International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

A Real Time Approach for Secure Text Transmission by using Video Cryptography

Rashmi Sharma
Electronics Comm. & Engineering,
Integral University, Lucknow, India
rashmi.cest@gmail.com

Saima Beg
Electronics Comm. & Engineering,
Integral University, Lucknow, India
saimabeg@iul.ac.in

Archana Yadav
Electronics Comm. & Engineering,
Integral University, Lucknow, India
archana@iul.ac.in

Abstract--Text, Image and video are the most basic forms of transmitting information. With the help of text and Image encryption methods, any particular set of words or images can be transmitted without worrying about security. With the help of pixel mapping algorithm, we can securely transmit the Image inside the frames of video which are the basic building blocks of any video file. In the proposed project the video is distributed into the photo frames using a Mat lab code and all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. Same way each image can be converted into red, green and blue layer. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. In the proposed work, top layer of each frames, get from video, are modified so as to insert single line of each layer from image. After the Completion of the pixel value modification. All the frames are cascaded for generation of the original video file with encryption. This new video is almost similar to the original video file with no changes visible to the naked eye.
In this paper, we will describe a digital image watermarking algorithm based on combining two transforms; DWT and DCT. Watermarking is done by altering the wavelets coefficients of carefully selected DWT sub-bands, followed by the application of the DCT transform on the selected sub-bands.

1. Introduction:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Cryptography is an art of protecting the information by transforming it into an unreadable and known as cipher key. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is the technique by which one can send and share the information like text, image, secret manner. Due the cryptography the information seems to be appearing like a garbage value and it is always almost impossible to find the information content lying under the image or a video file. The information looks like hidden inside the image or the video file. A very simplest and well known file does not visible of video and of it and overwrite it by Similarly also over write the blue layer of for green layer of impose one pixel into with consecutive different pixels of image 2, 4 or 8 bits. 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.

The development of effective digital image copyright protection methods have recently become an urgent and necessary requirement in the multimedia industry due to the ever-increasing unauthorized manipulation and reproduction of original digital objects. The new technology of digital watermarking has been advocated by many specialists as the best method to such multimedia copyright protection problem[1,2]. Its expected that digital watermarking will have a wide-span of practical applications such as digital cameras, medical imaging, image databases, and video-on-demand systems, among many others.

In order for a digital watermarking method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, scaling cropping, collusion attacks among many other digital signal processing operations. Current digital image watermarking techniques can be grouped into two major classes: spatial-domain and frequency-domain watermarking technique, compared to spatial domain techniques, frequency –domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms.

2. Literature Survey

The “Transmission of image using SMS Technique” helps to transfer the image from one mobile phone to another using the SMS technique. It provides a solution for the people who regularly use SMS for communication and want to use any image or reference about the picture to explain their view or points to another person who is far away, without the use of internet connection.

International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Stenography is the art of hiding information by embedding message within each other. It works by replacing the very useless bits by the information content to be transmitted. It works by hiding information inside a cover. The cover may be an image file or a video file as per the user requirement. Even though the cover looks very simple and unchanged but it has information contained in it. First of all, the video file in converted into sequence of frames of equal size. The information content which is to be transmitted by mapping onto the video file is distributed into small portion depending on the size of the frames in the video file. From each frame a smaller region is modified depending upon the private key. Due to this the selected groups looks very random to the third party who does not have the private key with them.

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. 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.

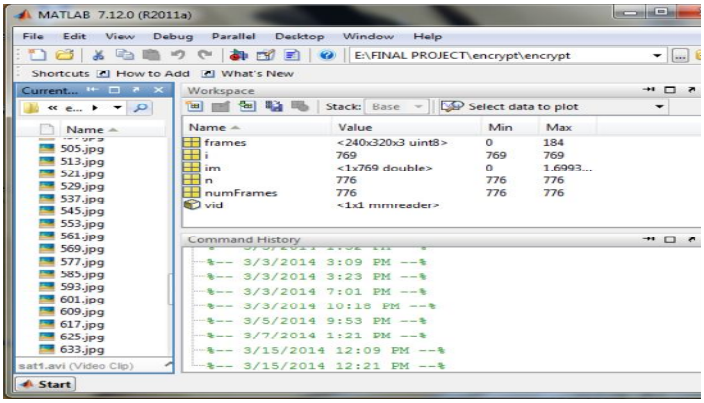

Fig. 1. Conversion of video signal into images

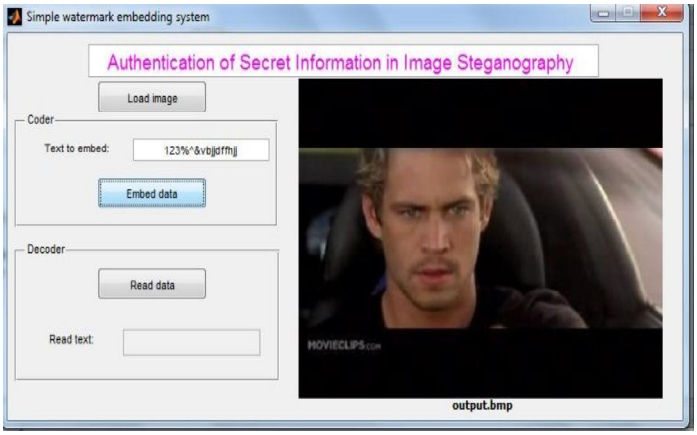

Fig. 2. Watermaked Image

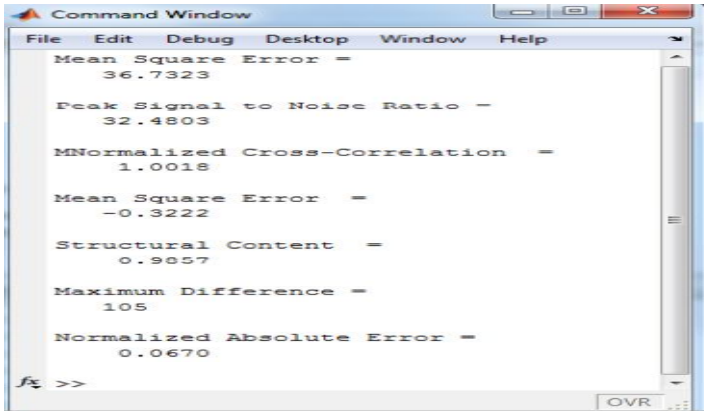

Fig. 3. Parameter Analysis

The future work of this method is that 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.

Visual Cryptography is used to hide information in images, a special encryption technique in such a way that encrypted image can be decrypted by the human eyes, if the correct key image is used. The technique was propose by Naor and Shamir in 1994[1]. It is uses two transparent images. One image contains image contains the secret information and the other random pixels.. It is not possible to get the secret information from any one of the images Both layers or transparent images are required to get the actual information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

3. Proposed Method:

The development of effective digital image copyright protection methods have recently become an urgent and necessary requirement in the multimedia industry due to the ever-increasing unauthorized manipulation and reproduction of original digital objects. The new technology of digital

watermarking has been advocated by many specialists as the best method to such multimedia copyright protection problem[1,2]. Its expected that digital watermarking will have a wide-span of practical applications such as digital cameras, medical imaging, image databases, and video-on-demand systems, among many others[3].

In order for a digital watermarking method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, scaling cropping, collusion attacks among many other digital signal processing operations.

The DCT And DWT Transforms

The DCT and DWT transforms have been extensively used in many digital signal processing applications. In this section, we introduce the two transforms briefly, and outline their relevance to the implementation of digital watermarking.

The DCT Transforms

The discrete cosine transforms is a technique for converting a signal into elementary frequency components [9]. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to Eq. 1 shown below. In the equation, x, is the input imagehaving N x M pixels, x(m,n) is the intensity of the pixel in row m and column n of the image, and y(u,v) is the DCT coefficient in row u and column v of the DCT matrix.

The DWT Transforms

Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWT-based watermarking algorithm, is to embed the watermark in the middle frequency ub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved.

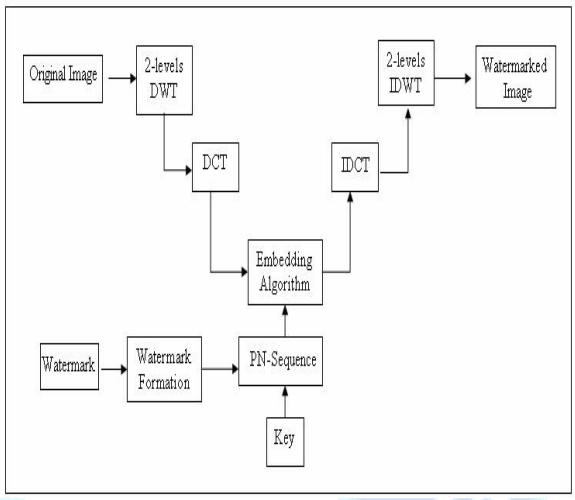

Fig. 4. Combined DWT-DCT watermark embedding procedure.

The Combined DCT-DWT Algorithm:

The watermark embedding procedure is depicted in Fig. 1 followed by a detailed explanation.

Step 1: Apply DWT to decompose the cover host image into four non-overlapping multi-resolution sub-bands: LL_1, HL_1, LH_1, and HH_1.

Step 2: Apply DWT again to sub-band HL_1 to get four smaller sub-bands and choose the HL_2 sub-band as shown in Fig. 2 a. Or, apply DWT to sub-band HH_1 to get four smaller sub-bands and choose the HH_2 sub-band as shown in Fig. 2 b.

Step 3: Divide the sub-band HL_2 (or HH_2) into 4 x 4 blocks.

Step 4: Apply DCT to each block in the chosen sub-band (HL_2 or HH_2) .

Step 5: Re-formulate the grey-scale watermark image into a vector of zeros and ones.

Step 6: Generate two uncorrelated pseudorandom sequences. One sequence is used to embed the watermark bit 0 (PN_0) and the other sequence is sued to embed the watermark bit 1 (PN_1). Number of elements in each of the two pseudorandom sequences must be equal to the number of mid-band elements of the DCT-transformed DWT sub-bands.

Step 7: Embed the two pseudorandom sequences, PN_0 and PN_1, with a gain factor , in the DCT transformed 4x4 blocks of the selected DWT sub-bands of the host image.

Embedding is not applied to all coefficients of the DCT block, but only to the mid-band DCT coefficients. If we donate $\boldsymbol{X}$ as the matrix of the mid-band coefficients of the DCT transformed block, then embedding is done as follows:

If the watermark bit is 0 then

$$X' = X + \ * PN\_0 \qquad (3)$$

otherwise,

if the watermark bit is 1 then,

$$X' = X + \ * PN\_1 \qquad (4)$$

Step 8: Apply inverse DCT (IDCT) to each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 9: Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the watermarked host image.

The watermark extraction procedure is depicted in Fig. 3, and described in details in the following steps. The combined DWT-DCT algorithm is a blind watermarking algorithm, and thus the original host image is not required to extract the watermark.

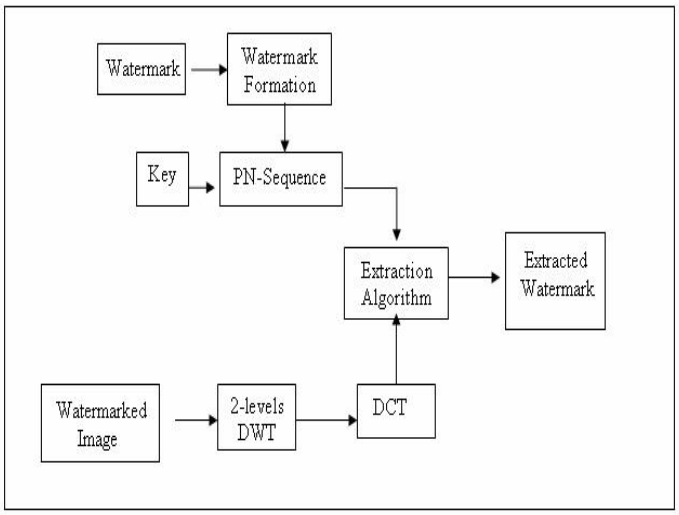

Fig. 5. Combined DWT-DCT watermark extraction procedure

The original host image not required to extract the watermark.

Step 1: Apply DWT decomposed the watermarked image into four non overlapping multi resolution sub bands LL_1 HL_1 LH_1 and HH_1.

Step 2: Apply DWT to HL_1 to get four smaller sub- bands, and choose the sub-band HL_2, as shown in Fig. 2 a. Or, apply DWT to the HH_1 sub-band to get four smaller sub-bands, and choose the HH_2 sub-band as shown in Fig. 2 b.

Step 3: Divide the sub-ban HL_2 Blocks.

Step 4: Apply DCT to each block in the chosen sub-band (HL_2 or HH_2), and extract the mid-band coefficients of each DCT transformed block.

Step 5: Regenerate the two pseudorandom sequences (PN_0 and PN_1) using the same seed used in the watermark embedding procedure.

Step 6: For each block in the sub-band HL_2 (or HH_2),

Step 7: Reconstruct the watermark using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

Performance Evaluation:

We evaluated the performance of the combined DWT DCT image watermarking algorithms using a 512□512 'Lena' as the original cover host image, and a 256□256 grey-scale image of the expression 'copyright' as the watermark image. The two images are shown in Fig. 4 and 5, respectively.

Performance Evaluation Metrics: Watermarking algorithms are usually evaluated with respect to two metrics: imperceptibility and robustness [21]. The two metrics are described below.

Imperceptibility: Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used.

Robustness: Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, internationally or unintentionally, by different types of digital signal processing attacks[22]. In this chapter we will report on robustness results which we obtained for three major digital signal processing operations attacks): Gaussian noise, image compression and image cropping.

4. Results and Discussion:

We described the performance of the combined DWT-DCT watermarking algorithm. For the sake of comparison, we also evaluated the watermarking performance when DWT-Only was used. The results we obtained for the DWT-Only approach indicated a better imperceptibility performance was obtained when the watermark was embedded in the HL_2 or HH_2 sub- bands. The robustness performance, however, was not acceptable. To improve performance, we combined DWT with the another equally powerful transform; the DCT. The combined DWT-DCT watermarking.

Fig. 5. Host image

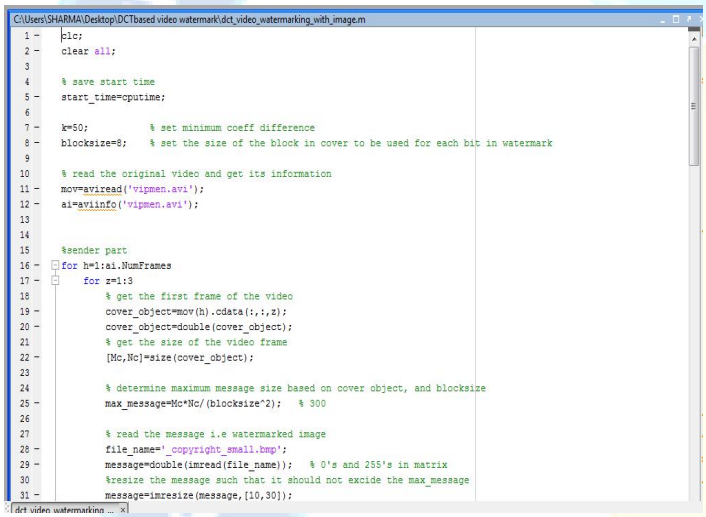

Fig. 6. Parameter Analysis

5. Conclusions

The discrete wavelet transform (DWT) and the discrete cosine transform (DCT) have been applied successfully in many in digital image watermarking. In this paper, we described a combined DWT-DCT digital image watermarking algorithm. Watermarking was done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improved the watermarking performance considerably when compared to the DWT-Only watermarking approach. In conclusion, in DWT-based digital watermarking applications, combining appropriate transforms with the DWT may have a positive impact on performance of the watermarking system.

References

[1] "A real time approach for secure text transmission using video cryptography" by Viral Metaliya,
[2] Deepak Jain and Raven Sardhara in conference on Communication Systems and Network Technologies (CSNT) ISBN 978-1-4799-3069-2.
[3] R. Schaphorst, "Videoconferencing and video telephony Adnan M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Trans. On Image Processing, vol. 13, no.8, Aug, 2004.
[4] Avcibas, N. Memon, and B. Sankur " Steganalysis using image quality metrics", IEEE Trans. IP, VOL. 12.
[5] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani hiding using cryptography and steganography" ISSN: 2277-1581 ternational ISSN: 2277-9477, Volume 4, Issue 2 Vithalani,"Dual layer data in IJSET volume 1, issue 4.
[6] 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.
[7] Allam Mousa (1) and Ahmad Hamad, "Evaluvation of the RC4 algorithm for data encryption", International Journal of Computer Science & Application Vol. 3.
[8] Marwa Abd El-Wahed, Saleh Mesbah, and Amen Shoukr,"Efficiency and Security of some image encryption algorithms", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008,London.
[9] Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.
[10] R.Asha & M.Raja babu, Discrete Wavelet Transform Based Steganography for Transmitting Images, IJMETMR.
[11] Jayanta Kumar Pal1, J. K. Mandal2 and Kousik Dasgupta3 in (IJNSA), Vol.2, No.4, October 2010.
[12] Sherif A. Mohamed and Moustafa M. Fahmy, "Binary image compression using efficient partitioning into rectangular regions" IEEE *Trans. on Comm.*, vol. 43, No. 5.