International Journal on Emerging Technologies **6**(2): 126-130(2015)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Study and Development of Image Authentication using Slepian Wolf Coding

***Soheb Munir*[*]*, Dr. A.S. Zadgaonkar and Dr. Manish Shrivastava*[*]**
[*]*Department of Electronics and Communication Engineering,*
AISECT University, Bhopal, (MP), India,

(Corresponding author: Soheb Munir)
(Received 10 September, 2015 Accepted 12 October, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: This paper investigates the performance and proposes various methods for Image Authentication using Slepian Wolf coding (LDPC).The key idea is to provide an encoded quantized image projection as authentication of image or data. This can be correctly decoded with the help of an authentic data using as side information. Slepian Wolf source coding provides the desired robustness against legitimate variations while detecting illegitimate modifications. Additional adjustment might not change the means of the content, but could be misclassify as tampering. In the field of Data Communication whether images or texts, the top priority issues is security. Distinguishing legitimate encodings with possible adjustments from tampering and localizing tampering are the challenges addressed in tis paper. We apply Slepian Wolf coding and statistical method to solve the image authentication problem. Experimental results have been presented for data or image authentication.

Keywords: Image Authentication, LDPC, Cryptography, Encryption, Decryption, Tampering, Slepian Wolf coding

I. INTRODUCTION

In today's commercial environment, establishing a framework for the authentication of computer-based information requires a familiarity with concepts and professional skills from both the legal and computer security fields. Combining these two disciplines is not an easy task. Concepts from the information security field often correspond only loosely to concepts from the legal field, even in situations where the terminology is similar. For example, from the information security point of view, "digital signature" means the result of applying to specific information certain specific technical processes described below. The historical legal concept of "signature" is very broad. It recognizes any mark made with the intention of authenticating the marked document whether it is images or texts [1].

In the field of Data Communication whether images or texts, the top priority issues is security. Classical cryptography is one of the ways to secure plain text messages. In this thesis we consider the distributed source coding for digital data. A method is developed for compressing binary and non-binary sources using low density parity check codes.

Consider a sensor network consisting of sensors that are gathering information from a common environment. These sensors send the highly correlated information to a data gathering node, which forms an amalgamated view of the environment being sensed, based on a fusion of information collected by all the sensors. As the sensors have highly correlated information, communication among them will result in removal of redundant information and will also reduce the bandwidth of the transmission channel between the source (sensors) and the destination. This can be achieved as a consequence of the information theoretic bounds established by Slepian-Wolf [1] for distributed lossless coding, and by the Wyner and Ziv [7] for lossy coding using the decoder side information. One of the enabling technologies for the implementation of these theoretic bounds is distributed source coding (DSC), which exploits the source statistics at the decoder by using a simple encoder. DSC [7] is the compression of multiple correlated sensor outputs that do not communicate with each other, but send their compressed outputs to a common decoder for joint decoding. This results in increased complexity at the decoder, reversing the traditional complex encoder and simple decoder. Such systems are suitable for wireless sensor networks as the complexity of the transmitter at the sensor is reduced enabling the design of sensor transmitters that are less complex.

Driven by a host of emerging applications like remote sensing, military applications and wireless video networks, practical schemes for the implementation of the well know Slepian-Wolf [1] information theoretic bounds have appeared recently and are being explored. Such coding schemes have many other applications and hold a great promise for the new generation wireless communications as they can be applied in reliable communications to real world problems that will prove extremely exciting and will yield fruitful results. Wyner and Ziv have extended the Slepian and Wolf theorem to continuous valued Gaussian sources. According to Wyner and Ziv for two correlated sources X and Y shown in figure 3.1, the rate distortion performance obtained for encoding X is the same whether the encoder has an understanding of Y or not, if Y is available at the decoder. Most companies and institutes work diligently to maintain an effective data security policy, implementing the latest products and services to prevent fraud, sabotage, and information leakage. However this proactive up-to-date approach does not result in a successful security policy.

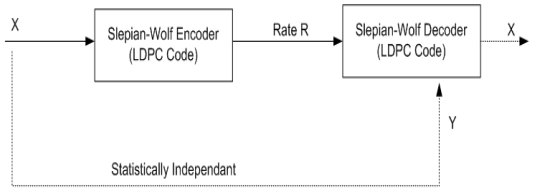


Fig. 1. Encoder and Decoder of an Image X.

The problem is that they still do not know whether and where they are vulnerable. Unfortunately, the up-to-date security approach is not adequate because it does not detect mis-configured settings An organization that truly wants to adopt a proactive approach, aggressively seeks out all types of vulnerabilities by using relevant methods.

II. LITERATURE SURVEY

A. Literature Review

This thesis first reviews about the introduction of distributed source coding techniques and low density parity check (LDPC) codes. A new method of distributed source coding for binary sources using low density parity check codes is to be developed. This new scheme for distributed source coding of binary sources using low density parity check codes is developed and implemented in the probability domain as opposed to the log domain presented by Liveris *et. al.* [4]. The performance of these schemes is analyzed by comparing the bit error rate and symbol error rate for different correlations between two randomly generated binary and non binary sources respectively.

Gallager's [5] low density parity check (LDPC) codes are defined by sparse parity check matrices, usually with a random construction. Such codes have near Shannon limit performance when decoded using an iterative probabilistic decoding algorithm. Low density parity check codes are also shown to be useful for communicating over channels which make insertions and deletions as well as additive (substitution) errors. LDPC codes can also be extended over non binary sources for channel coding by Davey *et. al.* [6]. These codes were shown to have a 0.6 db improvement in signal to noise ratio for a given bit error rate. The use of LDPC codes for distributed source coding was suggested by Liveris *et. al.* [4]. They developed distributed source coding scheme for binary sources in the log domain. This thesis deals with the development of distributed source coding for non binary sources using LDPC codes.

The first scheme is the implementation of distributed source coding scheme proposed in the paper [1]. The implementation in this dissertation is carried out using Slepian-Wolf coding (LDPC codes) in the probability domain described in [1]. This was necessitated as the development of distributed source coding for binary sources over a log domain could not be directly extended for non binary sources. Two binary sources with different correlations are considered. One of the sources is assumed to be available at the decoder and is acting as the side information. The other source is compressed and sent to the decoder. The decoder decodes the compressed source by using the side information available to it from the other source. The performance of this scheme is evaluated for different correlations between the two binary sources. The bit error rates are computed and plotted.

One of the aims of this LDPC codes is transmission of video frames using the above mentioned scheme. Video frames are highly correlated which lend themselves well for transmission using distributed source coding. The above mentioned scheme is for binary domain. This necessitated the conversion of the video frames into its binary equivalent. On conversion of the video frames into binary sequences, it was observed that the correlation between the video frames decreased drastically thereby rendering the above scheme unsuitable for video frame transmission. This led to the investigation of modifying non binary LDPC for distributed source coding which would allow the transmission of video frames without conversion to binary sequences thereby preserving the correlation. Thus the second scheme developed in this thesis provides an ideal way of implementing distributed source coding for non binary sources like video sources. The scheme devised for distributed source coding in the non binary domain is implemented for different Galois fields.

The performance of this scheme is evaluated for different correlations between the two non binary sources. The above scheme is implemented for Galois field 2 (GF(2)) and Galois field 4 (GF(4)) binary and non binary fields. Higher order Galois fields and video frame transmissions were not simulated due to memory constraints. The performance of the above scheme is quantified by using sources with different correlations as well as different compression rates at the encoder. The symbol error rates are computed for the above cases and are plotted [1]. Thus the second scheme developed in this paper provides an ideal way of implementing distributed source coding for non-binary sources like video sources. The scheme devised for distributed source coding in the non-binary domain is implemented for different Galois fields. The performance of this scheme is evaluated for different correlations between the two non-binary sources. The above scheme is implemented for Galois field 2 (GF(2)) and Galois field 4 (GF(4)) binary and non-binary fields. Higher order Galois fields and video frame transmissions were not simulated due to memory constraints. The performance of the above scheme is quantified by using sources with different correlations as well as different compression rates at the encoder [6].

III. PROPOSED METHOD FOR DATA AUTHENTICATION

A. 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 4.2 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.

-Than to the transformed image Mean Projection and Quantization is done through which a projected data is obtained which is of size 60×60.

-In the next step the projected data is used for two purposes in the first part a Non regular Low density parity Check codes is applied to the projected data through which Ldpc Encoded data is yield and a conversion is done simultaneously on the projected data to form a projected image which is again of the size 336×336.

-The next part is encrypting the projected image .the encryption is done with the help of 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 is generated.

-The system than sends the Original image X, Ldpc Encoded data , Encrypted Projected Image by using a Two Way State Channel.

B. Algorithm at the receiver end

-Let the image received through the two way channel be Image Y. the image is transformed and transformed image is formed.

-The mean projection and Quantization is done on the transformed image of 336×336 through which a projected data is generated which is of the size 60×60.

-Than with the help of Ldpc Encoded data which is received by the receiver and projected data a non linear low density parity check decoding is applied which gives decoded projected data.

-Then again conversion is done on the decoded projected data on which decoded projected image is outcome.

-After this decryption is done using the key (k) on the Encrypted Projected Image forming Decrypted Projected Image.

C. Comparison

On the basis of Decoded projected image and Decrypted Projected Image comparison is done and if there is not a single bit error than the message will be generated as 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.

D. Flowchart

Fig. 2 depicts proposed image authentication scheme. This denotes the source image as X. The user receives the image to- be-authenticated Y as the output of a two-state lossy channel that models legitimate and illegitimate modifications.

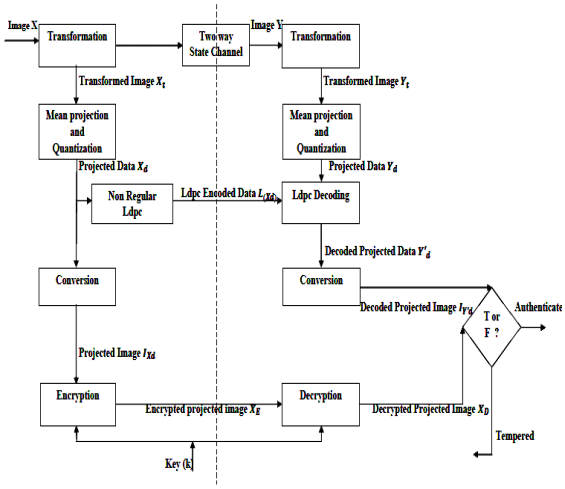


Fig. 2. An Image Authentication Scheme.

The left-hand side shows that the authentication data consist of a Non regular low density parity check code encoded mean projected and quantized image projection of X and an encrypted form of that version. The verification decoder, in the right-hand side knows the statistics of the worst permissible legitimate channel and can correctly decode the authentication data only with the help of an authentic image y as side information.

IV. RESULTS AND ANALYSIS

A. Results

It is not uncommon that a data authentication based on proposed scheme has undergone some additional adjustments, some of these we might want to accept as legitimate image adjustments. Some results based on proposed method discussed above are presented here:

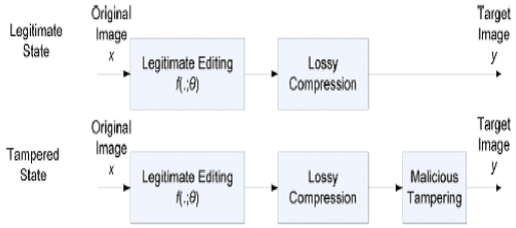
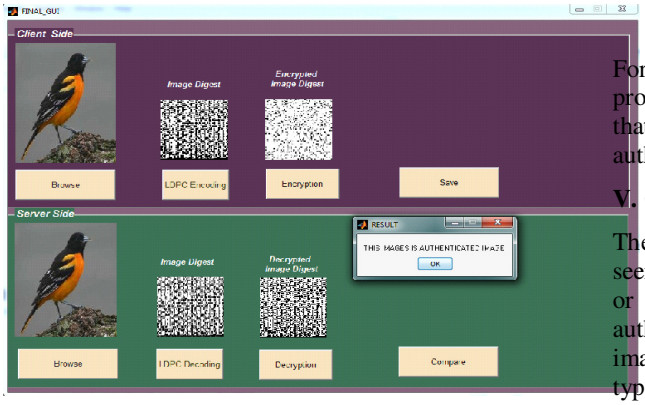


Fig. 3. The target image is modeled as an output of a two-state channel affected by a global editing function f(.;θ) with unknown but fixed parameter θ. In the tampered state, the channel additionally applies malicious tampering.

Figure 4. shows that after received the data via the transmitter side receiver start authentication process of the received data. For this process receiver apply decoding, and decryption process of encoded data if since image is not tampered so that result displayed that received image is authenticated. Figure 5 shows that after received the data via the transmitter side receiver start authentication process of the received data.



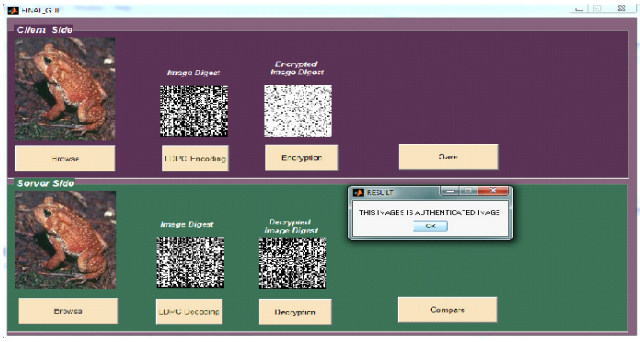
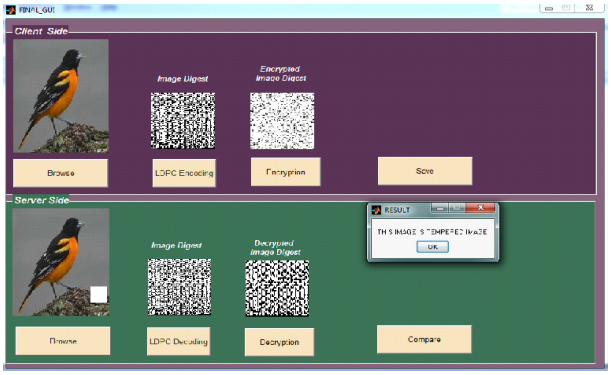


Fig. 4.



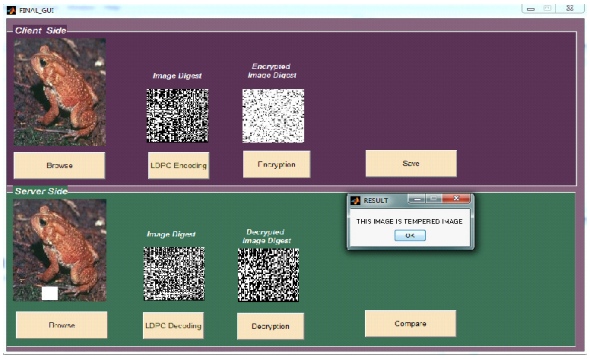


Fig. 5.

For this process receiver apply decoding and decryption process of encoded data if since image is tampered so that result displayed that received image is not authenticated.

V. 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 low density parity check 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 defence, medical, scientific etc. purposes. The findings are given below:

-In this work we have shown that non regular low-density parity-check (LDPC) codes can be used to image authentication.

-The system can work with any type of image and the result shows that even a single bit distortion in the image can be detected.

-We can observe from the results that LDPC in the probability domain can be used to implement distributed source coding.

-A high performance is given by these codes.

-Distributed source coding is an ideal tool for the image authentication problem in which the data sent for authentication are highly correlated to the information available at the receiver.

-This method gives the better performance in all aspects in comparison to the previous work.

1. In the future, the proposed scheme can be extended for the compression of video frames. It can be used for practical implementation of distributed source coding in video communication and sensor networks.

2. The approaches in which the projection or the features might be invariant to the contrast, brightness, and affine warping adjustment, we solve this problem by decoding the authentication data while learning the parameters that establish the correlation between the target and original images. 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. The work can be extended accordingly.

REFERENCES

[1]. D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. **IT-19**, no. 4, pp. 471–480, Jul. 1973.

[2]. Kshetri, N., "The simple economics of cybercrimes", *IEEE Security and Privacy* ,vol. **4**, no. 1, 2006.

[3]. J. Liang, R. Kumar, Y. Xi, and K. W. Ross, "Pollution in P2P file sharing systems," *in Proc. IEEE Information communication*, Mar. 2005, vol. **2**, pp. 1174-1185.

[4]. A.D. Liveris, Z.Xiong and C.N. Georghiades. "Compression of binary sources with side information at the decoder using LDPC codes". *IEEE Commum. Lett.,* vol. **6**, pp.440-442 .

[5]. R.G. Gallager, "Low density parity check codes". PhD thesis, MIT, Cambridge, Mass., September 1960.

[6]. Matthew. C. Davey and D.J.C. Mackay. "Low density parity check codes over GF(q)". *IEEE Commum. Lett.*, vol. **2**, pp.165-167, June 1998.

[7]. Y.C. Lin, "Image Authentication Using Distributed Source Coding," Ph.D. dissertation, Stanford University, Stanford, CA, 2010.

[8]. D. Varodayan, A. Aaron, and B. Girod, "Rate-adaptive codes for distributed source coding," EURASIP Signal Process. J., *Special Section on Distributed Source Coding,* vol. **86**, no. 11, pp. 3123-3130, Nov. 2006.