

## International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

*IJCSMC, Vol. 4, Issue. 5, May 2015, pg.1002 – 1011*

### **RESEARCH ARTICLE**



# **INTEGRATED DCT, DWT AND MODIFIED SVD BASED DIGITAL IMAGE WATERMARKING**

**Ramandeep Kaur, Prof. Jatinder Kumar**

Dept. of Computer Science and Engineering, SIET, Amritsar, (Punjab) India  
rkramankang@gmail.com, jkteji@gmail.com

*Abstract:-Watermarking is an effective technology that solves many problems within a digitization. By embedding Intellectual Property data (e.g. the creator, licence model, creation date or other copyright information) within the digital object, the digitiser can demonstrate they are the creator and disseminate this information with every copy, even when the digital object has been uploaded to a third party site. It can also be used to determine if a work has been tampered with or copied. This paper describes methods for establishing if an application requires watermarking techniques and criteria for choosing the most suitable type. This paper has focused on evaluating the role of the SVD, DCT and DWT based image watermarking for secure transmission. And also enhancement is done by using the modified SVD to enhance the results further.*

*Index Terms: DCT, DWT, MODIFIED SVD, WATERMARKING.*

## **1. INTRODUCTION**

The advancing world of digital multimedia communication is faces problems related to security and authenticity of digital data. A click on the computer can send digital data from one network to a different network. Millions of digital data cross network every day. Copyright protection is a way to give authentication of digital data, which can be a severe issue in today's digital world. Copyright protection of digital data is an important legal issue [2, 3]. Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Watermarking technology protects ownership of multimedia data. A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties [6].

Watermarking tries to hide a message related to the actual content of the digital signal, but in steganography the digital signal has no relation to the message and it is merely used as a cover to hide its existence. Watermarking is used for providing a kind of security for various type of data (it may be image, audio, video, etc.). Watermarking is the process of embedding a message on a host signal. Watermarking, as different to steganography, has the extra requirement of robustness against possible attacks [12].

Digital watermarking schemes can be categorized as “visible” and “invisible” watermarking. The visible watermarks are easily identified like different logos either on paper or on a TV screen. They are usually not robust against common image processing operation. The invisible watermarks are more secure and robust than visible watermarks. In invisible watermarking, the watermarked image should look similar to the original image [11]. An invisible watermark can be either robust or fragile.

Watermarking algorithms can be classified on several criteria are, according to domain of watermark insertion like watermarks can be embedded in the pixel/spatial domain or a transform domain [9]. Second is according to visibility of watermark (visible and invisible) and according to watermark detection and extraction which contain blind and non blind techniques.

## 2. PROPOSED ALGORITHM

**How Integrated DCT, DWT and modified SVD works:** The insertion process is divided into following steps and is briefly described as given below

### 2.1 Watermark Insertion Process:

**Step 1:** Let CI be the Cover image of size  $N \times N$ . Select color channel and apply DWT to decompose it into; four  $N/2 \times N/2$  sub-bands LL, HL, LH and HH.

**Step 2:** Evaluate LL band and then DWT will come in action to decompose DWT coefficients into four  $N/4 \times N/4$  sub bands LL\_LL, LL\_HL, LL\_LH and LL\_HH.

**Step 3:** Evaluate LL\_HH band, and divide it into 484 square blocks and apply DCT on them, select first DCT coefficient of each block and get DCT coefficient matrix B.

**Step 4:** Apply modified SVD to B,  $B=U1*S1*V1T$ , and acquire U1, S1 and V1.

**Step 5:** Let OW of size  $N/16 \times N/16$  to represent watermark. Apply SVD to it,  $OW=W_U*W_S*W_V'$  and obtain  $W_U$ ,  $W_S$  and  $W_V$ .

**Step 6:** Modify S1 with watermark such that  $S=S1 + a*WS$ .

**Step 7:** Obtain  $B^*$  using  $B^*=U*S*VT$ .

**Step 8:** Apply inverse DCT to  $B^*$  to produce LL\_HH\*.

**Step 9:** Apply inverse DWT to LL\_LL, LL\_HL, LL\_LH and LL\_HH\* to get matrix LL\*.

**Step 10:** Apply inverse DWT to LL\*, HL, LH and HH, set it to selected color channel to get watermarked image WI.

### 2.2 Watermark Mining Process:

The Mining process has been alienated into subsequent steps and is momentarily designated as given below:

**Step 1:** Select color channel and apply DWT to WI to get LL\*, HL, LH and HH.

**Step 2:** Apply DWT to WI to get LL\_LL, LL\_HL, LL\_LH and LL\_HH\*.

**Step 3:** Select LL\_HH\* band and divide it into 4X4 square blocks.

**Step 4:** Apply DCT to each block of sub band LL\_HH\*, select first DCT values and get matrix A.

**Step 5:** Apply SVD to A,  $A=WU*WS*WVT$  and obtain WU, WS, WVT.

**Step 6:** Obtain  $SW=(S-WS) /a$ .

**Step 7:** Obtain  $EW= W_U*SW*W_VT$ .

### 3. EXPERIMENTAL SETUP

We programmed with Mat lab to realize the algorithm above, and did watermark signal embedding and detecting. These are some following images which helps to compare the results of proposed algorithm with existing approach.



**Fig-3.1:** a) Extracted watermark image b) Scrambled watermark image



**Fig-3.2:** c) Original image



**Fig-3.3:** Watermarked image

### 4. PERFORMANCE EVALUATION

#### 4.1 NCC Analysis

Normalized Cross Correlation (NCC) is used to measure the similarity between the original watermark and extracted watermark. Normalized Cross Correlation is calculated to evaluate the robustness of algorithm [4]. Table 4.1 demonstrates the evaluation of existing and proposed methods where CI is the cover image, WI stands for watermark image and WA, MFA, GNA, HA stands for without attack, median filter attack, gaussian noise attack and histogram attack. By using proposed algorithm, the results of NCC Analysis become higher than previous results.

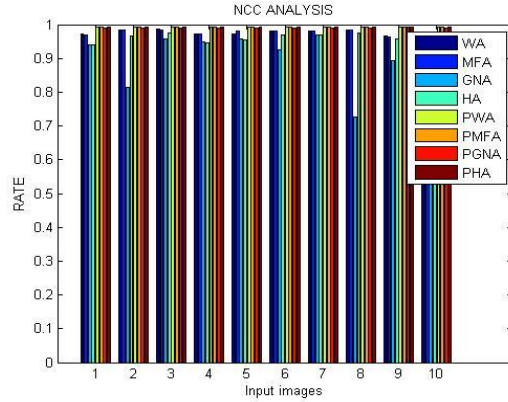
Images		Existing			
CI	WI	WA	MFA	GNA	HA
6	1	0.9728	0.9699	0.9414	0.9395
21	20	0.9836	0.9836	0.8151	0.9671
8	3	0.9858	0.9853	0.9572	0.9750
6	11	0.9719	0.9709	0.9484	0.9451
8	11	0.9710	0.9819	0.9589	0.9536
10	15	0.9805	0.9799	0.9257	0.9682
6	15	0.9805	0.9799	0.9686	0.9698
16	7	0.9851	0.9844	0.7257	0.9761
18	2	0.9659	0.9642	0.8925	0.9568
6	9	0.9728	0.9737	0.9393	0.9436

**Table 4.1: NCC Analysis**

Images		Proposed			
CI	WI	WA	MFA	GNA	HA
6	1	0.9925	0.9925	0.9906	0.9925
21	20	0.9925	0.9925	0.9906	0.9925
8	3	0.9925	0.9925	0.9906	0.9925
6	11	0.9926	0.9925	0.9906	0.9926
8	11	0.9925	0.9925	0.9906	0.9925
10	15	0.9925	0.9925	0.9906	0.9925
6	15	0.9925	0.9925	0.9906	0.9925
16	7	0.9925	0.9925	0.9906	0.9925
18	2	0.9925	0.9926	0.9916	0.9925
6	9	0.9925	0.9925	0.9906	0.9925

**Table 4.2: NCC Analysis**

The following graph presents the information of NCC Analysis and evaluates it within two statements. WA, MFA, GNA, HA expose the existing method and PWA, PMFA, PGNA, PHA describe the proposed method which is improved as compared to earlier ones.



**Graph-4.1: NCC Analysis of previous results and proposed results for different images.**

**4.2 Peak Signal to Noise Ratio**

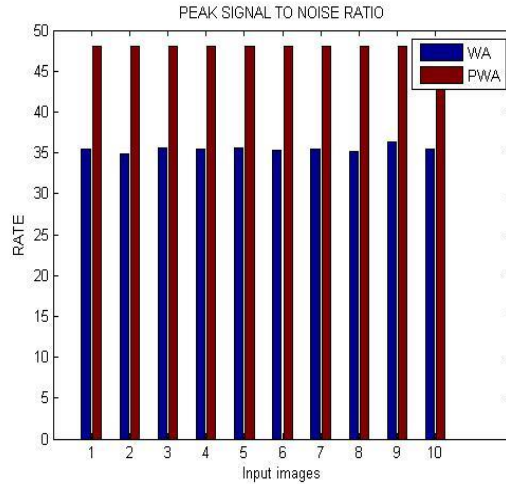
The PSNR is employed to evaluate the difference between an original image and watermarked image. In order to evaluate the transparency of watermarked image, we use parameter peak value signal-to-noise ratio (PSNR). Peak signal-to-noise ratio is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affect the reliability of its representation.

Table 4.3 illustrates the comparison of Peak signal-to-noise ratio between existing and proposed method. By using proposed algorithm the value of PSNR becomes improved as compared to previous results.

Images		Existing	Proposed
Cover Image	Watermark Image	WA	WA
6	1	35.4553	48.0587
21	20	34.8924	48.0333
8	3	35.6013	48.0479
6	11	35.4553	48.0601
8	11	35.6013	47.9889
10	15	35.3204	48.0323
6	15	35.4553	48.0440
16	7	35.1798	48.0257
18	2	36.2984	48.0491
6	9	35.4553	48.0522

**Table 4.3: Peak signal-to-noise ratio Evaluation**

The following graph shows the representation of peak signal to noise ratio between previous and proposed techniques. Blue bar expose the existing method and maroon bar describe the proposed method which are superior as compared to previous ones.



**Graph-4.2: PSNR of previous results and proposed results for different images**

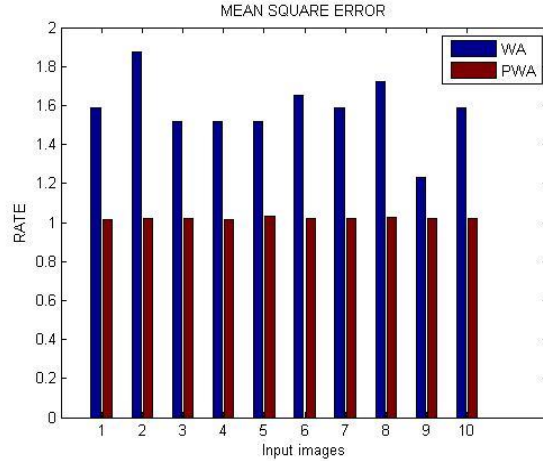
**4.3 Mean Square Error**

In statistics, the MSE of an estimator measures the average of the squares of the errors that is the difference between the estimator and what is estimated. Table 4.4 illustrates the comparison of Peak signal-to-noise ratio between existing and proposed method. By using proposed algorithm the value of PSNR becomes improved as compared to previous results.

Images		Existing	Proposed
Cover Image	Watermark Image	Without Attack	Without Attack
6	1	1.5858	1.0167
21	20	1.8771	1.0227
8	3	1.5179	1.0193
6	11	1.5179	1.0164
8	11	1.5179	1.0332
10	15	1.6512	1.0230
6	15	1.5858	1.0202
16	7	1.7222	1.0245
18	2	1.2318	1.0190
6	9	1.5858	1.0183

**Table 4.4: Mean Square Error**

The following graph shows the representation of peak signal to noise ratio between previous and proposed techniques. Blue bar expose the existing method and maroon bar describe the proposed method which are improved as compared to previous ones.



**Graph-4.3: MSE of previous results and proposed results for different images**

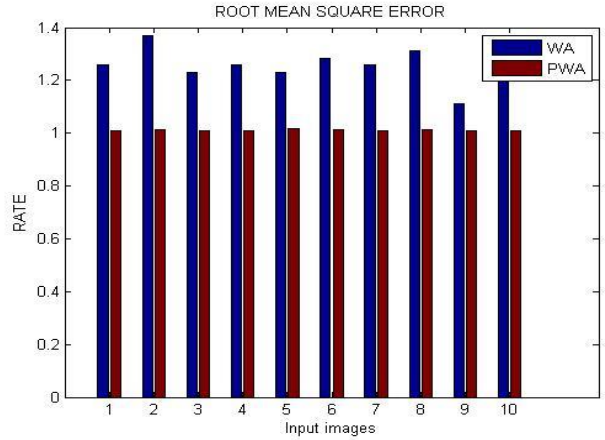
**4.4 Root Mean Square Error**

RMSE is a quadratic scoring rule which measures the average magnitude of the error. The RMSE is most useful when large errors are particularly undesirable. Table 4.5 illustrates the comparison of **root mean square error** ratio between existing and proposed method. By using proposed algorithm the value of RMSE becomes improved as compared to previous results.

Images		Existing	Proposed
Cover Image	Watermark Image	WA	WA
6	1	1.2593	1.0083
21	20	1.3701	1.0113
8	3	1.2320	1.0096
6	11	1.2593	1.0082
8	11	1.2320	1.0165
10	15	1.2850	1.0114
6	15	1.2593	1.0100
16	7	1.3123	1.0122
18	2	1.1099	1.0095
6	9	1.2593	1.0091

**Table 4.5: Root Mean Square Error**

The following graph shows the representation of **root mean square error** between previous and proposed techniques. Blue bar expose the existing method and maroon bar describe the proposed method which are improved as compared to previous ones



**Graph-4.3: RMSE of previous results and proposed results for different images**

**4.5: Average Error**

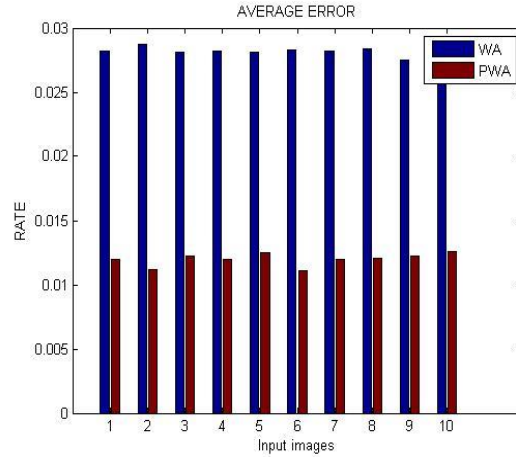
Average also called arithmetic mean the result obtained by adding the numbers or quantities in a set and dividing the total by the number of member in the set. Table 4.5 illustrates the comparison of average error between existing and proposed method. By using proposed algorithm the value of average error becomes improved as compared to previous results.

Images		Existing	Proposed
Cover Image	Watermark Image	Without Attack	Without Attack
6	1	0.0282	0.0120
21	20	0.0287	0.0112
8	3	0.0281	0.0122
6	11	0.0282	0.0120
8	11	0.0281	0.0125
10	15	0.0283	0.0111
6	15	0.0282	0.0120
16	7	0.0284	0.0121
18	2	0.0275	0.0122
6	9	0.0282	0.0126

**Table 4.5: Average Error**

The following graph shows the representation of **root mean square error** between previous and proposed techniques. Blue bar expose the existing method and maroon bar describe the proposed method which are improved as compared to previous ones.





**Graph-4.4: Average error of previous results and proposed results for different images**

## CONCLUSION

Digital watermarking is a multifaceted technique essentially concerning numerous conflicting necessities and trade-offs thus subsequent in many real-world as well as technical tasks. Digital watermarking using SVD is a rapidly developing arena with heaps of potential in upcoming novel applications, also its present applications in the information security, manufacturing and information hiding areas. A watermark is a recognizable image or pattern in paper that appears as various shades of lightness. Adding a visible watermark is a common way of identifying images and protecting them from unauthorized use online. This paper has proposed a new modified SVD based watermarking to enhance the results further. Various kind of attacks are also applied to evaluate the effectiveness of the proposed technique. The comparison has clearly shown that the proposed technique outperforms over the available methods.

In near future, embedding ++ to enhance the security further. However, further enhancement will also be done by implementing the proposed algorithm in real time environment. Also, some more attack will be considered to evaluate the performance of the proposed algorithm further.

## REFERENCES

- [1] Zebbiche, Khalil, and Fouad Khelifi, "Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking," *IET Image Processing* 8, pp.23-32, January 2014.
- [2] Zhu, Yong, Xiaohong Yu, and Xiaohuan Liu, "An image authentication technology based on digital watermarking," *IEEE International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)*, pp.179-183, May 2013.
- [3] Raval, Keta, and S.Zafar, "Digital Watermarking with Copyright Authentication for Image Communication", *IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)*, pp.111-116, March 2013.
- [4] Divecha, Nidhi, and N.N.Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images," *IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)*, pp.204-208, March 2013.
- [5] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad, "Video Watermarking Techniques for Copyright Protection and Content Authentication," *IEEE International Journal of Computer Information Systems and Industrial Management Applications*, vol.5, pp. 652–660, 2013.
- [6] Qianli, Yang, and Cai Yanhong, "A digital image watermarking algorithm based on discrete wavelet transform and discrete cosine transform," *IEEE International Symposium on Information Technology in Medicine and Education*, vol.2, pp.1102-1105, August 2012.
- [7] Shi, Hailiang, Nan Wang, Zihui Wen, Yue Wang, Huiping Zhao, and Yanmin Yang, "An RST invariant image watermarking scheme using DWT-SVD," *IEEE International Symposium on Instrumentation and Measurement, Sensor Network and Automation(IMSNA)*, vol.1, pp.214-217, August 2012.

- [8] Ghosh, Sudip, Pranab Ray, Santi P.Maity, and Hafizur Rahaman, "Spread Spectrum Image Watermarking with Digital Design," IEEE International Conference on Advance Computing (IACC), pp.868-873, March 2009.
- [9] Dorairangaswamy, M.A., and B.Padmavathi, "An effective blind watermarking scheme for protecting rightful ownership of digital images," IEEE Region 10 Conference in TENCON, pp.1-6, January 2009.
- [10] Harsh K Verma, Abhishek Narain Singh and Raman Kumar, "Robustness of the Digital Image Watermarking Techniques against Brightness and Rotation Attack," International Journal of Computer Science and Information Security (IJCSIS), 2009.
- [11] Tiwari, Nirupma, Monika Sharma, Manoj Kumar Ramaiya, and Naveen Hemrajani, "DWT based Self-Embedding watermarking" UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA, Volume 3: Issue 2, [ISSN 2250 – 3765], 05 June 2013.
- [12] Vinita Gupta, and Mr. Atul Barve, "A Review on Image Watermarking and Its Techniques" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), pp.92-97, January 2014.