Implementation of Optimum Compression Algorithm for Image and Text Data Transmission using DWT

Sudha Rani J
Mtech Student in Digital Electronics Dept of ECE
BITM, Ballari, Karnataka, India

Manjunath G
Assistant Professor
Dept of ECE
BITM, Ballari, Karnataka, India

ABSTRACT
Companies, parliaments, institutes and military often need to transfer a highly sensitive data and always be alert about the risk if the data is leaked by unauthorized parties. Encryption can be implemented to securely transfer the data. It can further be secured by a secret key by the sender and sent to the recipient who can decrypt the data only using the secret key created by the sender. Text data being hid in the picture is another method to predict the limited text data, ability and its measure during encoding and decoding. This project involves the plan of how the text and image data can be securely sent from the source to destination without any fear of data being stolen or leaked by the unauthorized parties. The transform methodology used here is "discrete wavelet transform [DWT] and watermark" is embedded in the raw image and can be extracted by the recipient. It exhaustively defines data encoding and decoding using mat lab for small text messages and recommends such features.

General Terms
Image compression, data transfer, video.

Keywords
Cryptography; Video watermarking; DWT; Encryption.

1. INTRODUCTION
Digital media has replaced the conventional analog media and will go on with doing so. Digital media means digital representations of text data, audio clips, images, videos, three-dimensional scene, and so on. Digital media offers a great advantage over its analog ancestors for example audio and video cassettes. Unlike analog media, the digital media cannot just be stocked up but also copied, and redistributed with zero loss of data. Digital media can further be manipulated and modified easily and so it offers many advantages, but also builds problems to the parties who aspire to prevent illegal reproduction and distribution of digital data.

The effortlessness in editing, copying and sharing digital data has created many complexities to the authorized parties who desire to prevent prohibited use of such documents. And so "digital watermarking" is put forward as a "last line of defense". Digital watermark is a robust, imperceptible, and secure message rooted straight into a document. The watermark is imperceptible statistically as well perceptually. It further defines that watermark can neither be erased nor edited until the document is modified to the moot point. Watermark is said to be secure if the illegal parties can neither erase nor modify it. Existing methods can be analyzed as spread spectrum communications structure, which transmits data redundantly by means of low amplitude, pseudo noise carrier signal.

2. PROBLEM STATEMENT
The existing method uses the 'diffusion and substitution' scheme. This method is based on the spatial domain transformation which is not as secure as the proposed method and yet time consuming. The other method is transposition cipher. The method of substitution and transposition is collective into diffusion ciphers, which is implemented in all modern symmetric key ciphers. Example smart phones. This kind of encryption methods, known as the digital signature, wouldn't shield the secrecy of data. The sender is not permitted to show that he was the designer of the data signed until the secret key was negotiated.

3. METHODOLOGY
3.1 Proposed methodology
The proposed method involves the encryption of the data using the secret key. The key is used for both encryption and decryption process. The data is encrypted using this secret key. This key is also called as symmetric key. The cryptographic method is used for encryption process. The data may be an alphabets, symbols and numbers. The data can be of any length. The data is securely transmitted with the help of video signal. Initially, the video signal is split into frames of equal size. The encrypted data is embedded into any one of the frames. Then various parameters of the image are analyzed. The frames are then converted into video signal and are transmitted through wireless channel. The video signal has different formats such as MPEG, AVI, etc. They are converted into different image formats such as JPG, BMP, etc. Their performance parameters are analyzed. The parameters include Mean Square Error, Peak Signal to Noise Ratio, Structure similarity.Fig.1 shows the block Diagram of data embedding using water marking, shows the general information of the process. The cryptographic method is used for encryption process. The data may be alphabets, symbols and numbers. The data can be of any length. The data is securely transmitted with the help of video signal. The video signal can be of any type of format. Initially, the video signal is converted into frames of equal size. The encrypted data is embedded into any one of the frames. Then various parameters of the image are analyzed. The frames are then converted into video signal and are transmitted through wireless channel.

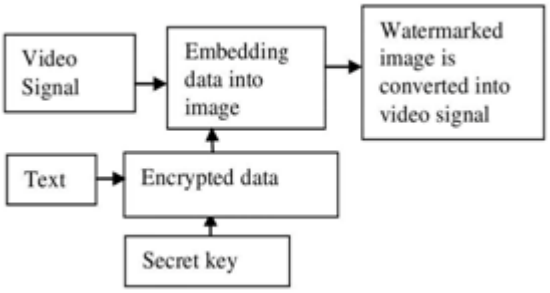

Figure 1: Encryption of data

In secure communications using cryptography, which is the main focus of the present work, the encryption and decryption operations are guided by one or more keys. Techniques that use the same secret key for encryption and decryption are grouped under private key cryptography. Fig.2 shows Block Diagram of data retrieval process using water marking is shown for the decryption of data. There are two levels of security for digital image encryption low level and high level security. There are two fundamental properties which every secure encryption method must satisfy .The first is the confusion property which requires that cipher texts should have random appearance, i.e. uniformly distributed pixel values. The second is the diffusion property which requires that similar keys should produce completely different cipher texts for the same plaintext.

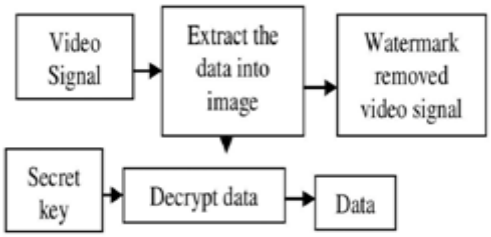

Figure 2: Decryption of data

3.2 Results and Discussions

Simulation results for image data transmission

The transmission of text data through video is done at 100% accuracy. The privacy of the data is maintained till the data reaches to person who has the secret key to retrieve the data. For text data, it is a lossless compression. At the receiving end, the video is split into frames and the encoded text is extracted with no loss of information and is as shown below

Inputs: The Confidential text data given here

First input: Hello

Second input: How are you

Third input: What are you doing

Secret Key1: Apple Secret

Key2: BallSecret

Key3: Camel

The confidential text data is encoded in the frame 9

Figure 3: Frame 9, in which text is embedd.

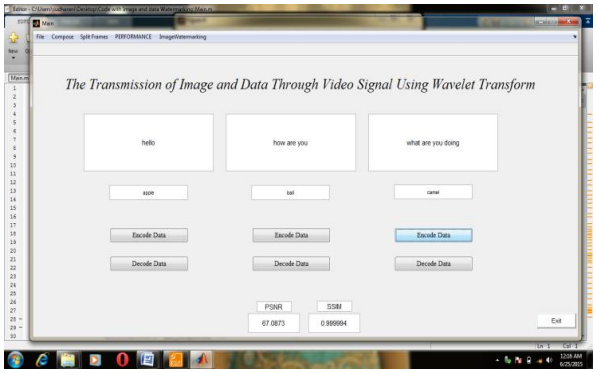

Figure 4: PSNR and SSIM

The confidential data and secret key are entered. The PSNR and SSIM are the two performance metrics considered here whose values are seen in the figure4. The encoded image data in stored in MATLAB into one particular frame in RYB format.

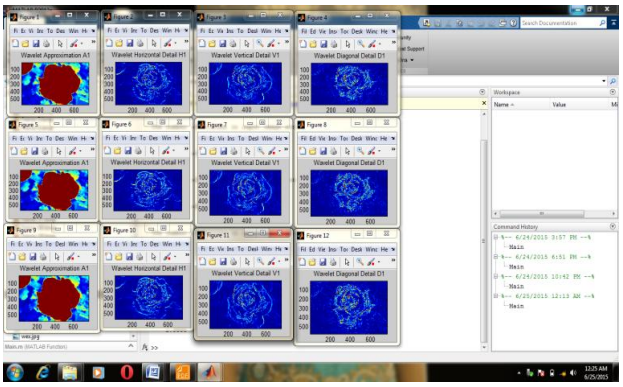

Figure 5: Data storage in MATLAB

Output:

By entering the correct secret key and choosing the suitable encoded frame, the confidential text data is recetrieved.

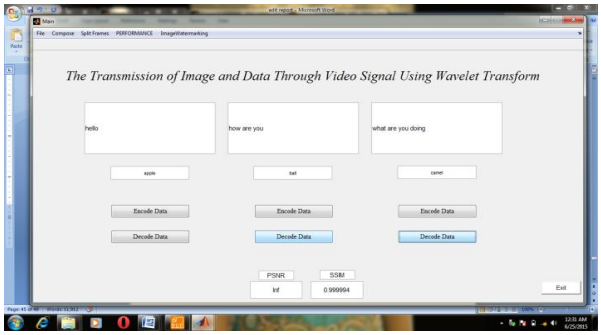

Figure 6: Retrieved output text data.

At the receiving end, the text data is received that is lossless and the privacy is maintained till the data is received at the end user. The SSIM (Structure Similarity) is 0.999994~1

Simulation results for image data transmission

The transmission of the image data through video is performed. The privacy of the data is maintained till the data reaches to person who has the secret key to retrieve the data. This compression is a lossy compression. An invisible watermark affects the visual quality of the image.

There is a difference in quality of the image sent and the image received as a result of variations in the PSNR and the compression losses during the encryption and decryption process, this leads to the changes in overall performance. There is an evident decrease in perceptual quality of the watermarked image data extracted from encoded image data which is featured due to the imbalance between robustness against incidental distortions, and fragility to tampering attacks.

Figure 7: Base image.

Figure 8: Watermarked image.

The Watermarked image is a gray scale image and the PSNR of the watermark is 41.4819dB . The extracted image is as shown below

Figure 9: Confidential image.

The Base image in which the confidential image must be embedd is chosen.The image to be embedd is also chosen as shown in figure 10 and figure 11.

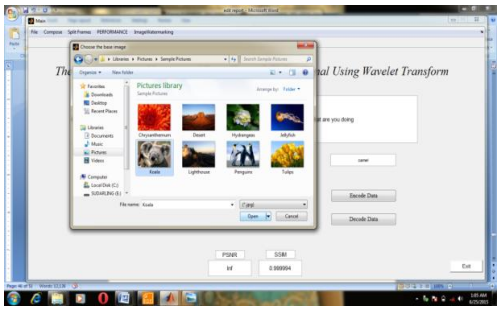

Figure 10: Choose base image.

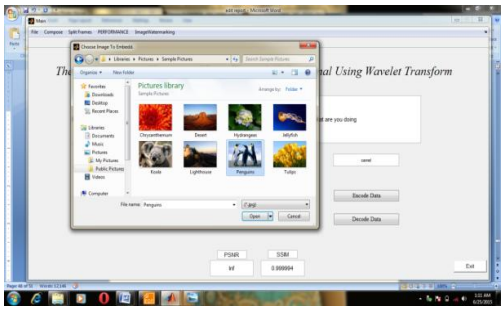

Figure 11: Choose image to embed.

Like the text data transmission, the video is composed with the split frames along with the embedded image

Output: The video is split into frames and the confidential image is extracted from the embedded image

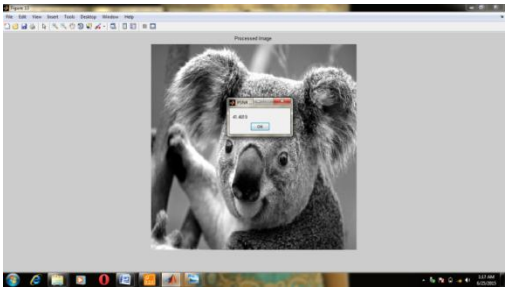

Figure 12: image PSNR

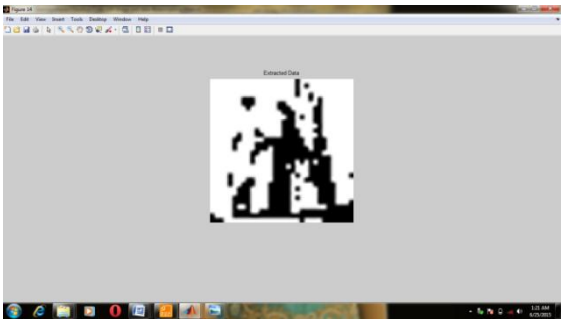

Figure 13: Retrieved output image

4. ADVANTAGES

1. On implementing encryption, the data to be transferred can be kept secured.
2. The illegal parties cannot retrieve the data because they do not have the secret key that decrypts the data.
3. With the aid of the proposed algorithm, any illegal activities such as theft or data editing can be caught.
4. This algorithm also helps in safe decommissioning of data.
5. On implementing the proposed method also provides with peace of mind along with the illegal access shield and fulfillment with data protection acts.

5. CONCLUSION

The data transfer through video for both image and text data using DWT and watermark methods is designed and performed individually for different data types according to the proposed software specifications with proper optimization. The proposed algorithm is tested for different videos, text data and image data, the result analysis of image data and text data is tabulated together and compared with respect to the corresponding simulation results. From the above work we can conclude that the results obtained are 80-90% matching with proposed results.

The differences in the comparison are obtained as a result of small variations in the signal to noise ratio and the compression losses during the encryption and decryption process, this leads to marked changes in overall performance. There is also an apparent shift in perceptual quality of the watermarked image data extracted from desired image data which is attributed due to the imbalance between robustness against incidental distortions, fragility to tampering attacks. This scheme provides two tier securities, first using cryptographic key and second using steganography key where the secret message is encrypted before embedding and decrypted after decoding. An invisible watermark affects the visual quality of the image. To overcome this problem a measure by which one can judge how the quality of image is degraded, is essential. The PSNR metric is widely used to measure the difference between two images based on pixel differences.

6. FUTURE SCOPE

This work can be extended in future in the following directions.

1. Error detection and correction techniques can be applied to reduce errors.
2. In the proposed algorithm, 2D-DWT algorithm and Haar wavelet filter are used for the watermark functionality against various geometrical distortions. For further improvements 3-D DWT and directionality features of new transforms like the Curvelet transforms, Slantlet transforms could also be possibly investigated for its exploitation.

7. REFERENCES

[1] Yvette E. Gelogo and Tai-hoon Kim ,"Compressed images transmission issues and solutions"2006

[2] C-C Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". The Journal of Systems and Software, 58:83–91, 2001

[3] Vladimir Cherkassky, Xuhao He, Prakash Balasubramanian, "Wireless transmission of image and video data",1996

[4] S.Poongodi and Dr.B,Kalaavathi, "The Transmission of Image and Data Through Video Signal Using Wavelet Transform" 2014.

[5] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC" 2006.

[6] Anwar H. Ibrahim and Waleed M. Ibrahim, "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time", IJITCS, vol. 7, no.3, January / February, 2013.

[7] F. Hartung and M. Kutter, "Multimedia watermarking techniques", Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[8] I. J. Cox and M. L. Miller, "Electronic watermarking: the first 50 years". Fourth, IEEE Workshop on Multimedia Signal Processing, 2001, pp. 225-230, October 2001.

[9] Bibhudendra Acharya1, Saroj Kumar Panigrahy2, Sarat Kumar Patra3, and Ganapati Panda3, "Image encryption using advanced hill cipher algorithm", ACEEE International Journal on Signal and Image Processing Vol 1,No. 1,37-41, Jan 2010.

[10] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukr, "Efficiency and Security of some image encryption algorithms", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008,London, U.K. 978-988, July2- 4,2008.

[11] Gang Qiu, Pina Marziliano, Anthony T.S. Ho, Dajun He, and Qibin Sun, "A hybrid watermarking scheme for H.264/AVC video", Proceedings of the 17th International Conference on Pattern Recognition ICPR, 2004.