International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

An Improved Technique for Hiding Secret Image on Colour Images Using DWT, DCT, SVD

Amal Saroj[1], Dr. S Saira Banu[2]

[1] *MPhil. Scholar, Department of Electronics and Communication Systems, Karpagam Academy of Higher Education*
[2]*Associate Professor, Department of Electronics and Communication Systems, Karpagam Academy of Higher Education*

Abstract - *Information secret strategies have recently become important in many cases. Digital audio, video and images are increasingly different, but they have specific references that may contain a late copyright notice or serial number otherwise it will be unauthorized copies. Content of Multimedia will have been attacked and unauthorized reproduction of digital multimedia data by the hackers. To detect and protect copyright ownership, digital reservoirs have been built to respond to the growing demand for intellectual property protection. In our work the digital steganography algorithm is a hybrid scheme based on a Discrete Wavelet Transform (DWT), Discrete Cosine Transformation and (DCT) Singular Value Decomposition (SVD). The cover image is Wavelet decomposed to two levels and cosine transformed by one level. The Singular Value Decomposed message image is then cosine transformed and embedded with the cover image by replacing the least prominent datas.*

Key Words: Discrete Wavelet Transformations (DWT), Discrete Cosine Transformations (DCT), Singular Value Decompositions (SVD), Human Visual System (HVS), Peake Signal to Noise Ratio (PSNR), Diamond Encoding and Discrete Wavelet Transform (DE-DWT), XieBeni integrated Fuzzy C-means clustering (XFCM), Particle Swarm Optimization (PSO).

1. INTRODUCTION

Now a day's the digital data transmission over the wired and wireless channels are facing the big problem due to the illegal access of the data. Dedicated communication channels for each communication is impossible all time. Shared media or wireless communication channels are preferred for communicating digital multimedia data like images and videos to reduce the cost of communication. There arises the legal problem of piracy and copyright. In this case, for achieving the secrecy and authenticity, several cyphering methods are adopted like secret keying, watermarking, and steganography etc. steganographic technology can be applied for image, voice, video data. Here we are illustrating an improved method for hiding an image within an image without losing the data's and also explained the normalised correlation factor for the steganographic images with various resolution secret images.

In order to achieve security several steganographic schemes are applied in different studies. Multiple transformations are getting most effective than a single transformation. Steganography is not cryptography, but for secret privacy, then multiply data encrypted by stenographer. The goal is to create an image in the same way as a human eye but if necessary it gives its constructive recognition than the owner's key. Transform-domain technology combines cover image and secret images by controlling the size of transform-domains like DWT and DCT. More information and vulnerabilities can be changed against common attacks-Modified domain modes, but the cost of these procedures is higher in the Transform-domain steganographic system.

1.1 HVS and DWT

A powerful analogy that leads to the widely used technique – Human Visual System (HVS) images are Discrete Wavelet Transformations (DWT). Discrete Wavelet Transformations can be used as an effective version of Frequency models for HVS. DWT is a transformational strategy by interrupting the image at a new time and frequency band of Low frequency, medium and high frequency input image. The Filter selection depends on the type of signal analyzed. The following filters like Haar, Daubechies, Biorthogonal, Meyer, Morlet, Mexican Hat, Daubechies. Coiflets & Symlet can be used with Discrete Wavelet Transformation,

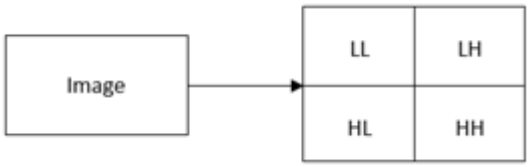

Fig- 1: DWT Transformation

1.2 Two-dimensional DWT

DWT method can be used for decomposition of input image to multi stage transform according to the frequency. For a two-dimensional image two-dimensional DWT transformation is used. The first level of DWT is composed of approximately equivalent length coefficient in column wise, and the second is made of raw wise with a down sampling of two, the third group combines vertical wavelet s coefficient, and fourth has diagonal coefficient.

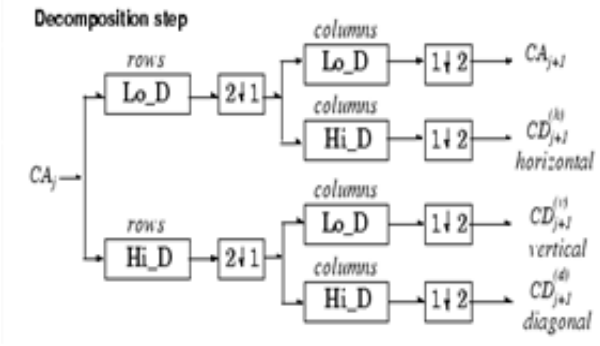

Fig- 2: DWT Decomposition

$$\psi_{s,\tau}(t)=\frac{1}{\sqrt{2^j}}\psi\left(\frac{t-k*2^j}{2^j}\right)$$

values of s and τ are $s = 2^j$, $\tau = k*2^j$

1.2 DCT and SVD

For Discrete Cosine Transformation the functions of the oscillation coefficient in various frequencies reveal a limited sequence of data points in total. Discrete Cosine Transformation works to highlight images within the areas of different frequencies. During the quantisation, the abstraction part is actually present lower mainstream frequencies, only the most important frequencies are preserved and retrieve to the original image. As a result, some of the reconstructed pictures have been distorted. When the compression level is adjusted, quality of image can be adjusted. But the human eye can only identify if the distortion reaches to a certain level.

$$F(u,v)=\left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}+\sum_{i=0}^{N-1}.\sum_{j=0}^{M-1}\Lambda(i).\Lambda(j).$$

$$.\cos\left[\frac{\pi.u}{2N}(2i+1)\right]\cos\left[\frac{\pi.u}{2M}(2j+1)\right]f(i,j)$$

P(x,y) is the x, yth element of the image represented by the matrix p. N represents the size of the block that the DCT is done. The equation calculates one entry (ith, jth) of the transformed image from pixel values of the original image matrix. For the standard 8X8 block the compression uses N=8 and x and y ranges from 0 t0 7. In the case of steganography DCT is very much helpful because the non-abstraction frequency region can be used for the insertion of stegano data.

Singular Value Decomposition is a method of changing variables basically a group that exposes different relationships on the original matrices. Also, we can say that, SVD is a method of detection. Sorting levels of the information points differ greatly. SVD identifies where most are variable and find it and optimal measurement of key data points using lower levels. So, SVD can be seen as a method for reducing data. According to Singular Value Decomposition, Let us consider an m x n matrix A converted to a factorised form where U will be a unitary matrix of the same size of A, is a rectangular diagonal matrix of same size. V is also having the size of A and it will be a unitary matrix. Here U (m n) and V (m n) are orthogonal matrices so that and where I is the identity matrix.

$$\Sigma \text{ is a diagonal matrix } \Sigma_{(1\,1)} \geq \Sigma_{(2\,2)} \geq \Sigma_{(3\,3)} \dots\dots\dots \Sigma_{(n\,n)}$$

2. LITERATURE SURVEY

The researchers incorporated various techniques for hiding secret image on a cover image. The most common technique for hiding data is the LSB substation algorithm which is a lossy steganographic technique. Another technologies like DWT, DCT, XCFM, SVD are applied for better quality image. In all algorithms the correlation between the secret image and the extracted images are tested with the normalized correlation factor for identifying the quality of the received image. Alexandru Isar1, et al [2] explained the statistical analysis of 2D DWT as well as 1D DWT in their probability density function and correlation factor for various datas. Samer Atawneh, et al [4][5] described the diamond encoding algorithm for steganography and DWT technique is used for better security. PSNR values are analysed for different images in DE system nd DE-DWT system.

T.Morkel, et al [6] explains the different steganographic techniques commonly used and the performance evaluation procedures for different schemes in their paper. Mashruha Raquib Mitashe, etal [1] XieBeni integrated Fuzzy C-means clustering (XFCM) technique is applied in this research work. Particle Swarm Optimization (PSO) is used for processing the images, before entering to the steganographic process. Discrete Wavelet Transform (DWT) is used for steganography. A correlation coefficient of 0.9934 is achieved in this work. Hadis Tarrah, Qazvin, et al [3], a combination of DWT and SVD is used for steganography. A PSNR value of 45 and Correlation value of 0.59 is achieved in this paper (PSNR > 30 gives high similarity). Anita Pradhan, et al [8], Sudha Rawat, et al [9], This paper deals with the image compression techniques and the comparison of different steganographic schemes and their performance evaluations.

Samer Atawneh Hussein Al Bazar et al. [10] Illustrates the new hybrid steganographic scheme using Diamond encoding and Discrete wavelet transform. The Distortion caused by DWT is eliminated by DE algorithm and it improves the security of the steganographic image. R. Shanthakumari and Dr.S. Malliga [11] proposed new method in LSB substation algorithm such that the substation of bits is with respect to the size of secret data. Preservation of smoother and sharp edges in the carrier data is maintained in this algorithm, hence, they get better quality image with a better PSNR value up to 80. Vijay Kumar & Dinesh Kumar [12] reduces the complexity while extracting secret image and improved the

security of steganographic image by adding key in the improved DWT algorithm. The researcher obtained a PSNR value of 49.08 and Similarity ratio of about 0.9918. Vivek Kapoor et al [13], Hemant Gupta et al Chaturvedi [14], Pooja Yadav, et al [15] explains different LSB substation methods for embedding secret data on to the video frames and analysed the performance parameters PSNR and Correlation factor. Rajkumar R and Saira Banu. S [16][17] explained in detail about the effect of noise in the quality of image and proposed an algorithm for removing noise.

3. PROPOSED ALGORITHM

In this research steganography is achieved using a hybrid steganographic scheme by applying DWT, DCT, SVD on cover image as well as secret image.

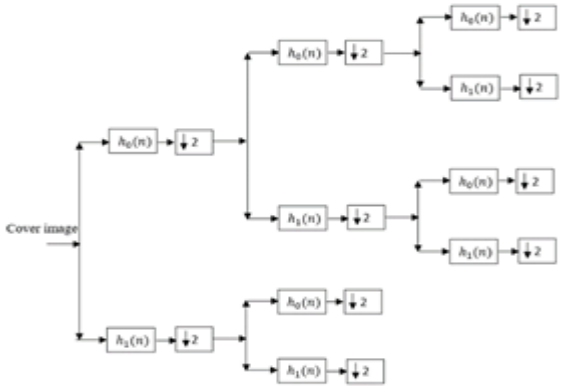

Fig- 3: DWT Tree algorithm

The cover image is DWT transformed and we get the coefficients LL, LH, HL, HH. The higher frequency part is separated and again it will undergo the DWT transformations. Then we will get the coefficients LL1, LH1, HL1, HH1. After this second transformation the highest frequency part is then cosine transformed using the DCT function. As a result of this pre-process the secret image of size one by quarter of the cover image is taken and it will split to three parts, two orthogonal unitary non-negative matrix U and V and a diagonal matrix Σ. All these matrices having the size same as the secret image. Discrete cosine transformations are applied to the decomposed secret image. Separate cosine transformations are done for the matrices U, V and Σ. Cosine transformed portion of the cover image and the secrete image are of same class and dimensions. Embeding secret image on the cover image is now easy because the image parts belongs to same class. High frequency part of the cover image is very less sensitive to the human eye, so that portion is replaced with the transformed secret image. All inverse transformations are applied to the cover image to make it viewable and it is transmitted over a distance. In decoding session, the highest frequency part of the steganographic image is separated using DWT tree and by applying cosine transformation the secret image parts filtered out. Inverse cosine transformations are applied to the filtered value, which are in the format of Singular value decomposed and the values are multiplied using the formula $A = U\Sigma V'$ and hence the secret image is reconstructed.

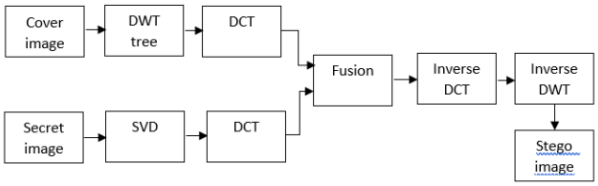

Fig -4: Proposed algorithm for Steganography

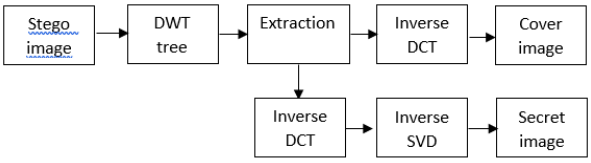

Fig -5: Proposed algorithm for Message Extraction

3. EXPERIMENTAL RESULTS

Cover1 Message1 Stegano img Recovered
Cover1=1024X1024
Message1=256X256
Correlation factor = 1.000

Cover1 Message2 Stegano img Recovered
Cover1=1024X1024
Message1=256X256
Correlation factor = 1.000

Cover2 Message3 Stegano img Recovered
Cover1=1024X1024
Message1=256X256
Correlation factor = 1.000

Cover1 Message1 Stegano img Recovered
Cover1=1024X1024
Message1=307X307
Correlation factor = 0.9991

Cover1 Message1 Stegano img Recovered
Cover1=1024X1024
Message1=205X205
Correlation factor = 0.9994

Table- 1: Correlation for different message length

Message length	Correlation
307	**0.9991**
256	**1.0000**
205	**0.9994**

Table- 2: Comparison of average correlation of Steganographic methods

Method	Average Correlation
LSB	0.7723
DWS	0.8408
DCWS	0.9124
PVD-MDR	0.9753
DWT	0.9804
DE-DWT	0.9887
EI-XOR	0.8988
DWT-SVD	0.9990
DWT-DCT-SVD	**0.9995**

3. CONCLUSIONS

This paper describes a method of hybrid steganographic scheme using the combination of DWT, DCT and SVD. The secret image is hiding inside the cover image by replacing the HH1, HL1, LH1 portions of the cover image decomposed by DWT tree transform. By using this method, the generated cover image having less distortion which is not identified by the human eye because the minute changes in the high frequency values are less identified by human eye. The performance is evaluated in the terms of normalized correlation coefficient. In this research work, different images with different resolutions are used for experiment. The important feature of this work is that the correlation coefficient for the secret image which is exactly one quarter of the cover image is 1.000. which indicates, at the time of extraction the data's of secret image is cent percent recovered when the secret image is 1/4th in size with respect to the cover image. In other cases, the correlation factor is less than unity and it is closely related to unity. The average value of correlation is also very closed to unity, indicates the better quality of the decoded image.

REFERENCES

[1] Mashruha Raquib Mitashe, Ahnaf Rafid Bin Habib, Anindita Razzaque, Ismat Ara Tanima, Jia Uddin "An Adaptive Digital Image Watermarking Schemewith PSO, DWT and XFCM", Department of Computer Science and Engineering BRAC University Dhaka, Bangladesh (2017).

[2] Alexandru Isar1, Sorin Moga2, and Xavier Lurton3 "A Statistical Analysis of the 2D Discrete Wavelet Transform"

[3] Hadis Tarrah Qazvin, Iran Sattar Mirzakuchaki," Performance Evaluation Parameters of Image Steganography Techniques", "A secure steganography scheme Efficient Steganography Scheme based on Logistic Map and DWT-SVD", Electrical Engineering Dept. Science & Research branch, Iran University of Science & Technology 2017

[4] Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain, Springer Science+Business Media New York 2016.

[5] Samer Atawneh, Hussein Al Bazar & Ammar Almomani & Putra Sumari & Brij Gupta' "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain", Received: 18 June 2016 / Revised: 5 August 2016 / Accepted: 1 September 2016.

[6] T.Morkel, J.H.P.Eloff, M.S.Oliver, "An overview of image steganography", ICSA Research group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa 2006.

[7] Proceedings of the International Conference on Data Engineering and Communication Technology ICDECT 2016, Volume 1, Advances in Intelligent Systems and Computing Volume 468.

[8] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain K. Raja Sekhar Department of Computer Science & Engineering, K L University Vaddeswaram-522502, Guntur, Andhra Pradesh, India (2016).

[9] 10. Sudha Rawat, Ajeet Kumar Verma "Survey paper on image compression techniques", M.tech Babasaheb bhimrao ambedkar university Department of Computer Science, Babasaheb bhimrao university, Lucknow, U.P 2017, IRJET,Impact Factor value: 5.181

[10] Samer Atawneh Hussein Al Bazar& Ammar Almomani & Putra Sumari & Brij Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain", Springer Science+Business Media New York 2016

[11] R. Shanthakumari and Dr.S. Malliga," Video Steganography using LSB matching revisited algorithm",

IOSR Journal of Computer Engineering, Volume 16, Issue 6, Ver. IV (Nov – Dec. 2014), PP 01-06

[12] Vijay Kumar & Dinesh Kumar Springer Science+Business Media, LLC 2017 A modified DWT-based image steganography technique.

[13] Vivek Kapoor and Akbar Mirza, "An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission", International Journal of Computer Applications (0975 – 8887) Volume 121 – No.10, July 2015

[14] Hemant Gupta and Dr. Setu Chaturvedi, "video steganography through LSB based hybrid approach", International Journal of Engineering Research and Development, Volume 6, Issue 12 (May 2013), PP. 32-42

[15] Pooja Yadav, Nischol Mishra and Sanjeev Sarma, "video steganography technique with encryption and LSB substitution", 2013, School Of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India.

[16] R. Rajkumar and S. Saira Banu. "Impulse Noise Removal using Enhanced Leading Diagonal Sorting Algorithm", August 2016 Indian Journal of Science and Technology, Vol 9(32).

Rajkumar R and Saira Banu. S, "Impulse Noise Removal Using Improved Leading Diagonal Sorting Algorithm", 2016 IEEE International Conference on Advances in Computer Applications (ICACA).