Digital Image Watermarking Using Alpha Blending

by

Name	Roll No.	Registration No:
Mainak Majumder	11700314050	141170110232 OF 2014-2015
Debprasad Sardar	11700314037	141170110219 OF 2014-2015
Alokendra Pal	11700314007	141170110189 OF 2014-2015
Abhijit Kumar Shaw	11700314001	141170110183 OF 2014-2015

A comprehensive project report has been submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

ELECTRONICS & COMMUNICATION ENGINEERING

Under the supervision

of

Dr. Abhishek Basu

Assistant Professor

Department of Electronics & Communication Engineering

RCC INSTITUTE OF INFORMATION TECHNOLOGY

Affiliated to Maulana Abul Kalam Azad University of Technology, WestBengal

CANAL SOUTH ROAD, BELIAGHATA, KOLKATA – 700015

MAY, 2018

CERTIFICATE OF APPROVAL

This is to certify that the project titled **"Digital Image Watermarking Using Alpha Blending"** carried out by

Name	Roll No.	Registration No:
Mainak Majumder	11700314050	141170110232 OF 2014-2015
Debprasad Sardar	11700314037	141170110219 OF 2014-2015
Alokendra Pal	11700314007	141170110189 OF 2014-2015
Abhijit Kumar Shaw	11700314001	141170110183 OF 2014-2015

for the partial fulfillment of the requirements for B.Tech degree in **Electronics and Communication Engineering** from **Maulana Abul Kalam Azad University of Technology, West Bengal** is absolutely based on his own work under the supervision of **Dr.Abhishek Basu** The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

.....

Dr. Abhishek Basu
Head of the Department (ECE)
RCC Institute of Information Technology

DECLARATION

"We Do hereby declare that this submission is our own work conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute and that, to the best of our knowledge and belief, it contains no material previously written by another neither person nor material (data, theoretical analysis, figures, and text) which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text."

.....

Mainak Majumder
Registration No: 141170110232 OF 2014-2015
Roll No: 11700314050

.....

Debprasad Sardar
Registration No: 141170110219 OF 2014-2015
Roll No:11700314037

.....

Alokendra Pal
Registration No: 141170110189 OF 2014-2015
Roll No: 11700314007

.....

Abhijit Kumar Shaw
Registration No: 141170110183 OF 2014-2015
Roll No: 11700314001

Date:

Place:

CERTIFICATE of ACCEPTANCE

This is to certify that the project titled "**Digital Image Watermarking Using Alpha Blending**" carried out by

Name	Roll No.	Registration No:
Mainak Majumder	11700314050	141170110232 OF 2014-2015
Debprasad Sardar	11700314037	141170110219 OF 2014-2015
Alokendra Pal	11700314007	141170110189 OF 2014-2015
Abhijit Kumar Shaw	11700314001	141170110183 OF 2014-2015

is hereby recommended to be accepted for the partial fulfillment of the requirements for B. Tech degree in **Electronics and Communication Engineering** from **Maulana Abul Kalam Azad University of Technology, West Bengal**

Name of the Examiner Signature with Date

1. ……

2.……..……..

3.……

4. ……

ABSTRACT

Watermarking the image files is an extremely proficient method used in the field of communication technology. When any information required transmitting from one place to another security is vital. This security is provided by hiding data into images, audio and video. This review on the different watermarking techniques gives the clear concept of the watermarking scheme. In this project, we propose a digital watermarking technique which is based on alpha blending. Using alpha blending technique, we watermark the image (Original Image) with another image (called Watermark Image). The resultant image is the watermarked image. We evaluate the performance of PSNR for different values of alpha and determine an optimum value of alpha. Evaluating the three parameters of PSNR, MSE and SSIM for different images, we find that the proposed watermarking technique is perceptible. We explore the robustness of the proposed watermarking technique by evaluating the parameters of PSNR, MSE and BER for the watermarked image which is subjected to various attacks.

CONTENTS

LIST OF ABBREVIATIONS

PSNR	Peak Signal to Noise Ratio
MSE	Mean-Squared Ratio
SSIM	Structural Similarity Index
BER	Bit Error Rate

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

1.1. Information Hiding

In this section, we briefly discuss the historical development of watermarking. We also introduce various data hiding terminologies used in current literature and attempts have clear distinction of them.

1.1.1. History

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Iliad [1]. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. Kautilya's Arthasastra and Lalitavista'ra, and Vatsayana's Kamasutra are few famous examples of the Indian literature in which secret writing / steganography have been used.

The idea of Watermarking technique has evolved from steganography. The use of watermarks is a very old technique. Our ancients poured their half-stuff slurry of fiber and water on to mesh molds to collect the fiber, then dispersed the slurry within deckle frames to add shape and uniformity, and finally applied great pressure to expel the water and cohere the fiber. Now a days we use the watermark technique for information hiding.

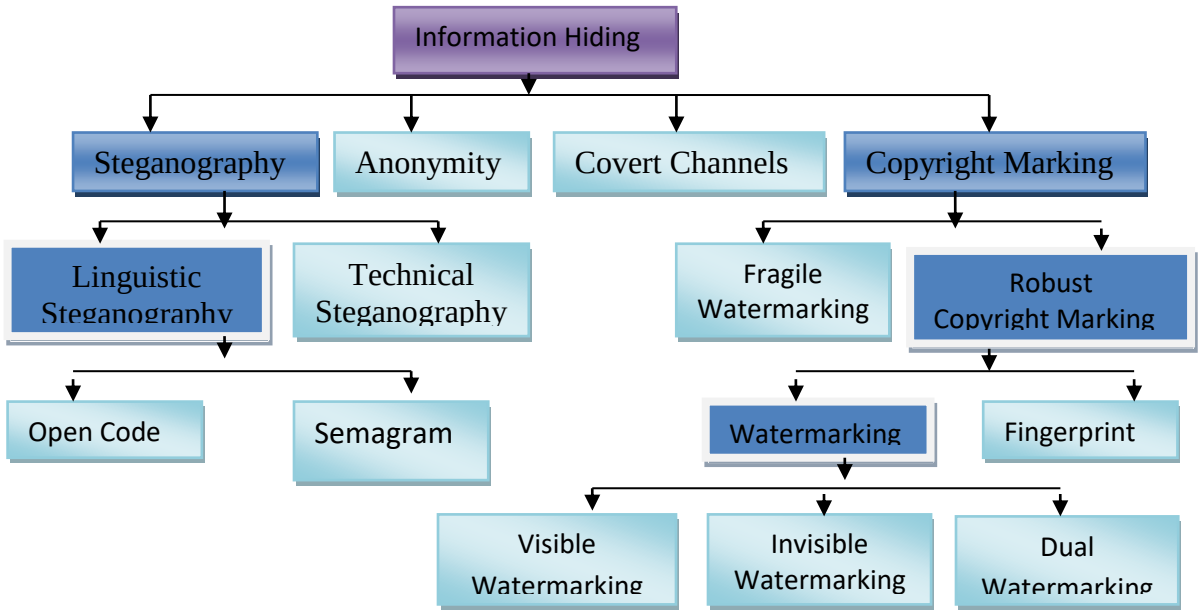


Figure.1 Classification of Information Hiding

One of the information hiding technique is the watermark technique of impressing into the paper a form of image, or text derived from the negative in the mold, as the paper fibers are squeezed and dried. Paper Watermarks have been in wide use since the late middle Ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In more recent times, water-marks have been used to certify the composition of paper, including the nature of the fibers used. Today most developed countries also watermark their paper, currencies and postage stamps to make forgery more difficult.

The digitization of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. Watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality ownership and source.

1.1.2. Steganography Vs Cryptography

To have a better understanding of the terms we compare "steganography" with "cryptography" . The term steganography means "cover writing" whereas cryptography means "secret writing". Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plain text and disguised message is called cipher text. [1] The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is the clear. Steganography hides messages in plain sight rather than encrypting the message; it is embedded in the data (that has to be protected) and doesn't require secret transmission. The message is carried inside data. Steganography is there-fore broader than cryptography. The schematic representation of the cryptography is given in Fig. 2(b).

1.1.3. Digital Watermarking

Watermarking is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. It may also be text only. Watermark is basically used as guarantee of authenticity, quality ownership and source.

1.1.4. Steganography Vs Digital Watermarking

They primarily differ by intent of use. A watermark can be perceived as an attribute of the carrier. It may contain information such as copyright, license, tracking and authorship etc. whereas in case of steganography, the embedded message may have nothing to do with the cover. In steganography an issue of concern is bandwidth for the hidden message whereas robustness is of more concern with watermarking.

1.1.5. Fingerprinting and Labeling

Fingerprints are also called labels by some authors. Digital watermarking differs from “digital fingerprinting”. Fingerprinting are characteristics of an object that tend to distinguish it from other similar objects. Fingerprinting is the process of adding fingerprints to an object and recording them, or identifying and recording fingerprints that are already intrinsic to the object. Dig-ital fingerprinting produces a metafile that describe the contents of the source file.

1.1.6. Digital Signature Vs Digital Watermark

There are conflicting viewpoints about the “digital signature”. Some authors use digital signature and digital watermark synonymously, whereas some authors distinguish between the digital signature and digital watermark. A digital signature is based upon the idea of public key encryption. A private key is used to encrypt a hashed version of the image. This encrypted file then forms a unique ”signature” for the image since only the entity signing the image has knowledge of the private key used. An associated public key can be used to decrypt the signature. The image under question can be hashed using the same hashing function as used originally. If these hashes match then the image is authentic [1]. Digital signature can be used for more than just image authentication. In particular when combined with secure timestamp, a digital signature can be used as a proof of first authorship. A watermark, on the other hand, is a code secretly embedded into the image. The water-mark allows for verification of the origin of an image. However, a watermark alone is not enough to prove first authorship, since an image could be marked with multiple watermarks.

1.2. DIGITAL WATERMARK

In today's world there is a rapid growth of internet technology and multimedia products such as image, audio, videos etc. the security and authenticity issues are becoming popular. Watermarking is a concept of embedding special symbol or logo or pattern watermark, in to video, image, text etc. so that some copyright information is fed into it. This information can inform users about rights holder or authority to permit the use of data, it can later prove for ownership, identify misappropriate persons, tracking of the video, image, text etc. The watermarking may be visible or invisible.Watermark is used basically to stop the duplicasy.

1.2.1. Encoding Process

Let us denote an image by ***I***, a signature by ***S= s1, s2 …*** and the watermarked image by $\hat{I}$. E is an encoder function, it takes an image ***I*** and a signature ***S***, and it generates a new image which is called watermarked image $\hat{I}$, mathematically,

$$E(I, S) = \hat{I} \qquad (1)$$

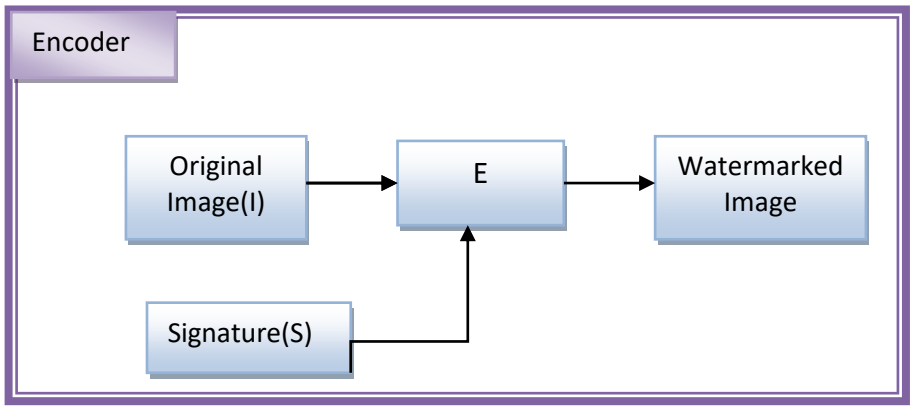


Figure.2 Generic Encoder

1.2.2. Decoding Process

A decoder function ***D*** takes an image ***J*** (can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature ***S'*** from the image. In this process an additional image ***I*** can also be included which is often the original and un-watermarked version of ***J***. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D(J, I) = S' \qquad (2)$$

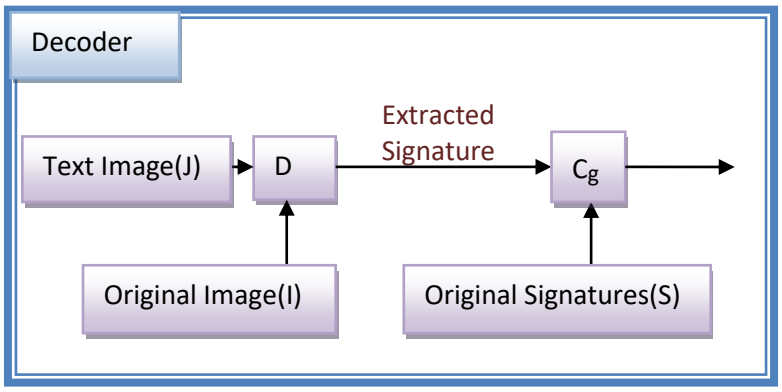


Figure.3 Generic Decoder

1.2.3. Types of Digital Watermarks

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in **spatial domain**. An alternative to spatial domain watermarking is **frequency domain** watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure below.

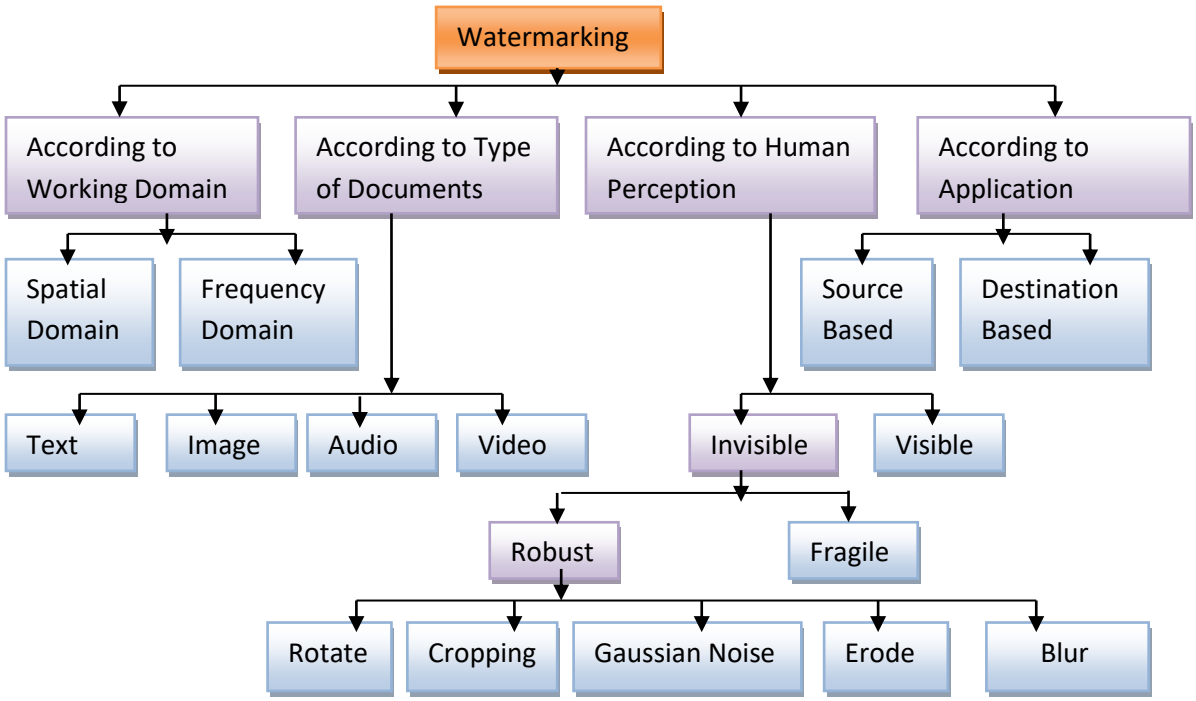


Figure.4 Classification of watermarking

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be divide into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

2. LITERATURE SURVEY

This section reports the previous works on watermarking and information hiding.

A proposal to develop a digital watermarking algorithm based on a fractal encoding method and the discrete cosine transform (DCT). [8]

To achieve both imperceptibility and robustness requirements, a hybrid image-watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) is proposed. [9]

Ongoing innovations are going in Digital Watermarking-based applications which can help content owners balance business requirements with consumer choice. [10]

A digital watermarking-based image quality evaluation method that can accurately estimate image quality in terms of the classical objective metrics, such as peak signal-to-noise ratio (PSNR), weighted PSNR (wPSNR), and Watson just noticeable difference (JND), without the need for the original image. [11]

A proposal for multiplicative watermarking method operating in the ridgelet domain wherein the directional sensitivity and the anisotropy of the ridgelet transform (RT) are employed in order to obtain a sparse image representation, where the most significant coefficients represent the most energetic direction of an image with straight edges. [12]

A proposal for a new measure of watermarking security, called the effective key length, which captures the difficulty for the adversary to get access to the watermarking channel. [13]

A detailed discussion of various aspects of watermarking technologies on various applications ranging from the embedding of marks in the pictorial information on paper to hardware protection. [15]

A proposal for a water marking algorithm based on discrete wavelet transform (DWT) of image and singular value decomposition (SVD). [16]

An efficient solution to avoid illegal copying of information from multimedia networks. Many watermarking algorithms have been developed and each of them has its own individuality because of its variety of applications. A new algorithm able to solve most of the practical issues of watermarking is designed. [17]

To protect confidential images a proposal for an efficient digital watermarking technique to deal with this complicated issue. [18]

A method is proposed which is a new and simple approach for detecting copy move forgery in digital images, which extract features based on color information of the forged image. The features are extracted using Auto Color Correlogram, Color Moments and HSV color space. [19]

A proposal for a blind digital audio water- marking algorithm that utilizes the quantization index modulation (QIM) and the singular value decomposition (SVD) of stereo audio signals. [20]

3. PROPOSED WATERMARKING TECHNIQUE

In this project we proposed an invisible image watermarking technique based on alpha blending method.

3.1. ALPHA BLENDING

Alpha blending is the process of combining a translucent foreground color with a background color, thereby producing a new blended color. The degree of the foreground color's translucency may range from completely transparent to completely opaque. If the foreground color is completely transparent, the blended color will be the background color. Conversely, if it is completely opaque, the blended color will be the foreground color. The translucency can range between these extremes, in which case the blended color is computed as a weighted average of the foreground and background colors [7].

Alpha blending is a convex combination of two colors allowing for transparency effects in computer graphics. The value of alpha in the color code ranges from 0.0 to 1.0, where 0.0 represents a fully transparent color, and 1.0 represents a fully opaque color. This alpha value also corresponds to the ratio of "SRC over DST" in Porter and Duff equations.

Alpha Blending can be accomplished by blending every pixel from the primary source image (cover image) with the relating pixel in the second source image (watermark)

3.2. ALPHA BLENDING METHOD

According to alpha blending technique watermarked image is obtained by equation

Equation: **WMI = (1-alpha)*LL + alpha*WM**

Where, **WMI** = Low frequency (recurrence) segment of the watermarked image,
LL = Low frequency (recurrence) segment of the cover image,
WM = Low frequency (recurrence) component of watermark,

And recovered watermark image is obtained by equation

Equation: **W** = (**WMI** – **LL**) / **alpha**

Where, **WMI** = Low frequency (recurrence) segment of the watermarked image,
LL = Low frequency (recurrence) segment of the cover image,

3.3. WATERMARK EMBEDDING PROCESS

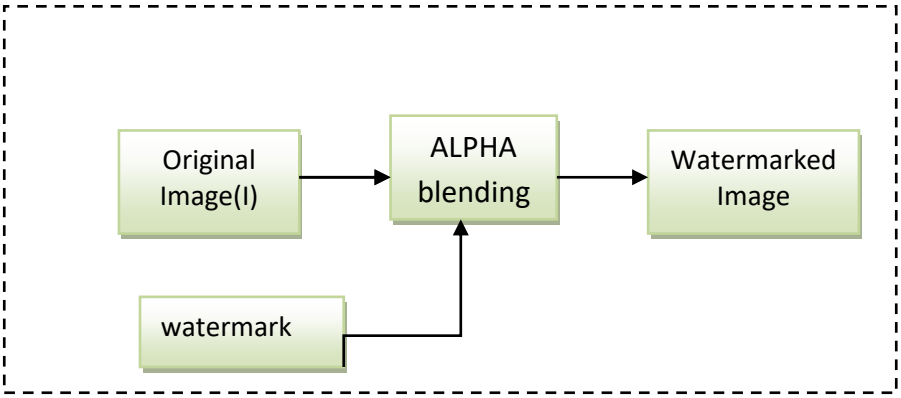


Figure.5 Embedding process

3.4 WATERMARK EXTRACTING PROCESS:

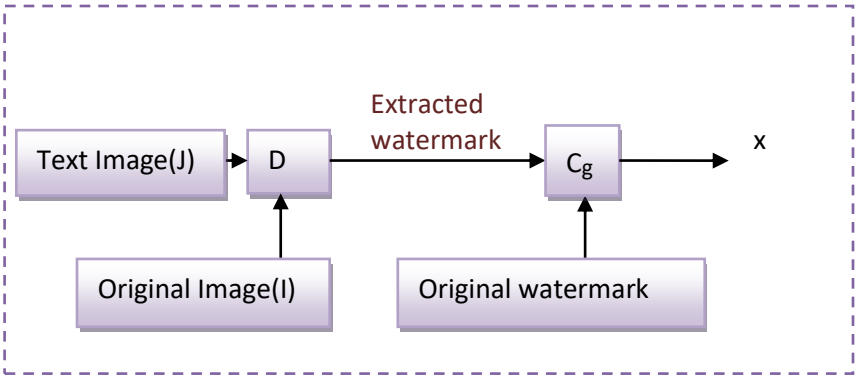
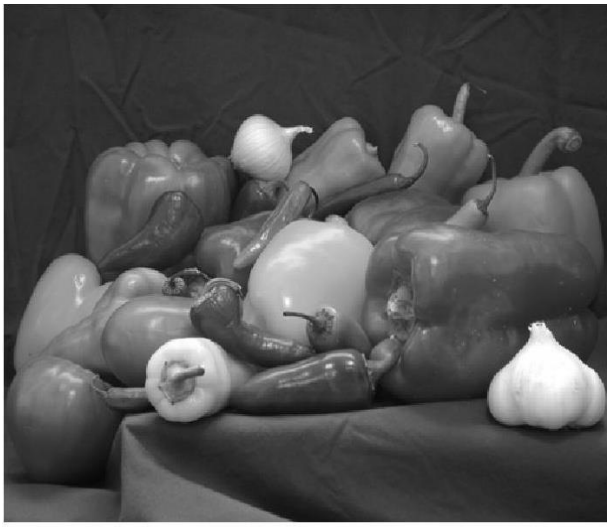


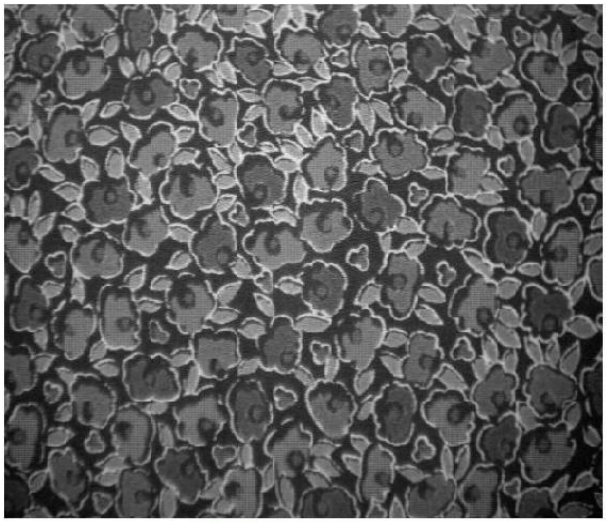
Figure.6 Extracting process

4. RESULT & DISCUSSION

We have performed this proposed method for three cover images. If the original image is color image then it has to be converted into grayscale image. The 'coins.png' is taken as a watermark. These input data are shown in figure below:

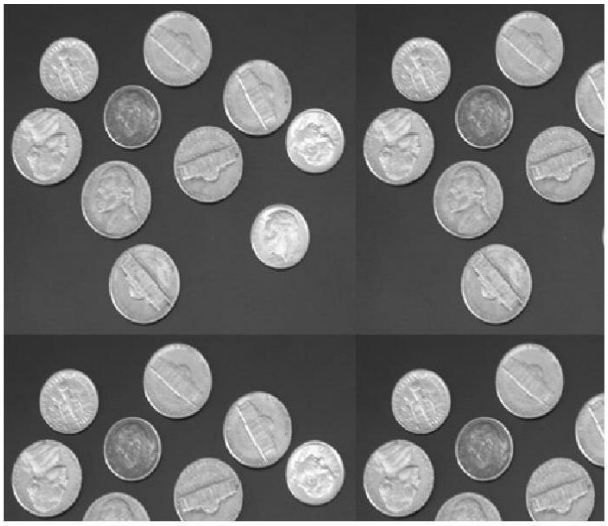


Original Image 1



Original Image 2

original image 3



Original Watermark

Figure.7 Different original image and original watermark

In this techniques low frequency band of cover image is taken and watermark is added using alpha blending technique. The watermark image is embedded into cover image by varying the

different value of alpha. Alpha gives the best result in between the 0.01 to 0.03. For the value of alpha in between 0.1 to 0.9 the watermark image becomes brighter and completely covers and destroys the cover image.

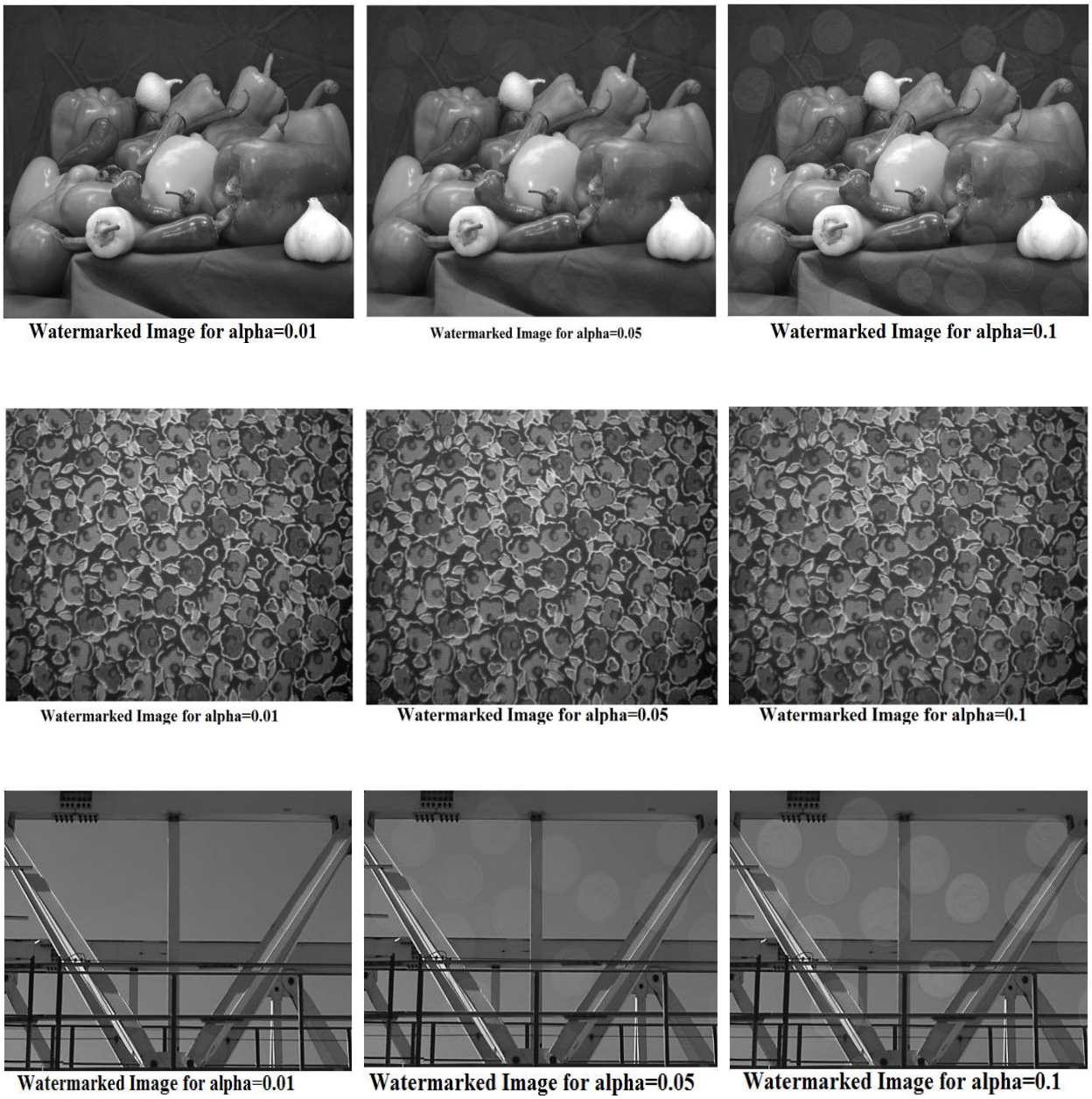


Figure.8 Watermarked images for different value of alpha

The following table shows the comparison of PSNR for different values of alpha of input image 'peppers.png'.

Table 1: Comparison between PSNR and alpha

Alpha	PSNR(dB)
0.01	45.2816
0.02	40.6213
0.03	36.9990
0.04	34.5142
0.05	32.5194
0.06	31.0106
0.07	29.6736
0.08	28.5067
0.09	27.4993

Alpha	PSNR(dB)
0.1	26.5584
0.2	20.6006
0.3	17.1112
0.4	14.6715
0.5	12.7476
0.6	11.2526
0.7	9.9941
0.8	8.9453
0.9	8.0731
1	7.3793

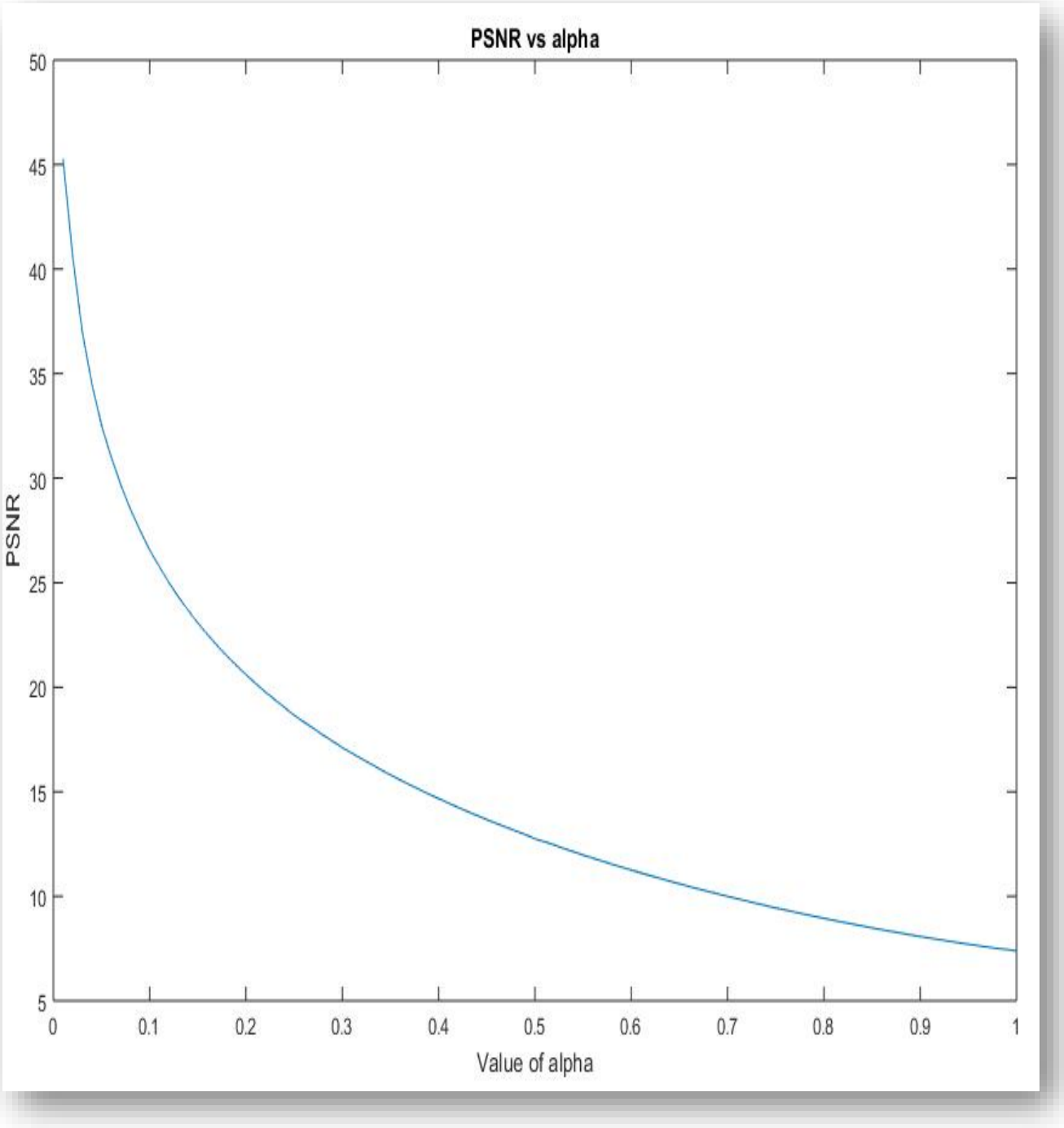


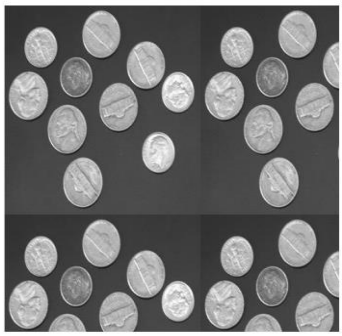
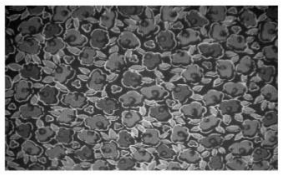
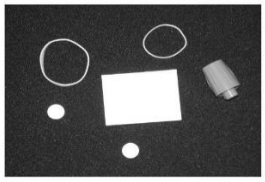
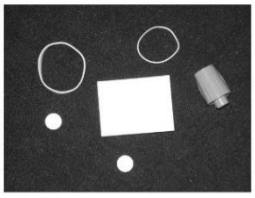
Figure.9 PSNR VS value of ALPHA

Here in the PSNR vs ALPHA graph we can see that for the value of alpha in between 0.01 to 0.03 we are getting best result.so we are taking alpha=0.02 as best case for further testing.

4.1. IMPERCEPTIBLITY

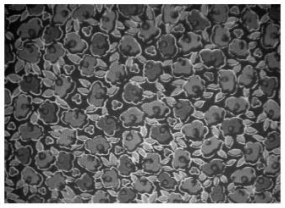
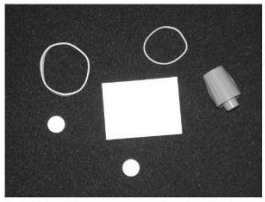
For evaluating the imperceptibility of the proposed technique the extracted watermarks corresponding to the different images are tabulated below.

Table 2: Original Image, WaterMark, Watermarkd Image

ORIGINAL IMAGE	WATER MARK	WATERMARKD IMAGE
		
		
		
		
		

The parameters of PSNR, MSE and SSIM are determined for different images subjected to the proposed watermarking technique are tabulated below.

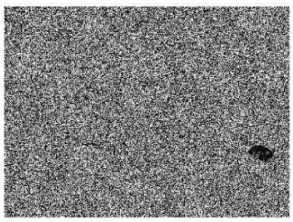
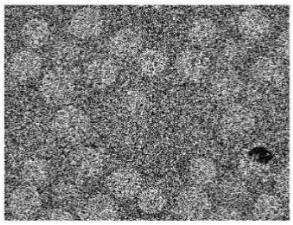
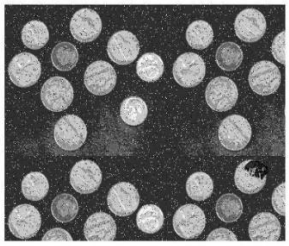
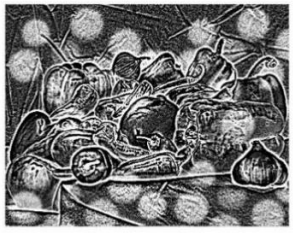
Table 3: Imperceptibility in terms of Metrics (alpha=0.02)

IMAGE	PSNR	MSE	SSIM
	40.6214	5.6356	0.9971
	40.9069	5.2770	0.9990
	40.8443	5.3537	0.9982
	40.8449	5.3529	0.9984
	40.9048	5.2796	0.9988

4.2. ROBUSTNESS

Various image processing attacks such as noise attacks including Gaussian, poisson, salt & pepper and in addition to that Blur attack is subjected on the image. The results are tabulated below.

Table 4: Robustness using different attacks and corresponding images

NAME OF ATTACK		IMAGE	EXTRACTED WATERMARK	Watermarked image
NOISE	Gaussin			
	Poisson			
	Salt & Pepper			
BLUR				

The parameters of PSNR, MSE, BER are tabulated when the image is subjected to image processing attacks

Table 5: PSNR, MSE, BER values after different attacks

IMAGE	NAME & ATTACKS		PSNR	MSE	BER
	**NOISE**	**1.GAUSSIAN**	5.4382	18589.0383962006	0.4975
		2.POISSON	6.2475	15428.7137908931	0.4911
		3.SALT & PEPPER	16.9021	1327.00813802193	0.4485
	BLUR		9.0989	8001.92093403845	0.4742

5. CONCLUSION

In this Project, implementation of basic digital image watermarking method based on alpha blending technique is described. The given results clearly show that the quality of the watermarked image and the recovered watermark is dependent only on the scaling factor alpha.

The proposed method of watermarking has been implemented to make the process of watermarking both robust and imperceptible. We have used various noise attacks on the watermark to determine the robustness of the watermark. Four types of noise attacks have been used. The noise attacks were Gaussian, Poisson, Salt & Pepper and Speck. Comparing the results of the noise attacks, the resultant watermark has been found to be imperceptible.
On determining the Mean-Squared Error(MSE), Structural Similarity Index(SSIM) and Bit Error Rate(BER) of the watermark, we can conclude that the watermark is robust.

Therefore, the proposed watermarking method is both Robust and imperceptible.

5.1. *FUTURE SCOPE*

The proposed watermarking technique have been developed under the assumption that the noise attacks are happening in isolation and not simultaneously. The project can be extended in scenario where the noise attacks happen simultaneously.

The proposed scheme is limited to only image watermarking. The future work can be extended to audio and video data.

The proposed scheme is limited to only software. The future work can be extended to the realization of the software implementation and the subsequent hardware implementation.

6. REFERENCES

[1]. S. P. Mohanty, A. Sengupta, P. Guturu and E. Kougianos, "Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection.," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 83-91, July 2017.

[2]. C. C. Lai and C. C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060-3063, Nov. 2010.

[3]. R. Samtani, "Ongoing Innovation in Digital Watermarking," in *Computer*, vol. 42, no. 3, pp. 92-94, March 2009.

[4]. S. Liu, Z. Pan and H. Song, "Digital image watermarking method based on DCT and fractal encoding," in *IET Image Processing*, vol. 11, no. 10, pp. 815-821, 10 2017.

[5]. P. Campisi, D. Kundur and A. Neri, "Robust digital watermarking in the ridgelet domain," in *IEEE Signal Processing Letters*, vol. 11, no. 10, pp. 826-830, Oct. 2004.

[6]. P. Bas and T. Furon, "A New Measure of Watermarking Security: The Effective Key Length," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1306-1317, Aug. 2013.

[7]. *https://www.ocf.berkeley.edu/~horie/alphablend.html*

[8]. Y. Li, "A Water Marking Algorithm of Digital Image Based on DWT-SVD," *2009 First International Conference on Information Science and Engineering*, Nanjing, 2009, pp. 5307-5310.

[9]. C. V. L. Priya and N. R. N. Raj, "Digital watermarking scheme for image authentication," *2017 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, 2017, pp. 2026-2030.

[10]. S. Bhatnagar, S. Kumar and A. Gupta, "An approach of efficient and resistive digital watermarking using SVD," *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, New Delhi, 2014, pp. 2470-2475.

[11]. A. V. Malviya and S. A. Ladhake, "Copy move forgery detection using low complexity feature extraction," *2015 IEEE UP Section Conference on Electrical Computer and Electronics (UPCON)*, Allahabad, 2015, pp. 1-5.

[12]. M. J. Hwang, J. Lee, M. Lee and H. G. Kang, "SVD-Based Adaptive QIM Watermarking on Stereo Audio Signals," in *IEEE Transactions on Multimedia*, vol. 20, no. 1, pp. 45-54, Jan. 2018.

[13]. P. Praveenkumar, R. S. Devi, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan, "Stego integrated image encryption using row and column indexing — An information security," *2017 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 2017, pp. 1-4.

[14]. A.K. Goyal, N.Agrawal, S.Verma, (2007) Robust Watermarking in Transform domain using edge detection technique, IEEE

[15]. Ingemar J. Cox: *Digital watermarking and steganography*. Morgan Kaufmann, urlington, MA,USA, 2008

[16]. Ravi K. Sharma, and Steve Decker, (2001) Practical Challenges For Digital Watermarking Applications, IEEE

[17]. Akhil Pratap Shing, A. M. (2011). WAVELET BASED WATERMARKING ON DIGITAL IMAGE . *Indian Journal of Computer Science and Engineering,Vol 1 No 2* , 86-91.

[18]. A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne . "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673.

[19]. Ge Xiuhui, Tian Hao, (2008), Research on Application of Reversible Digital, International Conference on Computer Science and Software Engineering.

[20]. Bo Shen, Iihwar K. Sethi and Vasudev Bhaskaran, (1998) DCT Domain Alpha Blending, IEEE