Digital Watermarking Technique using DWT, SVD, and AES

Shubham Godhar[1], Vyom Kulshreshtha[2]

[1]MTech Scholar, AKTU
[2]Professor, Sachdeva Institute of Technology

Publication Info

Article history:
Received : 23 February 2020
Accepted : 22 May 2020

Keywords:
Digital watermarking, Encryption, Decryption, Image, Textual, Cryptography

****Corresponding author:***
Shubham Godhar
e-mail: *godharshubham@gmail.com*

Abstract

As we are competing in advanced era, where the advancement and upgradation in technology takes place at every parameter (i.e. digitization, education) on daily basis. Such kind of use of internet involved in business environment, banking, hospitals etc seeking security, protection, concern towards illegal use of digital data. Internet is termed as the collection of various data in terms of audio, videos, images, text etc. Basically, while considering internet, the ownership identity needs to be protected. The suggested work will help in protecting the data from illegal use. In this manuscript we will present a technique named Water marking which will based on different algorithms like Singular Value Decomposition, Discrete Wavelet Transform & Advanced Encryption Standard. The term Watermarking is the way of securing data from copying, considering unauthorized access. The data availability can be either online or offline.

1. INTRODUCTION

Now a days, transfer of data done in an easy method. The data can be in any form like audio, video, images, text, animated pictures etc[1]. Just because of large way of communicating with each other through internet technology ,accessing to any zone, or part is easy. We all are the victims of E- Commerce business spreading at peak, where the customer makes payment online (done through Debit card, credit card, NEFT, RTGS, demand draft, online internet baking etc). When the customer is purchasing anything online and doing the payment, some minimum charges applied on the customer to make their complete by the bank. But, in one case the bank does not charge any amount while doing payment and that is Cheque payment. Whenever the payment done through cheque, no transaction charged by the bank for the clearance of the cheque. Doing the transferring process by CTS of home bank branch to cheque bank branch of clearing house, cheque can be cleared. As the transmission done through channel trough which we will send the image of cheque, may be the intruders having eyes on the channel carrying data. The attacker can apply any kind of attack to receive the details and data carried through channel [2, 3].

The applied attacks types are listed below.

- Gaussian noise attack
- Active attack
- Passive attack
- S & P buzz attack
- JPEG
- Rotation attack
- Filter attack

To overcome the issues created by the intruders or attackers, security and protection services is the required need to facilitate copyright [3].

Before the term Digital watermarking, the term Steganography was used to hide the critical text by using some other media. The term DWM is basically derived from the term Steganography, which is explained as the way of awning confidential text. A major difference between both the term is that digital water marking technique is restricting the unauthorized or illegal access of data, which in turn directly protecting the data from the intruders or attackers. In this method, the inserted watermark are not easy to remove and can be in any form. Water mark is just imperceptible which also cover the media too. Invisibility level is not defined in water marking technique. There are disadvantages too like

1.1. The quantity of data may be less if measured with the original data.

To overcome this, reversible water marking technique is

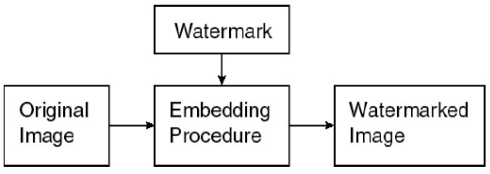

Figure 1: Imprecise form of water marking algorithm.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online) copyright © samriddhi,

applied to retrieve the original image. Reversible water marking technique is the way of cryptography.

2. TECHNIQUES USED IN PROPOSAL

2.1. DWT Transform: [4]

Discrete wavelet transform algorithm, picture is divided into four Parts.

- Horizonta
- Edge
- Upright
- Estimation part.

The isolation is done for changing into lower resolution goals picture. The method is repeated to figure out number scale wavelets declining. This strategy of water mark performs all calculations in all respects.

2.2. DCT Transform

In Discrete Cosine Transform, we install the watermark on picture with the help of utilizing numerous calculation, as this algorithm is very quick as contrast with different strategy[3]. While applying DCT, the watermark is implanted on the inside recurrence group on account of deterioration of picture

2.3. SVD

Singular value decomposition is one of the algorithm which is applied to calculate the matrices' in numerical ways.[5] Then in next step the matrices' will be transferred into various three sub matrix using the Singular valued decomposition concept. In this we will find that the size of both the matrices' are same either regenerated matrices' size will be as same as original, matrix size.

Example, An image is considered as an array of scalar quantities. Let P and squaring image, represented as P Ɛ Dnxn, locus D describes the domains real numbers,

In next step P's SVD will be P=USVT where U and V are orthogonal matrices, and A is a crossway matrix, as

$$S = \begin{bmatrix} s_1 & \square & \square \\ \square & \ddots & \square \\ \square & \square & s_n \end{bmatrix}$$

Here crossway components i.e. s's are one values and please S1≥ S2 ≥…. Sr ≥ Sr+1≥=……= Sn=0.

It is a capital grid decomposition technique in a least square sense that it packs the maximum signal energy into as few coefficients as possible.

3. LITERATURE REVIEW

In year 2008, Prof S. K. Bandyopadhyay, Debashis Ganguly, Swarnendu Mukherjee, Debnath Bhattacharyya, Poulami Das has proposed a heuristic way to deal with conceal tremendous measure of information utilizing LPB Steganography technique. The final stego-picture was contortion less. Additionally, they have given much accentuation on space multifaceted nature of the information concealing technique [15].

During the year 2008 a strategy chips away at more than one picture utilizing the idea of document hybridization presented by G Sahoo and R K Tiwari. This strategy executes cryptographic technique to implant two various data records utilizing Steganography and because of this reason they have utilized a stego key for the installing procedure [16]. Actually, the embedding of high-entropy information (regularly because of encryption) changes the histogram of shading frequencies in an anticipated manner. Along these lines, so as to get greater security in our recommended technique, we have inserted a whole picture over another picture of double the size of target picture for the surprising change in the previous picture.

During this paper, another technique for sorting watermark procedure through picture displaying is examined by Neil F. Johnson, Sushil Jajodia and Zoran Duric. [18] The picture displaying called _alpha channel syntheses utilizes steady veil. Two pictures with level cover and slow veil are utilized to make watermark which changes dim estimations of that exact pixel in the image. The technique for watermark recuperation by applying converse change to contorted pictures is appeared. The Image is watermarked utilizing the variant of Digimarc's Image Mark watermarking channel that is accessible with Adobe Photoshop and the image is contorted by using the Starmark instrument of relative change.

During this Paper, estimation for installing watermarking is displayed by utilizing DWT and encoded with QR codes by Vinita Gupta, Atul Barve(2014). [19]. at this point spread image is chosen and DWT is attached on it. A key X is selected to produce the QR code as mystery key. QR code and watermark picture is scrambled with the help of XOR task. At that moment the scrambled watermark is inserted into the spread image and backwards DWT is attached on the implanted watermark image. In support of extraction, essentially use the DWT on the spread image. This estimation is very basic in view of the utilization of straightforward X-OR task for encoding. This estimation is appropriate on various sort of Incursion on watermarked images like JPEG Compression, PNA, Salt and PN and GN.

4. PROBLEM STATEMENT

Number of algorithms like Single Value Decomposition, Discrete Wavelet Transform, and Discrete Encryption Standard etc will be used in our dissertation work for the digital water marking scheme. Every algorithm has its positive impact in this implementation field. If we discuss Advanced Encryption Standard Algorithm, this

copyright © samriddhi, 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

algorithm basically used to encode the data which is being transferred over the internet. It is one of the quality chunk coded method. If we do compare this algorithm with Data Encryption Standard, we will see AES is more methodical then DES. The term Chunk Code is used to explain that the method works over the insert code dimension and outcome the produced chunk of similar dimension. We do use insert clue in ASE. In the ASE algorithm the phase of choosing of functioning way is about the choice of particular execution. The dimension of insert chunk is 128 bits.

5. SUGGESTED WORK

In the discussed work, for the purpose of watermarking DWT [19], DCT [20] and SVD [21] is being used for the embedding process and for the AES [22] is also being used along with the other discussed techniques for the purpose of the extraction of the target image. DWT is being considered as one of the powerful and one of the most efficient tools of the watermarking process and for increasing the performance of the complete process DCT and SVD which results as the hybrid watermarking technique. The encryption technique is being for increasing the security level of the data and of the parameters as well.

In the suggested methodology AES (Advanced Encryption Standard Algorithm) is being used for encoding of the image which is to be transmitted using few digital averages. AES is based on grade block chipper concept means, in the technique the dimension of the input block is pre-defined and also the size of the output will always be equal to that of the input. In the AES technique the input clue is provided as input to the algorithm. The mode of operation actually defines the selection of the implementation of the AES technique. The size of input block which actually is pre-decided is considered of size 128 bits.

A DWM methodology is termed as escalate-spectrum only when noticeable wave prevails by advanced upgradation. The disadvantage with spread spectrum is that it has less facts volume due to monitor intervention. On the other side it is bashfully strong.

If the noticeable waves are obtained in quantity, then the digital water marking technique is called quantitative type. There is one issue with quantitative water mark that they tolerate less strength if noticeable wave prevails by advanced upgradation which is alike spread spectrum method but in a limited inserted in the dimensional domain.

5.1. Inserting Process

- *Move 1:* Image A and image B are opted as input image and target image (input image A as image used for hiding) and (target image B which is to be hided),
- *Move 2:* On the image B and cover image A separately, Single level DWT is being applied
- *Move3:* Over the B image and A image, DCT will be

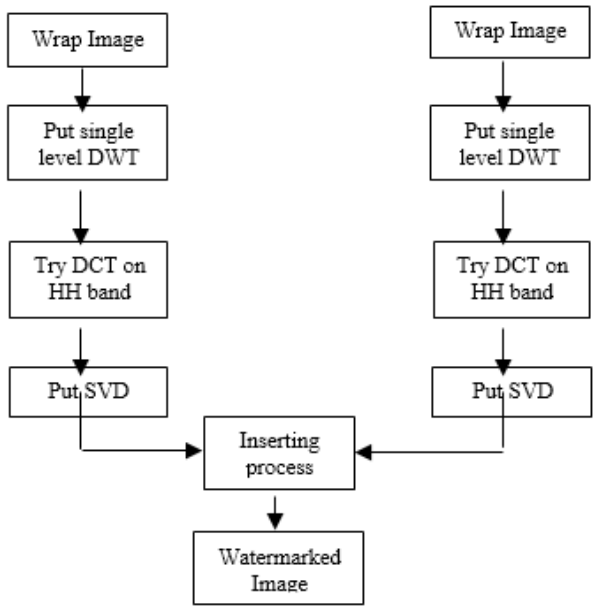

Figure 2: Embedding Process.

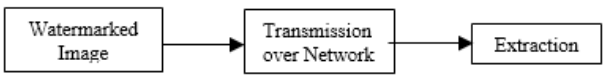

Figure 3: Transmission Phase.

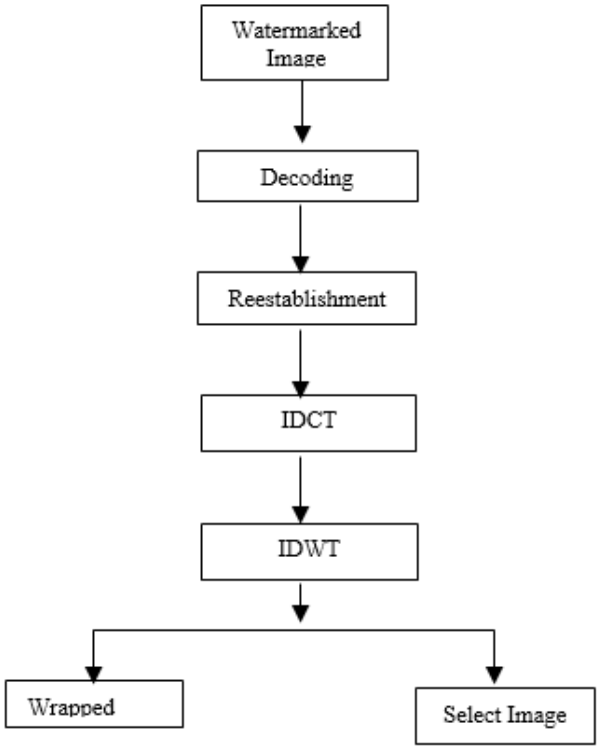

Figure 4: Extraction Process.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online) copyright © samriddhi,

implement over the HH band generated by Discrete Wavelet Transform.

- *Move 4:* SVD is applied On the DCT images which is generated from DWT, over A images and B images.
- *Move 5:* For better security and authentication the SVD images are embedded , AES methodology is being used for further encryption,
- *Move 6:* The output of the embedded method is the apex picture which is concealed inner the A image and the same is being coded by AES method,

5.2. Removal Process

- *Move7:* ***In*** removal process, watermarked image is considered as input to the process.
- *Move 8:* To receive the inserted picture , decryption method should be done, using the AES algorithm,
- *Move 9:* For both cover and target image, separate process of SVD picture is renovate.
- *Move 10:* Inverse Discrete Cosine transform is applied to get the DCT image A and image B.
- *Step 11:* Similarly, IDWT (Inverse Discrete Wavelet Transform is applied to get the cover image and target images)

6. OUTCOMES AND EXPLORATION

Using MATLAB 2015a at Intel dual core processor CPU 1.6 GHz PC with 4 GB of RAM the proposed is implemented.

We tried to find out all the recapture applicable particulars by measuring MSE, PSNR, computational fluids, safety, and certainty. The investigational outputs of subsists approaches are shown in the form of table.

The outcomes are described by searching out all the retrieved relevant information by estimating the MSE, PSNR, safety, hangings, fluids, effectiveness etc. The experimental outcomes of subsists proposals based on other perspective and proposed approach are depicted in the form of chart. Finally, the findings of the all experimented system will be discussed and analyzed.

Number of domains maintained while testing the proposed approach with the help of dataset:

- A set of target images
- A set cover image

Many parameters are used for the assessing of results with the help of calculation of the relevancy of proposed approach. These parameters are:

- Mean Square Error
- PSNR
- Effective
- Communication fluids
- Hanging
- Dimension of Key
- Split of Data
- Protection.

As the table is prepared for comparing the work parameters of proposed work which clearly shows that all the three parameters 1? Security of data to efficient use of data and 3. Integrity of data is increased. If we compare the value of security with the existing approach, we will find the value is greater. Computational fluid might be increase.

The snapshots in stepwise manner are shown below:

Table 1: Quantitative Outcome Examination

Image	*MSE*	*PSNR*
RTU logo	0	264.91
Thumps up	222.96	23.48
Patent	0	265.64

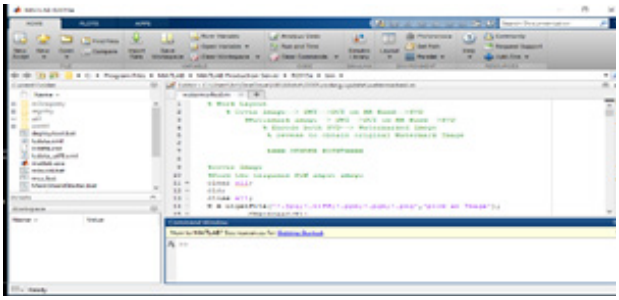

Figure 5: Snapshot 1

Table 2: Parameters Analogy Between Subsists Work & Suggested Work.

Variable	*Subsist Work(s)*	*Suggested Work*
Competence	Ordinary	Immense
Computational overhead or computational fluid	Median	Median (But compare to existing it raises because of hybrid and encryption steps)
Communication overhead or hanging	Equal	identical (no change at transmission channel)
Dimension of key	Depend on the approach (Nil, Average, High)	Median (encoding technique)
Certainty	Median	Enormous
Sharing of data	Authorize	Permit

copyright © samriddhi,

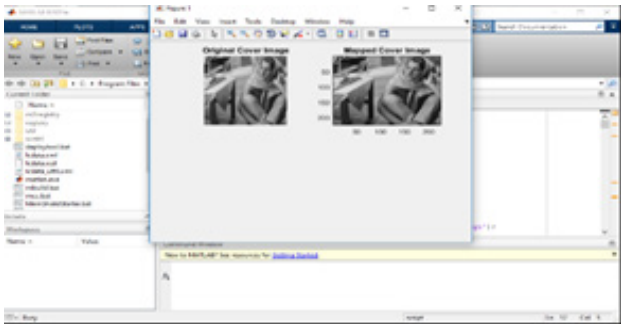

Figure 6: Snapshot 2

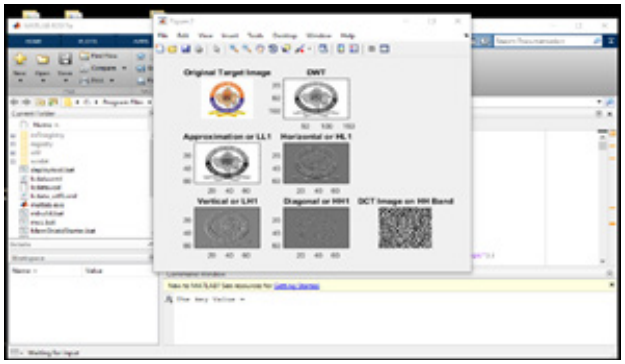

Figure 7: Snapshot 3

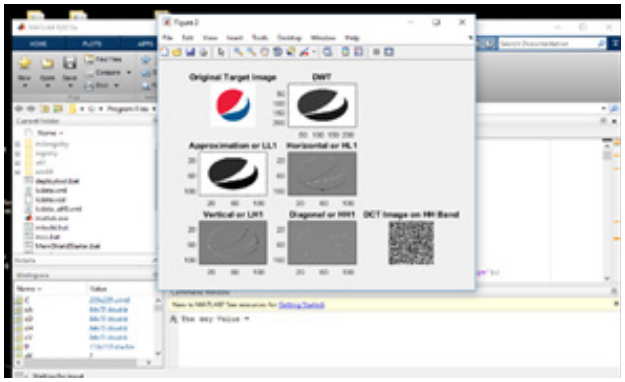

Figure 8: Snapshot 4

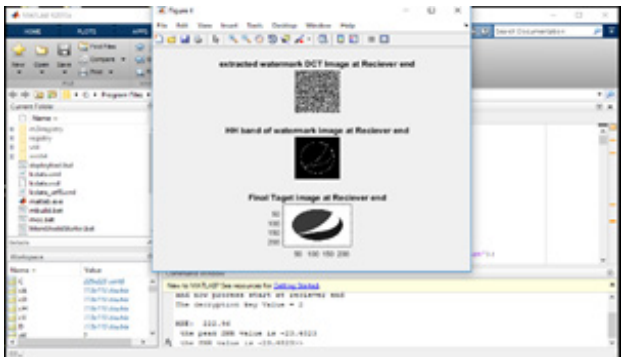

Figure 9: Snapshot 5

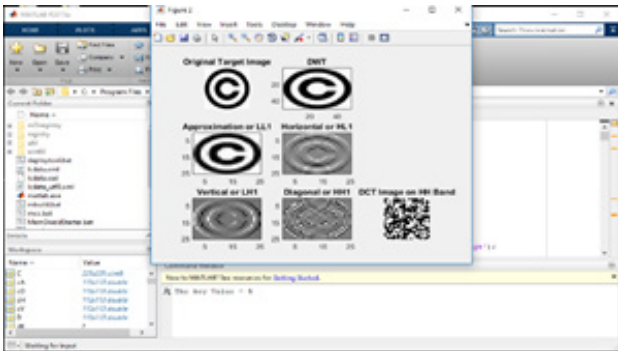

Figure 10: Snapshot 6

Figure 11: Snapshot 7

7. CONCLUSION

Structures like Singular Valued Decomposition, DCT, and DWT are used in the proposed report. In form of hybrid water marking us use method named Singular Valued Decomposition and for maintaining the security we used ASE.

SVD is an algorithm which is basically a water marking technique and encryption technique that focuses on security and protection of data while performing the transmission process.

AES i.e. Advanced Encryption Standard is used to encrypt the data or image. While comparing the Advanced Encryption Standard with Data Encryption Standard, AES is stronger block encrypting algorithm. Discrete Wavelet Transform is one of the most powerful and impactful algorithms which we used in this work. While keeping in mind, the increase the performance of water marking method we use Discrete Cosine Transform. Whatever model is prepared can be further studies to prepare toolbar, which comprises of all security and protection methods and also for valid users. So that in future, number of unauthorized users will be less and computational overhead would be minimum.

8. REFERENCES

[1] P. Karthigaikumar, Soumiya Rasheed, "Simulation of Image Encryption using AES Algorithm", *IJCA Special Issue on Computational Science - New Dimensions & Perspectives*

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online) copyright © samriddhi,

NCCSE, 2011, pp.166-172.

[2] Samir Kumar Bandyopadhyay, TuhinUtsab Paul and AvishekRaychoudhury, "Invisible Digital Watermarking through Encryption", *International Journal of Computer Applications (0975 – 8887)*, Vol. 4, No.8, August 2010, pp.18-20.

[3] Navas K. A., Ajay Mathews Cheriyan, Lakshmi. M, Archana Tampy. S, and Sasikumar M, "DWT-DCT-SVD Based Watermarking", *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops*, pp. 271-274, 2008.

[4] F. Huang and ZH. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR", *Pattern Recognition Letters*, vol.25, pp.1769-1775, 2004

[5] Radouane, M., "Robust method of digital image watermarking using SVD transform on DWT coefficients with optimal block", April 2014.

[6] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankarbabu, "Image Encryption Based on AES Key Expansion", *2011 Second International Conference on Emerging Applications of Information Technology,* IEEE, 2011, pp.217- 220.

[7] V. Amutha, C.T. Vijay Nagaraj, "A Secured Joint Encrypted Watermarking In Medical Image Using Block Cipher Algorithm", *International Journal of Innovative Research in Science*, Engineering and Technology Volume 3, Special Issue 3, March 2014, pp. 1099-1104.

[8] Mohammad Ibrahim Khan, Md. Maklachur Rahmanand Md. Iqbal Hasan Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation", *Department of Computer Science and Engineering, Chittagong University of Engineering and Technology Chittagong*-4349, Bangladesh.

[9] P. Parashar, "A Survey: Watermarking Techniques", 2014.

[10] V. Gupta, "A Review on Image Watermarking and Its. Techniques", *IJMEIT*, Vol. 2, Issue 1, January 2014.

[11] P. Rahmati, A. Adler, and T. Tran, "Watermarking in E-commerce", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 6, 2013.

AUTHORS

Shubham Godhar, Have done my schooling from Ramanlal Shorawala Public School, Mathura. Thereafter, I went to GLNA, Mathura (Affiliated to UPTU, Lucknow) for doing my B.Tech in Computer Science and completed it in 2014. In 2015 I enrolled in M.tech from SIT, Agra (Affiliated to UPTU, Lucknow) and left the course in middle because of some personal issues. Now, I am committed to complete my M.tech.

Vyom Kulshreshtha, Have Twelve years of experience in Industry and academics. Presently working as Assistant Professor in Department of Computer Science at Sachdeva Institute of Technology, Mathura, Uttar Pradesh. Have published 10 research papers in International Journals, and 5 research papers in National conferences. Key research field are Digital Image Processing, Distributed Systems, Soft computing Techniques and Artificial Intelligence.

copyright © samriddhi, 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)