ISSN:0975-9646
Sana Ali et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (5) , 2016, 2376-2380

Prevention of Unauthorized Image Tempering and Secure Data Transmission using Integrated Stegowater Algorithm

Sana Ali[1], Yogendra Kumar Jain[2]

Research Scholar[1], Head Of Department[2]
Department of Computer Science and Engg.
Samrat Ashok Technological Institute,Vidisha, M.P., India, 464001

Abstract- Digital video and images are used in numerous applications these days. On the other hand, sophisticated procedures are required to assurance the reliability of an image or safeguard it against malicious alterations. Steganography is hiding text or secret messages into another media file such as image, text, sound and video. Watermarking is used to verify the identity and authenticity of the owner of a digital image. Discrete Cosine Transform (DCT) is extensively used in image processing, particularly for image and video compression procedure decoding and encoding. The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. DWT gives better compression ratio without losing more information of image but it need more processing power. Watermarking procedures are extensively used in the prevention of images against tampering. We proposed a new method using watermarking and steganography to improve the PSNR value. Our proposed method detected the image tempering and data can be transmitted securely over the channel. We used cryptographic steganography for secure data transmission and watermarking to prevent unauthenticated image
access. We applied Discrete Wavelet Transform technique to compress the image with better compression ratio. Our experimental result showed that method is well suited for unauthorized tempering detection.

***Keywords*- Steganography, Watermarking, Image Security, Self-recovery, Image tempering.**

I. INTRODUCTION

Due to the tremendous growth of Internet the web may produce huge information in digital form. The information may be in the form of numbers, strings, images, and video. The easy availability and increasing volume of multimedia data (video and image) in digital form has directed to a marvelous development of methods to manipulate data in digital multimedia form. Digital video and images are used in various applications. Meanwhile, the internet develops very fast and hence becomes an important medium for digital information communication. Though, being a fully open medium, the internet brought us not only convenience but also some threats and hazards. If the information to be communicated are trustworthy, it is appropriate as well for some mischievous users to illegitimately duplicate, destroy, or change them on the internet. As a result, information security [1] becomes an essential issue. Various schemes for data hiding are developed recently. Steganography [2], Cryptography and Watermarking [3] are three favorite techniques used for Internet security. To maintain multimedia data integrity and privacy many multimedia tools are available. These techniques ensures that image and video information are privacy prevented by image and video authentication techniques [1]. Traditionally privacy preservation of digital data related issues are solved by message authentication functions, cryptographic hash functions which are key reliant on and sensitive to each binary digit of the input message. The meaning of steganography is hiding text for security. In Steganography, Steganos and graphic are related to security in image or video. Stegano which means "message which is undisclosed or enclosed" and the graphic means hiding text i.e. "writing" (text) in image. However, in the security of information the meaning of Steganography is message hiding using text or private messages into additional multimedia file such as sound, image, text, and video. The different technologies in Steganography are algorithm for message hiding, private message to be send, the key used as secret value authentication and cover message. The cover message is the message used to carry the message or information such as text, audio, image, video or some other information present in digital form. The private message is the message or information which may be hide in the text, audio, image, video or some other information present in digital form. The secret key is mainly used for authentication purpose. This secret is inserted into the original message for security. This secret key is generated using some hiding procedure.

For security cryptography is the traditional method used in many applications. As cryptography [2] is the process of encrypting and decrypting the data. Here data gets encrypted which sender wants to send to the receiving party and decrypted on the other side. Watermarking is also an important technique for video and image processing. The owner of a digital image can insert a secure information into digital image. Watermarking is used to authenticate the uniqueness and validity of the holder of a digital image. These information could be either audios, videos or image. If malicious user attempts to copy the digital image, the watermark is also copied along with the image. Watermarking is further of two types robust and fragile. Watermarking procedures have been extensively useful to the area of image forensics. Image tempering protection is

also an example of image forensics. On the other hand, sophisticated techniques are required to guarantee the integrity of an image or protect it against malicious modifications

Image compression is mainly used for image data communication. The most widely used image compression techniques are DCT [5] (Discrete Cosine Transform) and DWT [6] (Discrete Wavelet Transform). DWT and DCT both procedures can convert digital image into frequency domain. Discrete Cosine Transform (DCT) is widely used in image processing and compression procedures for decoding and encoding of digital image. The main advantage of DCT is low processing power. The disadvantage of DCT is it loss some information. DWT is better than DCT and gives best compression proportion. DWT works without losing additional information of digital image. The disadvantage of DWT it required extra processing power. We proposed a new method using watermarking and steganography to improve the PSNR value. Our method detected the image tempering and data can be transmitted securely over the channel. We used cryptographic steganography for secure data transmission and watermarking to prevent unauthenticated image access. We applied Discrete Wavelet Transform technique to compress the image with better compression ratio and low processing power.

The rest of the paper is organized as follows: Section II concentrates on the literature survey. Section III provides the proposed steps and algorithm. Section IV provides the implementation and result analysis. Finally, Section V provides concluding remarks, future scope.

II. LITERATURE SURVEY

For image security, an algorithm proposed by Saeed Sarreshtedari embed a watermark into original image to protect it against tampering. It means that the watermark must be capable of both finding the tampered areas of the received image, and recovering the content of the original image in those zones. In this method most significant bits of each pixel remains unchanged, and use the remaining bits for the watermark embedding. For the purpose of image recovery, compress the image using a source encoding algorithm, and embed the result as watermark. However, some of compressed image information might be lost because of image tampering, hence the compressed image bit stream must be channel coded to exhibit robustness against a certain level of tampering. In order to detect tampered blocks at the receiver, some check bits are generated from those parts of image which remain unchanged during watermark embedding procedure. These check bits are inserted as a part of total watermark. As a result, the least significant bits (LSB) are comprised of both channel coded bits and check bits.

Having tampered blocks known using the check bits, tampering can be modeled as an erasure error. Therefore, compressed bit stream is channel coded using a code capable of resistance against certain level of erasure. At the receiver, the check bits locate tampered blocks. The list of tampered blocks identifies erasure locations and helps the channel erasure decoder to find the compressed image bit stream despite the occurring erasure. Then source encoded image would be decoded and the estimation of the original image is recovered.

Zhang *et. al.* propose an image self-embedding method based on DCT coefficients of the image [10]. The reference data in is generated by the least square quantization of the DCT coefficients [12]. This information is then channel coded with the rate λ and embedded as the watermark data. Therefore, the λ parameter determines the trade-off between the quality of the restored image and TTR for a certain embedding capacity. The higher λ values mean lower channel code protection and hence lower TTR [13]. However, in this case the embedding capacity is dedicated more to the reference data and the lost data will be recovered with a higher quality while the tampering rate is below TTR. On the other hand, the embedding capacity is rather dedicated to the channel coding parity bits than reference bits for smaller λ cases, in which the restoration is possible with low quality for the tampering rates up to higher TTRs. The maximum PSNR of recovered area is limited to 40.7 dB.

Rupesh Gupta proposed a new technique that will provide better security for hiding data in an image and watermarked video [2]. Author proposed an algorithm for transmitting the secret image over a network by combining the cryptography steganography and watermarking techniques. He applied 4 level and 5 level DWT techniques to image, later he select Y band to embed watermark and applied lower to lower, lower to higher, higher to higher and higher to lower band to the watermarked image. He combine both decryption and encryption algorithm. The resulting PSNR and MSE by applying this technique are 40.5 and 22 approx. respectively. The embedding capacity in values is 50.

Chen proposed a method to hide data in the coefficients of high frequency domain resulted from DWT, in which the low frequency coefficients are unaltered [8]. Some basic pre-processing steps are applied before embedding the data. Author divided the method in two modes and three cases. The modes are fixed and varying. The cases are low embedding capacity, medium capacity and high capacity. Sequence mapping tables are used in raster scan manner to embed the data. Extraction is just reverse of the embedding processing. Authors show the results in form of stego image, capacity and *PSNR* on six different images. For fix mode, 46.83 dB is the highest *PSNR* value and 39.00 dB is lowest *PSNR* value. For varying mod highest *PSNR* is 45.85 dB and lowest is 40.76 dB.

Kumar proposed Dual Transform Technique for Robust Steganography (DTTRS) [15]. The cover image is segmented into blocks of 4×4 size and DWT is applied on each block. In the resulting DWT coefficients, blocks of vertical band of 2×2 are considered and IWT is applied to get single coefficient. The IWT is applied on vertical band of DWT to generate coefficients of payload and then embedded into IWT coefficients of cover image using LSB method. On applying Inverse IWT and Inverse DWT, stego image is generated. The results are shown in form of stego image and PSNR (maximum 39.84 dB) and capacity (maximum 25%).

III. PROPOSED WORK

Proposed step

Step 1 Select image from database
Step 2 Apply DWT technique
Step 3 Watermark embedding
Step 4 Image compression algorithm
Step 5 Apply Steganography algorithm
Step 6 Image tempering detection
Step 7 Message decryption
Step 8 Image recovery

The first step in our algorithm is to select an image from image database.
The next step is to apply DWT technique to the image

Encoding System

DWT steps:

Step1. First original source image have to been Passed through high pass filter and low pass filter by applying filter on each row.
Step2. Output of the both image l1 and h1 are combine into t1= [l1 h1].
Step3. T1 is down sampled by 2.
Step4. Now, again T1 has been passed through high pass filter and low filter by applying on each column.
Step5. Output of the step4 is supposed l2 and h2. Then l2 and h2 is combine into t3= [l2 h2].
Step6. Now down sampled t3 by 2. This is our compressed image.

Decoding System.

Decoding system's steps:

Step1.Extract low pass filter image and high pass filter image from compressed image simply by taking upper half rectangle of matrix is low pass filter image and down half rectangle is high pass filter image
Step2. Both images are up sampled by 2.
Step3.Now we take the summation of both images into one image called r1.
Step4. Then again extract low pass filter image and high pass filter image by simply dividing vertically. First half is low pass filtered image and second half is high pass filter image.
Step5. Take summation of both images that is out reconstructed image.

The next step is to embed watermark into the source image.
Now image compression algorithm is applied to compress the image.
The next step is to apply steganography algorithm with message embedding into the image.
The next step is to detect any tempering in image.
The next step is to decrypt the desired message.
f any tempering is done in the original image then recovery operation is performed to recover original image.

IV. IMPLEMENTATION AND RESULT ANALYSIS

For implementation we have used core i3 3.0 GHz processor speed, 4GB RAM, 500 GB Hard disk. We have used MATLAB10 for implementation of proposed work. MATLAB is widely used programming environment for image processing.
The evaluation parameters used in proposed system is PSNR, embedding capacity, MSE.
PSNR (Peak Signal to Noise Ratio) is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

where MSE [7] (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. The mathematical definition for MSE is:

$$MSE = \left(\frac{1}{M \times N}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(a_{ij} - b_{ij}\right)^2$$

Embedding capacity represent the size of the data can be embedded into original image. The output results are shown below:

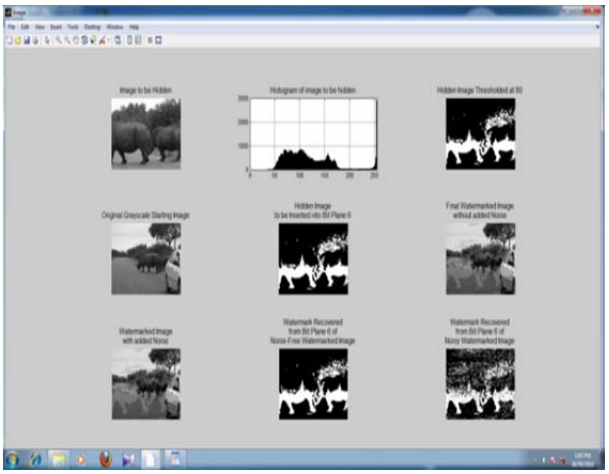

Figure.1 Dataset from rhino database

Figure 1 represents original gray scale image of 512x512 of rhino's video database after applying the DWT. The first part represents image to be hidden, original image, and watermarked image with and without noise. It represent the hidden image threshold at 80. It also represent histogram of the images.

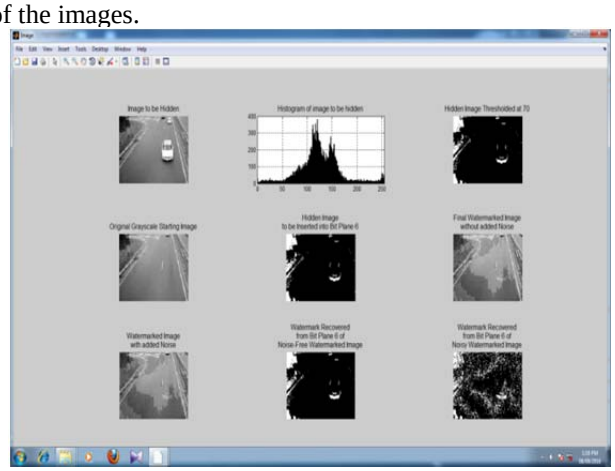

Figure.2 Dataset from car video database

Figure 2 represents original gray scale image of 512x512 of car video database after applying technique proposed in our paper. The first part represent image to be hidden, original image, and watermarked image with and without noise. It represent the hidden image threshold at 70. It also represent histogram of the images.

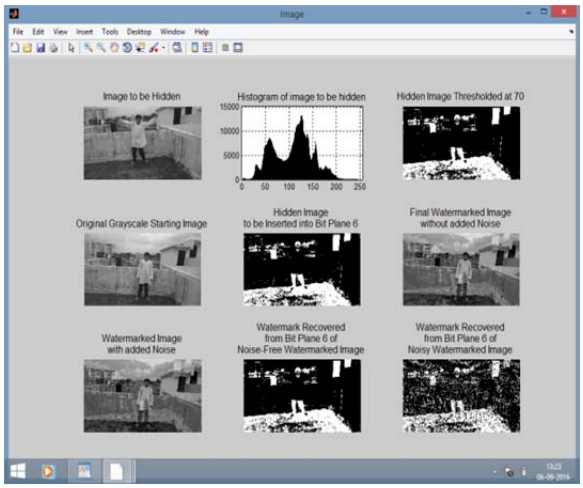

Figure.3 Dataset from dancing boy database

Figure 3 represents original gray scale image of 512x512 of dancing boy video database after applying DWT. The first part represents image to be hidden, original image, and watermarked image with and without noise. It also represent histogram of the images.

After executing our algorithm, we get following PSNR value:

Table. 1 Output results of PSNR Values

Results / Images	MSE	PSNR
Figure 1	11.7807	65.9482
Figure 2	15.7041	41.9752
Figure 3	13.8529	51.9481

Table 1 shows the PSNR value generated for different databases. The PSNR value generated by first database is 65.94, second database is 41.9752 and from third database is 51.94 respectively. Similarly the MSE values we got from different databases are 11.7808, 15.70, and 13.8529 respectively.

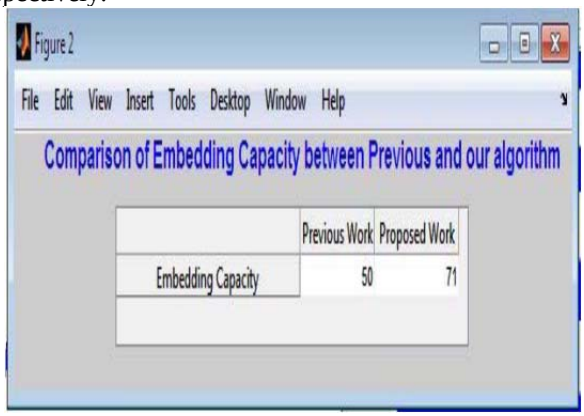

Figure.4 Embedding capacity result in values

Figure 4 shows the comparison of embedding capacity. From experimental results our embedding capacity is also improved to 71 while the embedding capacity of previous algorithm (SPIHT source coding algorithm) was 50.

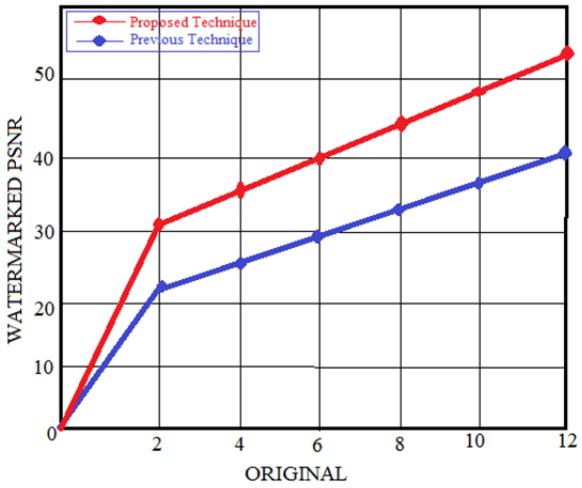

Figure. 5 Graph of PSNR after noise attack

Figure 5 shows parameter PSNR after the noise attack which compares our technique with the traditional one and producing better results. Our algorithm reaches upto 60dB as compared to previous algorithm which produces PSNR 40.16dB. It shows the better efficiency of our algorithm.

V. Conclusion

Security and robustness are two important requirements for digital image processing algorithms in applications involving authentication, watermarking, and image databases. Steganography means hiding text or secret messages into another media file such as image, text, sound and video. Watermarking procedures have been extensively used in the image and video forensics. We applied Discrete Wavelet Transform technique to compress the image with better compression ratio and low processing power. Our proposed method detected the image tempering and data can be transmitted securely over the channel. We used cryptographic steganography for secure data transmission and watermarking to prevent unauthenticated image access and to improve the PSNR value. Our method will improve the message hiding capacity, peak to signal ratio and mean square error. Our experimental result showed that method is well suited for unauthorized tempering detection.

In our future work we are planning to comprises new methods how to combine the suggested system with intra prediction and inter prediction, or together to further improve image/video HEVC coding performance.

References

[1] Saeed Sarreshtedari and Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery," IEEE transactions on image processing, vol. 24, no. 7, pp. 2266-2278, Jul. 2015.

[2] Rupesh Gupta anr Dr.TanuPreet Singh, "New Proposed Practice for Secure Image Combing Cryptography Stegnography and Watermarking based on Various Parameters," International

Conference on Contemporary Computing and Informatics (IC3I), pp. 270-280, 2014.

[3] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[4] M. Wu and B. Liu, "Watermarking for image authentication," in Proc. Int. Conf. Image Process. (ICIP), vol. 2, pp. 437–441, 1998.

[5] J. Fridrich, "Image watermarking for tamper detection," in Proc. Int. Conf. Image Process. (ICIP), vol. 2, pp. 404–408, Oct. 1998.

[6] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[7] M. U. Celik, G. Sharma, E. Saber and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," IEEE Trans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.

[8] Chen P. Y. and Lin H. J., "A *DWT* Approach for Image Steganography", International Journal of Applied Science and Engineering (*IJASE*), Vol. 4, No. 4, pp 275-290, 2006.

[9] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 10, pp. 1294–1300, Oct. 2006.

[10] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[11] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Comput. Sci. Softw. Eng., vol. 3, pp. 926–930, Dec. 2008.

[12] J. Lee and C. S. Won, "Authentication and correction of digital watermarking images," Electron. Lett., vol. 35, no. 11, pp. 886–887, 1999.

[13] R. Chamlawi, A. Khan, and I. Usman, "Authentication and recovery of images using multiple watermarks," Comput. Elect. Eng., vol. 36, no. 3, pp. 578–584, 2010.

[14] N. Wang and C.-H. Kim, "Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD," in Proc. 9th Int. Symp. Commun. Inf. Technol. (ISCIT), pp. 157–162, Sep. 2009.

[15] Kumar K. B. S., Khasim T., Raja K. B., Pattnaik S. and Chhotaray R. K. , "Dual Transform Technique for Robust Steganography", International Conference on Computational Intelligence and Communication Systems (*ICCICS*), IEEE Computer Society, pp 310-314, 2011.

[16] Nishtha Parashar, Nirupama Tiwari and Deepika dubey, "A Survey of Digital Image Tempering Techniques, "International Journal of Signal Processing,Image Processing and Pattern recoginition, vol. 2, no. 2, pp. 415-420, 2016.