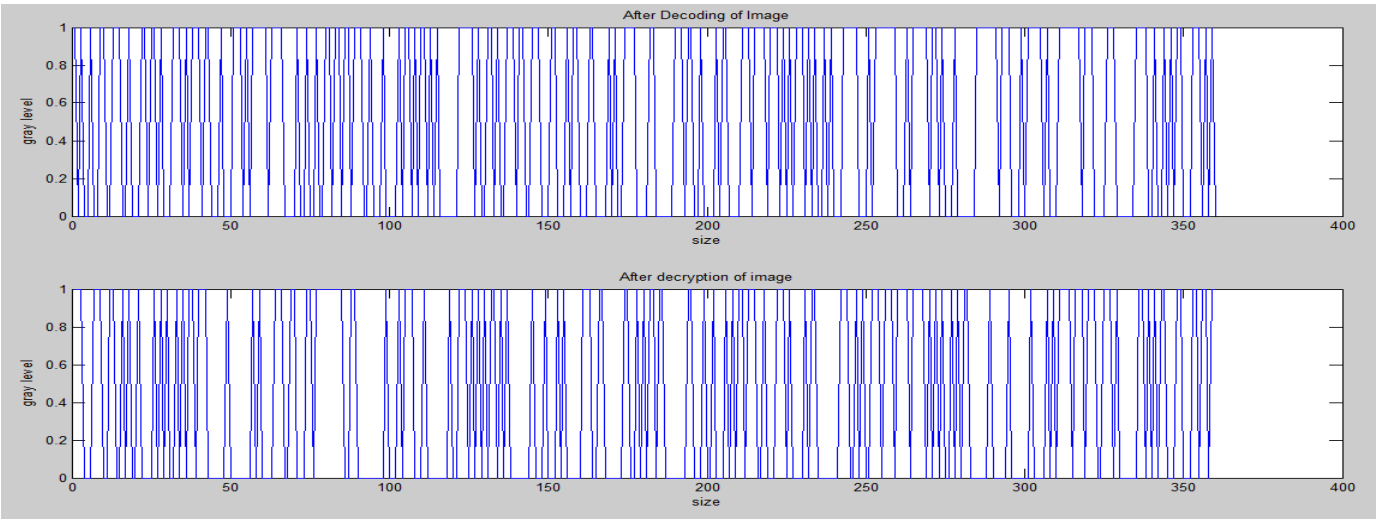

Fig 5: Graph for tempered image

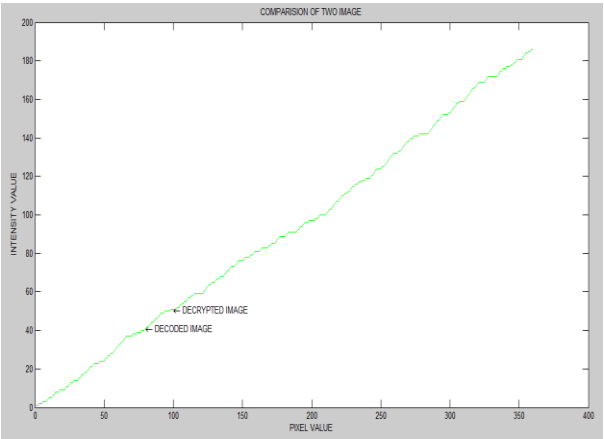

Fig 6: Comparative graph for original image

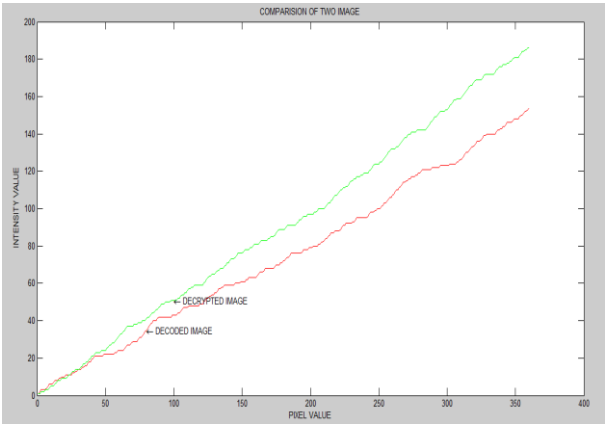

Fig 7: Comparative graph for tempered image

the same way in the summer or on a cloudy day the picture of the same person is taken might have some changes due to climatic conditions while taking the picture in two differ times. The point is the person whose picture is captured on both the occasion is the same person but the result of the two picture in the digital form or in the pixel form is different so for this the future enhancement in this work could be to appraise the features or characteristics of that person and at the time when such person has to gone through the security the system matches it features and if it's the same authenticate the person respectively.

9. REFERENCES

[1] Kostopoulos et al, "Color Image Authentication Based On Self Embedding Technique" IEEE 2002.

[2] Hossein Pishro-Nik, and Faramarz Fekri, "On Decoding of Low-Density Parity-Check Codes Over the Binary Erasure Channel " IEEE, Vol. 50, No. 3, MARCH 2004.

[3] Chi-Shiang Chan, Chin-Chen Chang ,"An efficient image authentication method based on Hamming code" Elsevier Page no.681 – 690 2007.

[4] Yao-Chung Lin, David Varodayan, and Bernd Girod, *"Image Authentication Based On Distributed Source Coding"* IEEE Vol 3 2007.

[5] Marco Tagliasacchi , Giuseppe Valenzise, Stefano Tubaro , "*Hash-based identification of sparse image tampering*" IEEE July 3, 2008.

[6] Yi-Kai Lin, Chih-Lung Chen, Yen-Chin Liao, and Hsie-Chia Chang "*Structured LDPC Codes with Low Error Floor Based on PEG Tanner Graphs*" IEEE 2008.

[7] Nabin Ghoshal, J. K. Mandal, A. Khamrui *"A Framework for Block based Image Authentication (FBIA)"* IEEE Page:343 - 348 Dec. 2009.

[8] Piming Ma, Kyung Sup Kwak "UEP-LDPC Codes with High Spectral Efficiency in Image Transmission" IEEE 2009.

[9] Jianrong Wang, Rongke Liu, Hongbo Zhao "Low Complexity DCT-Based Distributed Source Coding with Gray Code for Hyperspectral Image" IEEE 2009.

[10] Arash Habibi Lashkari et. al " A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms" IEEE 2009.

[11] GAO Bao-jian, DU Min "A binary text image authentication algorithm based on short digital signature" IEEE 2010.

[12] M Sreelatha, M Shashi, M Roop Teja, M Rajashekar And K Sasank "*Intrusion Prevention by Image Based Authentication Techniques"* IEEE 2011.

[13] Jose Antonio Mendoza Noriega, Brian M. Kurkoski, Mariko Nakano Miyatake, and Hector Perez Meana *"Image Authentication and Recovery Using BCH Error-Correcting Codes*" IJC Issue 1, Volume 5, 2011.

[14] Md. Shaik Sadi "Fingerprint Verification: A Comparison of Three Approaches" IEEE 2011.

[15] Phat Nguyen Huu, Vinh Tran-Quang, and Takumi Miyoshi "Distributed Image Encoding Scheme Using LDPC Codes over GF(q) on Wireless Sensor Networks" IEEE 2012.