ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

The Transmission of Image and Data Through Video Signal Using Wavelet Transform

S.Poongodi[1], Dr.B,Kalaavathi[2],

Assistant Professor, Dept. of ECE, K.S.R. College of Engineering, Tiruchengodu, Tamilnadu, India [1]

Prof & Head, Dept. of CSE, K.S.R. Institute for Engineering and Technology, Tiruchengodu, Tamilnadu, India[2]

Abstract: Due to the advanced network technology, security of data transformation is a big problem in this society. The usage of cryptography secret key method along with watermarking provides the security of data transmission. Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity. Cryptography is a method of encryption and decryption. The encryption is used to securely transmit the data in open network. Each type of data has its own features; therefore different technique should be used to protect confidential data from an unauthorized access. The proposed technique is simple to implement and has high encryption rate of security and this method embed the data into the image. The image is encrypted using secret key method and then watermarked into video signal. This encrypted image is transmitted through video signal and the security analysis is measured using some parameters. The comparison between the different file formats of the video signal.

.

Keywords: **Cryptography, Video watermarking, DWT, Encryption.**

I. INTRODUCTION

Cryptography is a tool that can be used to keep information confidential and to ensure its reliability and accuracy. Cryptography is a method of encryption and decryption. It plays a central role in mobile phone-communications, pay-TV, sending private emails, transmitting financial information, security of ATM cards, computer passwords, and touches on many aspects of our daily lives [2]. Cryptography has encrypted the image and data and also this method convert the plain text into cipher text and then retransforming that message back to its original form. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for text data [4]. Cryptographic algorithms can be divided into symmetric-key algorithms and public-key algorithms [3]. Encryption process transforms plain-image data into cipher-image through involving an algorithm for combining the original image with one or more keys [5]. Techniques that use the same secret key for encryption and decryption are grouped under private key techniques [6], [7]. While, asymmetric key techniques use two different keys; public key for encryption and private key for decryption [8]. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [4]. In most of the natural images, the values of then neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors) [4]. In order to dissipate the high correlation among pixels and increase the entropy value, we propose a new method along with watermarking, both are security related method. In this method, that divides the image into blocks and then shuffle theirs positions. The security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of user's privacy for all applications [6]. Encryption and steganography techniques of digital images are very important.

II. CRYPTOGRAPHY

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. There are two levels of security for digital image encryption –

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

low level and high level security [9]. There are two fundamental properties which every secure encryption method must satisfy [9].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.

In order to transmit data and image securely over public channels, a variety of encryption algorithms have been suggested. These algorithms can be classified into three major categories: position permutation], substitution transformation and permutation substitution transformations.

The secure transmission of data is very important over the multimedia network. The block diagram of the proposed work is in fig. 1 & 2. Here the data is encrypted by using secret key with the key size of 256 bits and then transmitted**.**

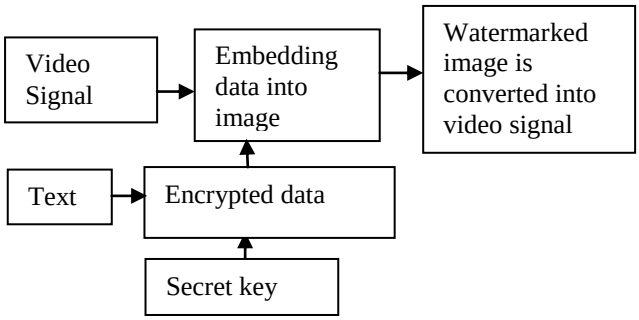

Fig.1 Block diagram of data embedding using watermarking

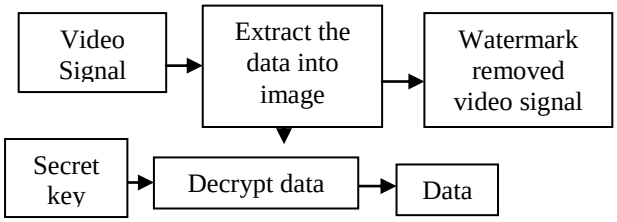

Fig:2 Block diagram of data retrieval process using watermarking

III. VIDEO WATERMARKING

The video watermarking is the emerging field in the secure data transmission.initially the video signal is converted into number of frames and then the encrypted data is embedded into any one of the video frame. Then after the embedding process the frames are again converted into video signal. Visually and as well as by analytically the variation in the video signal before embedding and after embedding, the difference between them is no change. So the third person cannot recognize from the video signal. Even though if somebody identified that something is embedded into the video then they cannot retrieval easily. Because they must known the frame number as well as the secret key Here we are providing better security for data transmission .In this method, tested many video file formats and that compared which video file format provide better results for the proposed method.

IV. PROPOSED METHOD

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

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

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. The video signal has different formats such as MPEG, AVI, etc.,. They are converted into different image formats such as JPG, BMP, etc.,. Their parameters are analyzed. The parameters include Mean Square Error, Peak Signal to Noise Ratio, Cross Correlation, Structural Content, Maximum difference and Normalized absolute error.

V. RESULTS AND DISCUSSION

Simulations are performed to evaluate the proposed method. The video watermarking technique with secret data sharing technique greatly increases the security. The results based on the sample of 6 different sets of video file formats. Here we used the 1364*768 raw data sequence with 200 frames. Among the all the comparison of file formats the mpg file format produce the better PSNR value with low maximum difference. After the decryption method the data as well as the video both are retrived properly. In the first step of the simulation, convert the video into frames. Each frame is an image. Among these images, select any one particular image and this is called as key frame. The data is embedded into that key frame and this key frame is again decrypted in the receiver side. Finally the data and video both are retrieved properly. Only the sender and receiver know the key frame number and the secret key. Any intruder must not retrieve the data without knowing the number of the key frame, because the video have many number of frames.

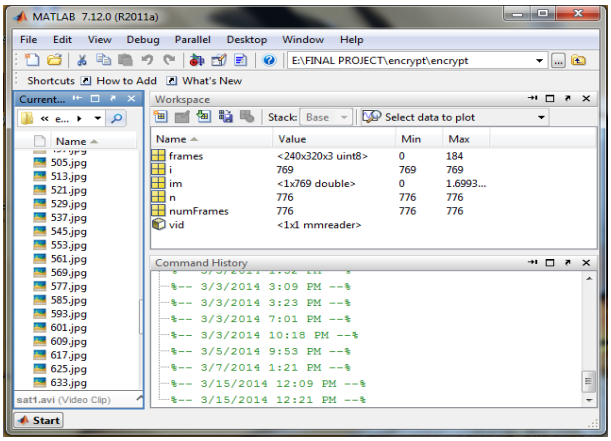

Fig:3 Conversion of video signal into images

The watermarked video does not include any variations as compared with the unwatermarked image. The simulated results show that the proposed method is simple, efficient and secure. In existing method they used the Diffusion and substitution method. That method is based on the spatial domain transformation.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

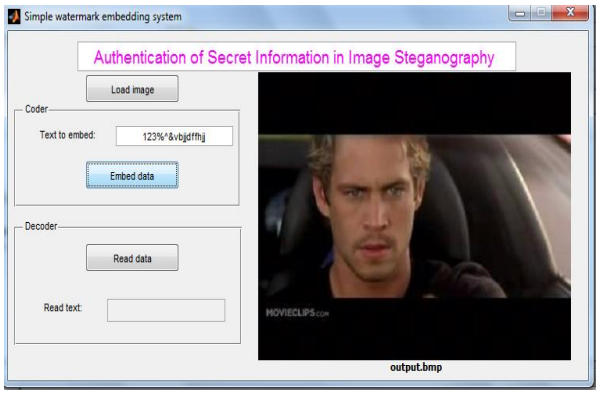

Fig 4: Watermaked Image

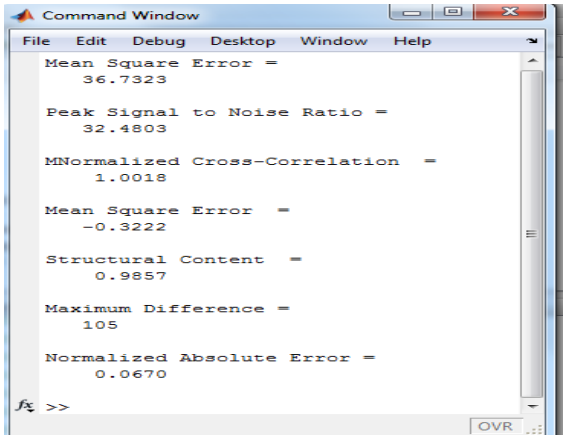

Fig 5: Parameter Analysis

Table 1: Comparison of different security parameters of video signal formats

Video format	Mean Square Error	PSNR (dB)	Normalized Cross-Correlation	Structural Content	Maximum Difference	Normalized Absolute
Avi	3.81	42.31	0.99	1.0	28	0.0258
Mkv	4.22	41.87	0.99	0.99	20	0.0218
mp4	4.25	41.84	0.99	1.0	20	0.0218
Mov	4.22	41.81	0.99	0.9	20	0.0218
Mpg	1.87	45.39	0.99	1.0	20	0.0256
Wmv	4.78	41.32	0.99	1.0	19	0.0222

VI. CONCLUSION

In proposed method frequency domain transformation is used. Haar Wavelet Transform has made the algorithm efficient and simple. On comparing different type of video formats MPG video format has a highest peak signal to noise ratio. On calculating various parameters such as MSE, Cross Correlation, Structural Content, etc, proves the proposed method is secured and simple when comparing to existing method. The future work of this method is that

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

the data is encrypted by using any one key and then watermarked into video. The error correction and detection technique can also be applied to reduce errors. The experimental results indicate that the proposed scheme is simple, efficient, has high order of security and good speed, thus the scheme can be used in real practice.

REFERENCES

[1] Narendra K.pareek, vinod patidar, krishan K.sud, "Diffusion-subtitution based gray image encryption scheme" Digital signal processing 894-901,2013.
[2] 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.
[3] Allam Mousa (1) and Ahmad Hamad, "Evaluvation of the RC4 algorithm for data encryption", International Journal of Computer Science & Application Vol. 3, No.2,44-56, June 2006.
[4] Ali B.Y.Mohammad, J.Aman,"Image encryption using block based transformation", IAENG.Int.J.Comput.Sci.15-23,2008.
[5] 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, July 2 - 4,2008.
[6] Guodong Ye," Image scrambling encryption algorithm of pixel bit based on chaos map",Pattern Recognit, Lett.31,pp.347-354,2011
[7] Jin-mei Liu, QiangQu,:cryptanalysis of a subtitutio-diffusion based image cipher using chaotic standard and logistic maps",Third International Symposium on Information Processing, ,pp.67-69, 2011.
[8] Hongxing Yao, Meng Li," An approach of image hiding and encryption based on a new hyperchaotic system:,Int. J. Nonlinear Sci.7,pp.379-38,2009..
[9] IsmetOzturk, Ibrahim Sogukpinar,"Analysis and comparison of image encryption algorithm", Trans. Eng. Comput. Technol.,pp.38-42,2009
[10] A.Syalim,T.Nishid, and K.Sakurai,"Preserving integrity and confidentiality of a directed acyclic graph model of provenance,"Proc. Working Conf. Data and Applications Security and Privacy,pp.311-318,2010.
[11] A.Mitre,Y.V.SubbaRao,S.R.M. Prasanna,"A New image encryption approachusing combinational permutation techniques, Int,J.Electr. Comput. Eng.,pp.127-131,2009.
[12]. G.Alvarez, Shujun Li,"Cryptanalyzing a nonlinear choastic algorithm(NCA) for image encryption", Commun. Nonlinear Sci. Numer. Simul.14,pp.3743-3749,2008.