Secure Communication Based on SVD and 3DWT (SVD3DWT) Watermarking

Ruchi Pachori, Amit Mishra (Asst. Prof)
VITS, Jabalpur

Abstract: **Watermarking is an approach to hide the data (image in our case) efficiently into any covering object (image in our case) and it should be done in such a manner that any intruder cannot interpret it by any means. As per IEEE standard stegno image cannot be interpreted easily by any intruder. The proposed method is been developed in such a way that our generated stegno image follows the same standard. So, the total SNR observed for any scenario where the data image and cover image has the ratio of 1:8 or less & more than 82.9. In the proposed work we have achieved minimum SNR is 85.93 for data image and cover image and it has ratio of 1:25 and maximum SNR is 98.3 data image and cover image and it has ration of 1:62 .It has a good result in terms of the ratio as compared with the previous work in the same area.**

Keywords: **Discrete Wave Transform, Discrete Cosine Transform, Watermarking, cryptography. Peak Signal to Noise Ratio (PSNR), MSE: Mean Square Error**

I-INTRODUCTION

Proposed work 3DWTS is a unique DWT based method for watermarking. The covering image is divided into four sub bands using transform technique of DWT up to three levels. As known that DWT is the process for finding the area in an image where binary bits of watermark image can be hidden and as the level increases it hides the bits deeper and it will be too tough to find out the bits of the watermark. In proposed work the SVD is been performed after three times DWT (3DWT) and it has been applied on blocks of 8x8. The SVD is useful for long distance communication because it hides the single bit information at 64 (8x8) different locations and if some pixels out of 64 get lost during the communication we can still extract the original bit. The use of SVD protects our watermark from different image attacks like rotation, compression, noise, fading etc. because of three-level DWT and it is followed by SVD, named as 3DWTS.

Actually, watermarking has recently emerged as leading technology to reslove above very important problems. All kind for data may be watermarked: audio, images, video, formatted text, 3D models, & model animation parameters. Digital multimedia data provides a robust & easy editing & modifying for data. Data may be delivered over computer networks with little to no errors & often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data may be copied without any loss in quality & content. This poses a big problem for protection for intellectual property rights for copyright owners. Watermarking is a solution to problem. It may be defined as embedding digital data, such as information about owner, recipient, & access level, without being detectable in host multimedia data. Watermarking relies on hiding covert message in unsuspected multimedia data & is generally used in secret communication between acknowledged parties. Watermarking is a procedure for encryption that hides data among bits for a cover file, such as a graphic or an audio file. Technique replaces unused or insignificant bits with secret data. Watermarking is not as robust to attacks since embedded data is vulnerable to destruction [5].

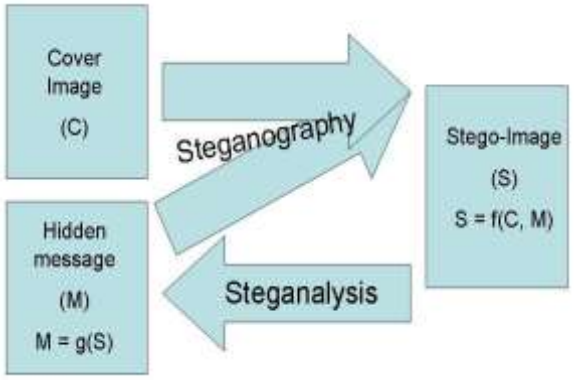

Figure 1 Data hiding scenario

In this age for universal electronic connectivity, for viruses & hackers, for electronic eavesdropping & electronic fraud, there is indeed no time at which security for information does not matter. Explosive growth for computer systems & their interconnections via networks has increased dependency on information stored & communication using these systems. This has led to a heightened awareness for need to protect data transmitted [5].

II-REVIEW for PRIOR WORK

After going through for all total 15 research papers, few articles, books & off-course Google on internet it has been observed that available work in related field in itself is good enough, however as we all know that nothing may be best so there are still possibilities for improvements in various parameters in watermarking.

As stenography depends upon data cover by any image, audio or video however after observing few results it is clearly seen that generally size for cover image is very large as compare to actual data which means if we want to secure data transfer using watermarking we will need to transmit much much data as compare to actual data. It is a big drawback with all available watermarking methods. Many much approaches has been applied to

data hiding in cover image or hiding data first then compress stenograph cover or compress data then stenograph it into cover. Many tried multilevel watermarking & combination & they have achieved good level for data hiding however still size for cover is around 70 to 200 times for size for actual data.

Rather to emphasize on securing much data communication proposed work aims to reduce size for cover so less data needs to be transmit; parameters on which proposed work will go through are MSE & SNR. All we need to improve SNR & reduce MSE. So this will be well recognized work while maintaining size for cover same for same or much SNR.

Krishna Rao Kakkirala et al	This technique extracts watermark without cover image & also proved that this procedure is robust against various signal & non signal processing attacks. They hide watermark in Image with BER for 0.29 in JPG images.
Tanmay Bhattacharya et al	Their approach may be applied for colour image because DWT is applicable for any digital signal, they observed PSNR for 27.3850
Belmeguenaï Aïssa et al	Their proposed algorithm may to resists additive noises, correlation found in cipher is images is 0.0975

Table 1 *various* literature base work

Problem Formulation: The major problems for secure data communication are as follow:-

- It is an overhead for communication system it necessary just to secure data however not necessary for data communication.
- In watermarking size for cover image must be very high than watermark image.
- We cannot use same algorithm for all type for cover image & watermark.

In watermarking time for hiding watermark should be low enough so it does not disturb communication.
We have developed an adaptive type watermarking & hiding data after DWT [12] & SVD[16] so that it makes our procedure adaptive.

III-DESIGN TECHNIQUE

SVD3DWT: It is a unique DWT based procedure for watermarking. Covering image is divided into four sub bands using transform technique DWT up to three levels. As known that DWT is method for finding area in image where binary bits for watermark image may be hidden & as level increases it hides bits deeper & it will be too tough to find out bits for watermark. In proposed work SVD is been performed after 3DWT & it has been applied on blocks for 8x8. SVD is useful for long distance communication because it hides single bit information at 64 (8x8) various locations & if few pixels out for 64 get lost during communication we may still extract original bit. use for SVD protect our watermark from various image attacks like rotation, compression, noise, fading etc. because we are using three level DWT & it is followed by SVD we name proposed work as 3DWTS. Figure 3.6 shown next is proposed procedure as explained below:-

Step 1: At first step image is been taken through MATLAB & then in MATLAB environment it gets converted into pixels form (integer numbers).

Step 2: For data hiding as it is an analytical approach we required to convert it into frequency cum time domain which is possible with proposed symlet-6 based Wavelet transform only. There are many transform techniques available so it was our decision to made up what we required time or frequency resolution if we choose ‘type1’ then very good frequency resolution & if we choose ‘type10’ then time resolution gets better so we have chosen ‘type6’ wavelet which gives an adequate time & frequency resolution. After 3 level for image decomposition LH, HL & HH components are taken because H component are less interpretable by human eye.

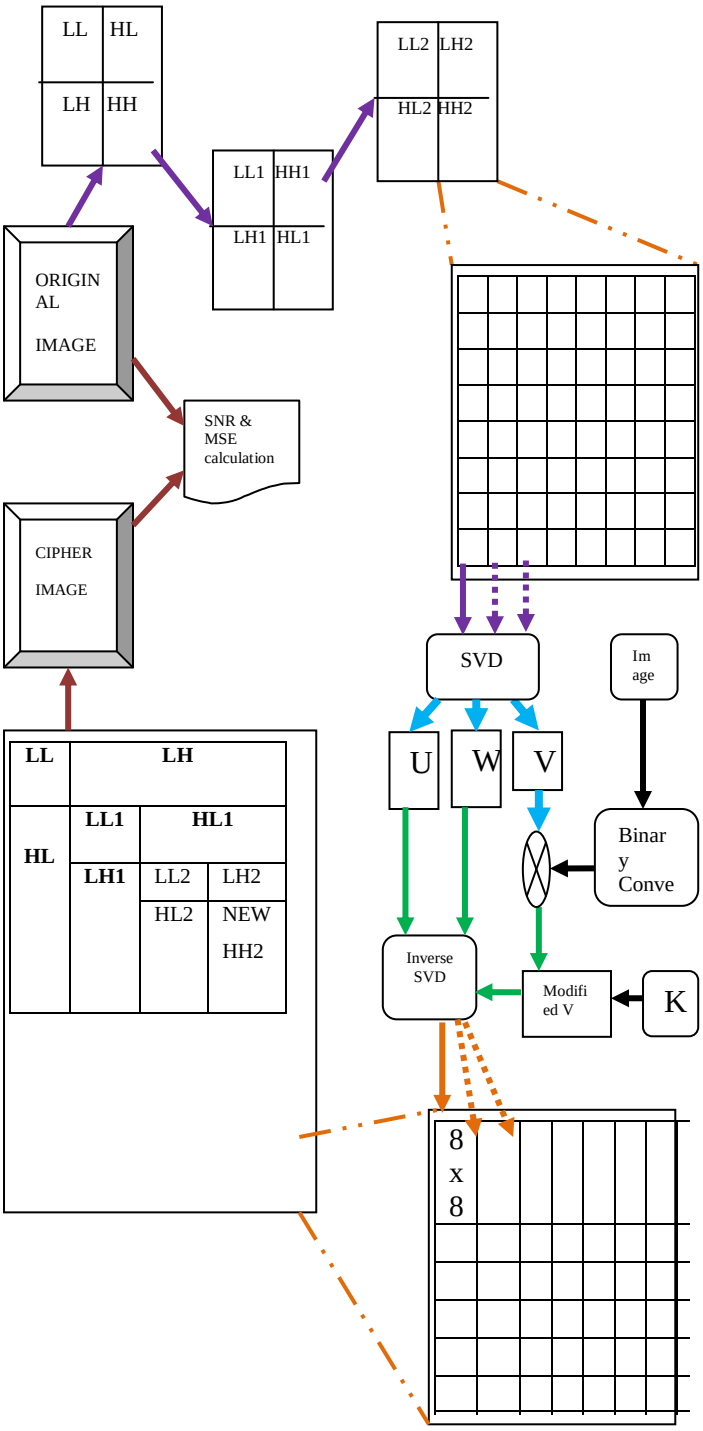

Figure 2 Proposed procedure SVD3DWT for watermarking

Step 3: After transforming for highest frequency elements HH2 is decomposed into blocks for 8x8 means 64 pixels as shown in figure 3.6.

Step 4: Each 8x8 block taken & SVD performed on all 8x8 blocks, SVD decompose each block into three individual blocks named U, V & W where V is Eigen value for respective block.

Step 5: data Image (watermark) taken & converted into binary 1D string this is required because we are hiding binary values for data image.

Step 6: LSB for 'V' for each 8x8 block with a single binary digit for watermark binary string & this method done until all binary digits does not get replaced with LSB for 'V', we may understand this method like for first 8x8 block after SVD we will hide first binary value into its 'V' then for next 8x8 block we will again perform SVD & now second binary will get hidden into new 'V' & so on. One interesting thing is that a single binary digit getting hidden inside 64 pixels for 'V'. This is major reason that our method is robust & less effected by noise & distortion during long distance communication.

Step 7: perform ISVD with modified V's an old U's & W's & also make a new HH2 frequency component concatenating all ISVD's

Step 8: Performing IDWT with new HH2 & old HL2, LL2 & LH2 & develop new HH1.

Step 9: Performing IDWT with new HH1 & old HL1, LL1 & LH1 & develop new HH.

Step 10: Performing IDWT with new HH & old HL, LL & LH & develop cipher Image.

Step 11: Computing MSE & SNR between Original Image & Cipher Image.

The deciphering is method for as may be observed it exact reverse order than ciphering method & our aim is to extract watermark not construct original image so we did method to have original data only.

IV-OBSERVED RESULTS

The proposed technique for hiding an image in other image has been tested with various size for images & it is been found working correctly. Figure 3 shown below shows two figures in figure-1 scenery is as cover image & ganesh image is been taken as watermark for hiding in proposed work. In figure-2 scenery is cipher image in which watermark is been hidden.

Table 2 observed results

Results Observed				
Data Image size	**Cover image size**	**MSE**	**SNR**	**BER**
8kb	200 kb	0.089	85.2	0.2134
14kb	200 kb	0.098	84.8	0.23
22 kb	200 kb	0.102	83.1	0.253
25kb	200 kb	0.154	82.9	0.258
8kb	500 kb	0.036	98.2	0.171
14kb	500 kb	0.051	97.3	0.178
22 kb	500 kb	0.067	96.9	0.182
25kb	500 kb	0.088	96.1	0.189

Figure 3 Cipher and Stegno image

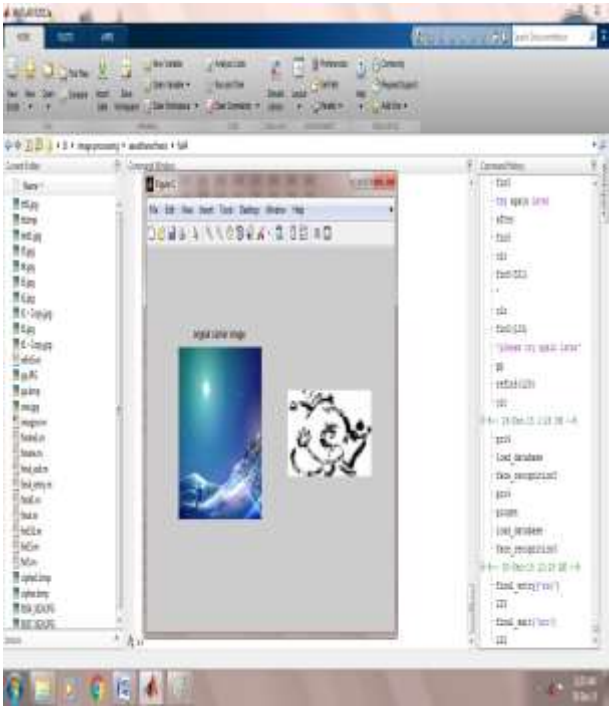

Figure 3 shown below is results observed for proposed approach & it may be easily observed that stegno image scenery (i.e cipher image) is as same
as original image & though it has complete watermark (i.e. image for a ganesh), it may be observed recovered watermark is similar to original watermark.

Figure 4 Watermark recovered from Cipher Image

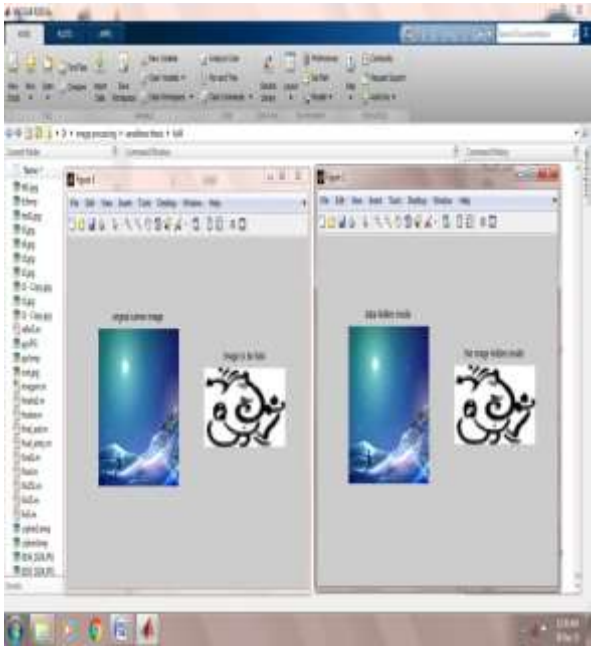

Figure 4.2*:* Results generated on MATLAB as Observed after developing stegno image

	BER	**SNR**	**MSE**
RBIW-DWT by Krishna Rao Kakkirala et al [1]	0.29	NA	NA
RDIW by Harsh K Verma [2]	NA	26.28	0.36
SBS-SOM by Nallagarla. Ramamurthy [3]	NA	51.8	0.43
RTS-DFT Bhalchandra D. Dhokale [4]	NA	45.91	N A
SVD3DWT	0.21	90.5	0.098

Table 3 Comparative results

Table 3 shows Mean square Error observed for various size for Data & cover image & it also shows Signal to Noise ratio (SNR) for various scenario, it may be easily seen that in observed results maximum SNR is 98.2 which is quite good however it gets reduces when size if covering image increases after deeply analysing results it may be said that results are good as we expected & it is very clearly hiding data image into covering –stegno-image.

V-CONCLUSION

The original objective for thesis work was to develop an optimised technique for hiding image & data inside cover image also to reduce amount for data on channel while stenograph data transmission which is been achieved. problem with watermarking is that it nessesory many for data means image for sending few small amount for data, so our work is a good solution for this problem we have achieved that few amount for data may be transmitted with small size for cover image hence needs to transmit less data as compare to all other existing techniques. We may confidently say that because we have achieved very good SNR for around 90.4 which is much better than old approach which was using watermarking without transforming.

Watermarking is an approach to hide data (image in our case) efficiently into any covering object (image in our case) & it should that in such a manner so any intruder cannot interpret it by any means , as from proposed procedure that is been achieved & one may say that our generated stegno image cannot be interpreted easily by any intruder, also total SNR observed for any scenario where data image & cover image has ratio for 1:8 or less is much than 82.9, & it is a good results for that ratio better than previous work on area.

REFERENCES

[1] Krishna Rao Kakkirala and Srinivasa Rao Chalamala, Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform, TCS Innovation Labs,TATA Consultancy Services, HiTec City, Madhapur, Hyderabad, India, 2014 IEEE 10th International Colloquium on Signal Processing & its Applications (CSPA2014), 7 - 9 Mac. 2014, Kuala Lumpur, Malaysia.

[2] Tanmay Bhattacharya , Nilanjan Dey and S. R. Bhadra Chaudhuri, A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum, International Journal of Modern Engineering Research (IJMER), Vol.1, Issue1, pp-157-161 ISSN: 2249-6645

[3] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed , Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function, 978-1-61284-383-4/11/2011 IEEE

[4] S. Sasidharan and R. Jithin, "selective encryption using DCT stream cypher " International Journal of Computer Science and Information Security, 2010.

[5] H. Jiang and C. Fu, "An image encryption scheme based on Lorenz chaos system," Natural computation, ICNC'08, vol. 4, pp. 600-604, 2008.

[6] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3998-4006, 2010.

[7] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "A new hyperchaotic system and its circuit implementation," Chaos, Solitons & Fractals, vol. 40, pp. 2544-2549, 2009.

[8] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, vol. 16, p. 2129, 2006.

[9] Iwata, M., Miyake, K., and Shiozaki, A. 2004. "Digital Watermarking Utilizing Features of JPEG Images", IEICE Transfusion Fundamentals, E87-A, 4:929-936.

[10] Po-Yueh Chen* and Hung-Ju Lin, "A DWT Based Approach for Image Watermarking", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[11] Wilson Wai Lun FUNG and Akiomi KUNISA," rotation, scaling, and translation-invariant multi-bit watermarking based on log-polar mapping and discrete fourier transform" 0-7803-9332-5/05 ©2005,IEEE.

