DEVELOPMENT AND IMPLEMENTATION OF IMAGE AUTHENTICATION ALGORITHM USING LDPC

Fiza Pathan[1], Rahul Sahu[2]
Lakshmi Narayan College of Technology

Abstract: This paper presents an image authentication method for digital images. The idea is to fabricate an authentication system which authenticates the digital image. The need for this type of scheme is to secure the digital image before sending it over a two way state channel. The digital image which is taken can be of any type, format, size etc. After selecting a digital image, transformation is done to make it of a fix size , the mean projection and quantization is to be done. After then on this digital image a Slepian-Wolf coding (regular low density parity check code) is to be applied which encodes the digital image. And at the same time encryption is to be done on the projected converted image on which a conversion is done. The sender then sends the digital image with its encoded and its encrypted form through a two way state channel to the other end.

On the receiver side a reverse process is to be applied to check the authenticity of the digital image. The digital image which is received on which the transformation of the digital image is to be done then its mean projection and quantization is done after that a non regular low density parity check matrix is to be applied on the projected image and at the same time using the encoded digital image which is received decoding is done. Then conversion is done on the decoded image while a decryption is done on the encrypted image.

Keywords: Image Authentication, digital image, authentication system, mean projection, Slepian Wolf coding, encryption.

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.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. Cryptography addresses the necessary elements for secure communication namely privacy, confidentiality, key exchange, authentication, and non-repudiation but reveals the fact that communication is happening. Authentication takes cryptography a step to determine that the received data is authenticated or not.

Need of Authentication

New ways of verification are being developed daily to daily life of humans. Biometrics and other methods keep getting formulated and incorporated into the information technology industry. One interesting biometric authentication mechanism developed by a leading Japanese biometric company has found a way to get your DNA. You sign a document and it is digitally scanned, this document is then can be scanned in the future to verify its authenticity. Identity should be verified whenever there is doubt of the 3rd party being whom they say or when there is personal information at risk. Personal information like credit card details and banking information should be kept safe using digital certification as one of the security layers. Some banking institutions require that a user verifies his/her identity by validating identification credentials using a digital certificate. Important e-mail can also use digital signatures that verify the e-mail is from the originating sender and that it has not been tampered with. On many occasions users are unsure if they are dealing with reputable suppliers of institutions. Digital certification gives the user a sense of legitimacy and formalizes the process. It ensures that the company that the user is dealing with has a registration with a trusted authority and that the transaction is guaranteed to be done with the intended parties. Now we will define the basic components of Digital Signature i.e. Encryption, Decryption and Hashing[3].

II. LITERATURE REVIEW

In this chapter we describe different literatures related to the field of image authentication. We conclude that various methods given by the researchers in the area of image authentication. In the chapter three we will describe in brief about the binary low density parity check codes (distributed source coding) is to use for image authentication.

This thesis first reviews about the 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 [1]. 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 low density parity check (LDPC) [11] 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. 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.. LDPC codes can also be extended over non binary sources for channel coding by Davey et. al. [2]. These codes were shown to have a 0.6 db improvement in signal to noise ratio for a given bit error rate.

LDPC CODES

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.

Low density parity check codes (LDPC) are a class of linear error correcting block codes introduced by Gallager[11] in 1962 [9] and rediscovered by Mackay and Neal [10]. Improvements of low density parity check codes have allowed them to surpass the performance of turbo codes. LDPC codes are defined in terms of a sparse parity check matrix in which most of the entries are zero and only a small fraction are nonzero values. Each code word satisfies a number of linear constraints and each symbol of the codeword participates in a small number of constraints. The constructions, description of an iterative probabilistic decoding algorithm and theory provided by Gallager goes beyond what is known today for turbo codes. Arriving before the computing power that was to prove their effectiveness they were largely forgotten until the rediscovery by Mackay and Neal[10].

Distributed Source Coding Using Binary LDPC Codes

Low density parity check codes can be used for applications involving compression of two correlated sources using the syndrome concept. The compressed sequence of the source output bits is the syndrome, which is determined using the parity check matrix H. It has been shown that LDPC codes can be employed when viewing the problem using an equivalent channel and applying the syndrome approach for the case where one of the two correlated sources is available lossless at the joint decoder. This can be viewed as application of LDPC codes to a compression problem with side information. It is based on modifying the conventional message passing LDPC decoder to take into account the syndrome information. Also all LDPC code design techniques can be applied to distributed source coding producing simulation results better than any turbo coding scheme.

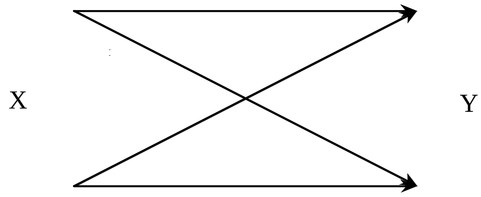


Figure : Modelling Correlation using BSC

Decoding

Decoding involves the estimation of the N-length sequence X from the (N-K) length syndrome S and the N-length sequence Y. The decoding algorithm is similar to LDPC decoding used for channel coding expect for the inclusion of the syndrome bits in the horizontal step of the algorithm. The set of noise bits n that participate in check m are denoted by $N(m)=\{n:H_{mn}=1\}$. We also define the set of checks in which noise bit n participates, $M(n)=\{m:H_{mn}=1\}$.$N(m)\backslash n$ denotes the set of noise bits excluding the noise bit n. There are two quantities q_{mn}andr_{mn}associated with each non-zero element in H matrix that is alternatively updated iteratively. q_{mn}^{a} is the probability that noise bit n of X has the value a, given information obtained via checks other than the check m. r_{mn}^{a} is the probability of check m being satisfied if bit n of X is considered fixed at a with the other bits having separable distribution given by $\{q_{mn} : n\in N(m)\backslash n\}$.

The most important chapter in this whole paper is Image Authentication System which is actually the proposed methodology of this work which is further discussed.

Image Authentication System

The image authentication based on Slepian-Wolf coding is shown in figure 1 In which we have shown that we apply Slepian-Wolf coding on legitimate image X with certain code rate say R and also we provide this information to Slepian-Wolf decoder with Y as side information.

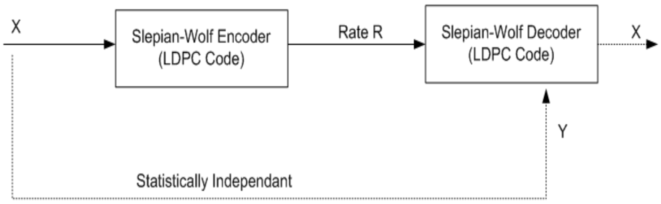


Figure 1: The source X and side information Y are statistically dependent, but Y is available only at the decoder.

Figure 1 shows that model of legitimate image X with original state in Jpeg/Bmp format with target image y and also in next part we have shown that legitimate image with tampered state i.e. legitimate image with malicious attack to produce target image. In the legitimate state, the channel consists of lossy compression and reconstruction, such as JPEG and JPEG2000; in the tampered state, the channel further applies a malicious attack.

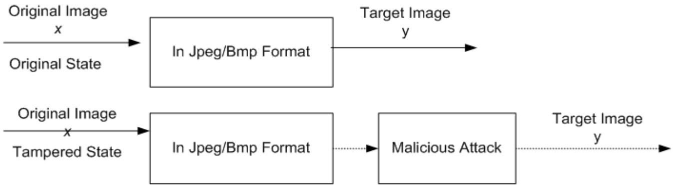


Figure 2: The target image y is modelled as an output of a two-state lossy channel.

We can conveniently formulate image authentication as a hypothesis testing problem. The authentication data provides information about the original image to the user. The user makes the authentication decision based on the target image and the authentication data. We first describe a two-state channel that models the target image and then present the image authentication system using distributed source coding.

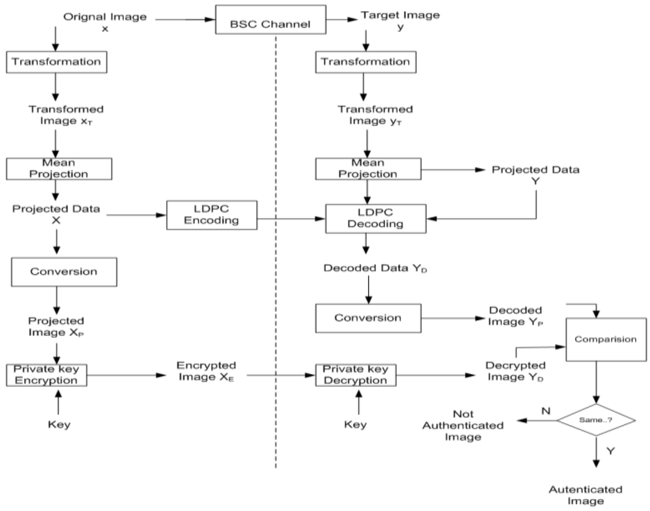


Figure 3: Block Diagram of Image authentication system using Slepian Wolf coding.

Figure 3 shows that the distributed source based image authentication system: from client side we transform original image with division of 16x16 block size and taking mean projection of each block, which is our projected data say, X_P encript this X_P with private key. From receiver side we send following data legitimate image through BSC channel, LDPC encoding and encrypted image X_E. We transform the target image y as $y_T$and taking mean projection of y_T which is our projected data Y and LDPC decoding of y_T as decoded data Y_D. Compare the decoded image Y_P and decrypted image Y_D, it produce binary output yes for image is authenticated and otherwise image was not authenticated

Decoding the authentication data by trying out all possible editing parameters is clearly not feasible.

III. PROPOSED ALGORITHM

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 below 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.

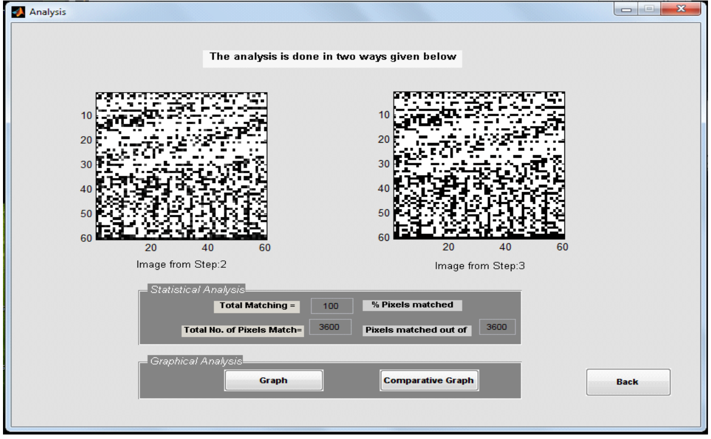
Algorithm at the receiver end

- 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.
- Then 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.

Experimental Results and Analysis

The experimental results of proposed image authentication system presented in this chapter can address various types of distributed source coding. The results for unaffected and affected image are compared on the basis of statistical and graphical analysis.

Statistical Analysis



The analysis is done in two ways given below

Total Matching = 100 % Pixels matched

Total No. of Pixels Match= 3600 Pixels matched out of 3600

Figure 4: Statistical analysis output of the image

Graphical Analysis

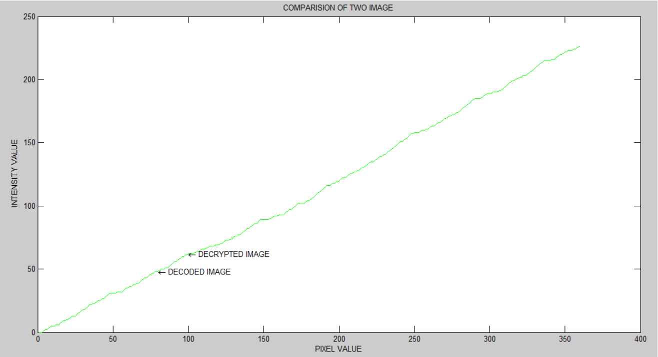


Figure 5: Graphical analysis output of the image

Graphical User Interface for affected or tempered Image
Consider the same digital image which was previously authenticated and its results shows that the image received is 100% authenticated one now some changes has been done with the same image with its properties. The server side will perform the same procedure for encoding and encryption for the affected digital image.

IV. CONCLUSION

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.

REFERENCES

[1] A.D. Liveris, Z. Xiong, and C. Georghiades, “Compression of binary sources with side information at the decoder using LDPC codes,” *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[2] Mathew.C.Davey and D.J.C. Machay. " Low density parity check codes GF(q)".IEEE Commun.Lett., "Image Authentication Using Distributed Source Coding" PhD. dissertation , Stanford University, Stanford ,CA,2010.

[3] H. Farid, “Image forgery detection,” *IEEE Signal Process. Mag.*, vol.26, no. 2, pp. 16–25, Mar. 2009.

[4] J. Lukas and J. Fridrich, “Estimation of primary quantization matrix in double compressed JPEG images,” presented at the Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003.

[5] A. Popescu and H. Farid, “Exposing digital forgeries in color filter array interpolated images,” *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3948–3959, Oct. 2005.

[6] Brajesh Kumar, Anand Rajput, Alka Aman, “ LDPC Based image Authentication System ,” 4th*International Conf . on Computer and Communication Technology(ICCCT)* , 2013.

[7] J. J. Eggers and B. Girod, “Blind watermarking applied to image authentication,” in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Process.*, Salt Lake City, UT, May 2001.

[8] R. B. Wolfgang and E. J. Delp, “A watermark for digital images,” in *Proc. IEEE Int. Conf. Image Process.*, Lausanne, Switzerland, Sep. 1996.

[9] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Jan. 1976.

[10] C.-Y. Lin and S.-F. Chang, “Generating robust digital signature for image/video authentication,” in *ACM Multimedia: Multimedia and Security Workshop*, Bristol, U.K., Sep. 1998, pp. 49–54.

[11] R.G. Gallager "Low Density Parity Check codes" phD thesis MIT , Cambridge, Mass September 1960.

[12] C.-Y. Lin and S.-F. Chang, “A robust image authentication method distinguishing JPEG compression from malicious manipulation,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, no. 2, pp. 153–168, Feb. 2001.

[13] C. Kailasanathan, R. S. Naini, and P. Ogunbona, “Compression tolerant DCT based image hash,” in *Proc. Int. Conf. Distributed Computing Syst. Workshops*, May 2003, pp. 562–567.

[14] C.-S. Lu and H.-Y. M. Liao, “Structural digital signature for image authentication: An incidental distortion resistant scheme,” in *ACM Workshops on Multimedia*, Los Angeles, CA, 2000, pp. 115–118.

[15] C.-S. Lu and H.-Y. M. Liao, “Structural digital signature for image authentication: An incidental distortion resistant scheme,” *IEEE Trans.Multimedia*, vol. 5, no. 2, pp. 161–173, Jun. 2003.