Data Hiding Technique for Consumer Applications

A Thesis Report submitted in fulfillment of the requirement for the award of the degree of

Master of Technology

In

Computer Science & Engineering

Under the Supervision of

Dr. Amit Kumar Singh

(Supervisor) By

Neha sharma Enrollment No: 152203



Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh- India 173234 May,2017

Certificate

This is to certify that thesis report entitled "**Data Hiding Techniques for Consumer Applications**", submitted by **Neha Sharma** in fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This synopsis has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Dated:

Supervisor's Name -Dr. Amit Kumar Singh

Signature

Acknowledgement

I would like to take this opportunity to acknowledge all those who helped me during this report work. Compiling a year's work in to this was an exhausting job, but writing this page of acknowledgement is a joyous task to cherish the memories of all those who helped me to enrich the newer experience of life.

I owe my deep sense of respect and heartfelt gratitude to my major Supervisor **Dr. Amit Kumar Singh, Assistant Professor, Department of Computer Science & Engineering, Jaypee University of Information Technology** for his valuable guidance and constant inspiration in preparing this report. I will always remain indebted to him for his unending guidance and untiring efforts in successful completion of this work. I consider myself fortunate to have worked under his able guidance. I am thankful to office staff of the department for providing all the necessary and timely help. I am also thankful to responds of my study for their co-operation who helped me to complete my study.

I wish to express my sincere thanks to all my friends for their support and guidance. There is paucity of words to express my heartiest thanks to my Sisters *Monika Sharma & Neelam Sharma* for the timely help Best wishes and cheerful company remained a morale booster and made things smoother throughout the course of this study.

I owe my achievements to the unconditional love and support of my mother *Mrs.Satya sharma* whose sacrifice I can never repay. They inspired me at every step of my life and encouraged me to never give up even in the face of overwhelming odds. I grope for words to express my deep feelings, love and affection to my youngest brother. Last but not least I would like to express my gratitude to all those who helped, guided and supported me in one way or the other but have been inadvertently left out because all may not have been mentioned but none have been forgotten.

Needless to say, omissions are mine.

Name of the Student: - Neha sharma

Signature

Dated:

Table of content

S.N	Topic name	Page No.
1.	Chapter 1 Data hiding techniques:-An introduction	1-19
1.1	Basic concept of digital watermarking	2
1.2	Important characteristics of watermark	3
1.3	Types of watermark	6
1.5	Embedding and Extraction process of watermarking	7
1.5.1	Applications of digital watermarking	8
1.5.2	Classification of digital watermarking techniques	9
1.5.3	Stages in watermarking	10
1.6	Watermarking embedding techniques	12
1.6.1	Spatial domain watermarking	12
1.6.2	Transform domain watermarking	13
1.7	Analysis and quality performance measures	17
1.8	Distortion and attacks	18-19
2	Chapter 2 Recent Survey on data hiding techniques	20-25
3	Chapter 3 A Novel technique for text watermarking using LSB	26-31
3.1	Steganography	26-27
3.2	Least significant bit	27
3.3	Adaptive Huffman coding	28
3.4	Implementation using Huffman coding	28
3.5	Algorithm for data embedding /extraction	30-31
3.6	Experiment and results	31-45
4	Chapter 4 MATLAB	47-51

8	References	56-60
7	List of publications	55
6	Conclusion and scope of future	54
4.7	Some limitations	51
4.5	Conversion b/w double and Uint8	50
4.5	Principal Operations	49
4.4	Working format in MATLAB	49
4.3	Image formats in mat lab	48
4.2	Introduction to Digital image	48
4.1	About MATLAB	47

List of Figures

S.NO	Title	no.
1.	Characteristics of digital watermarking	4
1.1	Classification of Watermarking	5
1.2	Watermark embedding and extraction process	7
1.3	Digital watermarking framework	11
1.4	Discrete cosine transform region	13
1.5	Two level DWT decomposition of host image	
3.	Flowchart for adaptive Huffman coding	28
3.1	Flowchart for Huffman coding	
3.2	Data Embedding for huffman coding	30
3.3	Data Embedding for huffman coding	31
3.4	Adaptive huffman coding with different text sizes	33
3.5	huffman coding with different text sizes	34
3.6	Adaptive Huffman coding with different image size	35

3.7	Huffman coding with different image size	
3.8	Adaptive Huffman with different types attacks	37
3.9	Huffman with different types attacks	38
3.9.1	Adaptive Huffman with different gain factors	39
3.9.2	Huffman with different gain factors	40
3.9.3	Adaptive Huffman with different size of images	
3.9.4	Huffman with different size of images	42

List of tables

S.N	Title	Page no.
1.	The classification of watermark and their description	9
1.1	Comparison between various watermarking techniques	15
1.2	Comparison between Spatial and Frequency domain watermarking	16
2.	Review of some reported watermarking techniques	24
3.	Adaptive huffman coding with different text sizes	33
3.1	huffman coding with different text sizes	34
3.2	Adaptive Huffman coding with different image size	35
3.3	Huffman coding with different image size	35
3.4	Adaptive Huffman with different types attacks	36
3.5	Huffman with different types attacks	37
3.6	Adaptive Huffman with different gain factors	38
3.7	Huffman with different gain factors	39
3.8	Adaptive Huffman with different size of images	40

3.9	Huffman with different size of images	41
3.10	Comparison between Adaptive Huffman and Huffman coding text size	42
3.11	Comparison between Adaptive Huffman and Huffman coding Image size	43
3.12	Comparison between Adaptive Huffman and Huffman coding of different type of attacks	43
3.13	Comparison between Adaptive Huffman and Huffman coding with different size of images	44
3.14	Comparison between Adaptive Huffman and Huffman coding with different size of images	44
4.	Commands for managing variables	48
4.1	Functions for image format conversion	50
4.2	Saving and Loading variables in MATLAB	51

List of Symbols

SN	Symbol	Description
1	I(x,y)	Cover image
2	$I_W(X, Y)$	Watermarked image
3	W(x,y)	Random noise
4	I _{max}	Maximum possible value of image pixel
5	W(I,j)	Original watermark image
6	W'(I,j)	Extracted Watermark image
7	μ	Degree of combination
8	E _b	Image pixels as black
9	E _W	Image pixels are white
10	A(x,y)	DWT coefficients before embedding watermark
11	A'(x,y)	DWT coefficients after embedding watermark

List of acronyms

S.N	Word	Description	
1.	DCT	Discrete cosine transform	
2.	DWT	Discrete wavelet transform	
3.	SVD	Singular value decomposition	
4.	LSB	Least significant bit	
5.	NC	Normalized correlation	
6.	PSNR	Peak signal noise ratio	
7.	BER	Bit error rate	
8.	MSE	Mean square Error	
9.	DFT	Discrete Frequency Transform	
10.	FRWPT	Fractional Wave Packet Transform for Robust	
		Watermarking	

ABSTRACT

The improvement of the Web has as regularly as conceivable extended the availability of cutting edge data, for instance, sound, pictures and recordings to general society. Progressed watermarking is an advancement being made to ensure and energize data affirmation, security and copyright protection of automated media.

A computerized watermark is an undetectable mark implanted inside a picture to show legitimacy and possession. A viable computerized watermark ought to be perceptually imperceptible to forestall check of the first picture. It ought to be measurably undetectable to anticipate discovery, and it ought to likewise be strong to many picture controls, for example, separating, added substance clamor, and pressure. Computerized Watermarking is the way toward inserting data into advanced interactive media substance with the end goal that the data can later be removed or identified for an assortment of purposes including duplicate avoidance and control. Advanced watermarking has been proposed as another, option technique to uphold the licensed innovation rights and shield computerized media from tampering. It includes a procedure of inserting into a host flag a perceptually straightforward computerized signature, conveying a message about the Mark is known as the advanced watermark. The computerized watermark contains information that can be utilized as a part of different applications, including advanced rights administration, communicate checking and sealing. Chapter wise description of the thesis report is describe as follows:

Chapter 1 presents the basic concepts of data hiding techniques and their importance in recent applications. Characteristics of watermarking system, major classifications of watermark and define the peak-signal-to noise ratio (PSNR), bit error rate (BER) as some metrics to determine the performance of the watermarking method (s) are also described in this chapter. Watermarking techniques are divided into spatial and transform domain techniques. Various spatial, transform domain techniques are described briefly in this chapter.

Chapter 2 presents the state-of-the-art watermarking methods and compares the performance of some recent techniques in tabular form.

In chapter 3, we propose a watermarking algorithm based on LSB and Huffman compression technique using text watermark. The performance of the method is tested in terms of PSNR and BER. The method is also robust for different attacks.

In chapter 4, we present an introduction of our simulation tool (MATLAB) and its important functions in brief.

Conclusion and future directions of the work is presented in Chapter 5.

CHAPTER 1

Data Hiding Techniques: An Introduction

1.1 Introduction

The internet is become most important thing in our day to day life. The multimedia and its technology have increased the protection of digital media. Digital media consists of text, images and digital audio, Video etc. From the most latest couple of years progression in innovation of PCs and PC systems gives better nature of administration and higher data transfer capacity for both remote and wired systems However the portrayal of media in advanced frame and extension of web additionally made simple to transmit computerized media, for example, picture, sound, video in a straightforward way[1-2]. There are different strategies for securing advanced substance encryption, verification and other time examining procedures are expected to keep the assurance of computerized substance against the duplicating and unlawful dissemination of pictures and recordings. The general watermarking framework comprises of three distinct parts implanting procedure, assault and Extraction handle. The watermarking framework utilized for vast size of utilizations like copyright insurance, fingerprinting and altering location. It serves security verification of item maker, media serialization and following computerized watermarking offers preferred standpoint to assurance of interactive media information by different security concerns. The insurance of online sites still these days turn into the most imperative substance Advanced watermarking innovation is a critical field in software engineering, cryptography, flag handling. Advanced Watermarking is create by its engineers as the answer for the need to offer some incentive included assurance top of information encryption and scrambling for substance insurance and validation [3]. The web has turned into the revisionary now days in the everyday life the need of web and correspondence innovation in life expanding far and wide along these lines applying web use to give constant scope of stories, daily papers, magazines ,music, and improved video needs to broadly expanding to circulate work. [3-4]. Automated Watermarking offers system to cover watermarks into cutting edge substance to shield

it from illegal copy or multiplication. Its qualities like impalpability, quality, security of cover picture [4]. The watermark should be worked as a free and it can be the extremely same appropriated. Energy of the watermark proposes the nature of the watermark against various picture taking care of attacks. Consistency is the variable which chooses the way of the photo in the wake of embedding the watermark [5]. The incorporation of a watermark under this organization makes the watermark incredible to banner taking care of operations and normal geometric changes gave that the main picture is open and that it can be adequately selected against the changed watermarked picture [5-6].

1.2 Basic concepts of digital watermarking

The expression "computerized digital watermark" was first created in 1992 by Andrew Tirkel and Charles Osborne, in their paper which named as "Electronic Water Stamp". The term utilized by Tirkel and Osborne was right off the bat utilized as a part of Japanese as "denshi sukashi" in Japan which is articulated as an "electronic watermark". Furthermore 700 years back, paper watermarks were used Fabriano, Italy to demonstrate the paper check and the plant that conveyed it. After their creation, watermarks quickly spread over Italy and a while later over Europe. By the eighteenth century, watermarks on paper made in Europe and America had ended up being used as trademarks, to record the date the paper was created and to exhibit the sizes of exceptional sheets, paper course of action, quality and quality. The watermarks begun to be used as bug copying measures on money and diverse reports which are comprehensively used as security components in cash today.

Moreover define as essentially watermarking, a case of bits implanted into a propelled picture, sound or video archive that recognizes the record's copyright information (maker, rights and identification of owner.). The name starts from the faintly observable watermarks engraved on stationery that perceive the maker of the stationery.

The explanation behind cutting edge watermarks is to give copyright security to authorized advancement that is in automated sort out [6]

Not in the slightest degree like printed watermarks, which are required to be to some degree unmistakable, automated watermarks are planned to be absolutely imperceptible, or because of sound catches, ill defined. Likewise, the honest to goodness bits addressing the watermark must be scattered all through the record with

the end goal that they can't be recognized and controlled. In conclusion, the propelled watermark must be adequately healthy so it can withstand regular changes to the record, for instance, diminishes from lossy weight counts.

Satisfying each one of these necessities is no basic deed, however there are different associations offering fighting progressions. Each one of them work by making the watermark appear as commotion - that is, unpredictable data that exists in most exceptional records at any rate. To see a watermark, you require a remarkable program that knows how to isolate the watermark data. Watermarking is moreover called data embedding and information concealing.

Watermarking, rather than steganography, has the additional thought of healthiness against attacks. Despite the likelihood that the nearness of the covered information is known it is troublesome—ideally incomprehensible—for an aggressor to pulverize the embedded watermark, paying little mind to the likelihood that the algorithmic run of the watermarking technique is open. An utilitarian consequences of the power essential is that watermarking methods can typically introduce extensively less information into host data than steganography systems. Steganography and watermarking are along these lines more basic than forceful procedures [4]. A watermarking structure is for the most part disengaged into two specific steps, introducing, and acknowledgment.

1.3 Important characteristics of watermark

Figure 1.1 the basic necessities of general watermarking systems. The genuine characteristics of modernized watermarking are designated a great many are classified as follows [6]:

a) Robustness: The watermark should be fit to contradict after regular picture taking care of operations, for instance, picture trimming, change etc.

b) Imperceptibility: The watermarked picture should appear like same as the primary picture to the basic eye. The onlooker can't recognize that watermark is embedded in it.

c) Security: An unapproved somebody can't identify, recover or change the installed watermark.

d) **Transparency:** It relates to the properties of the human substantial. A clear watermark causes no curious or highlight disaster.

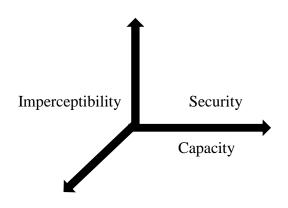


Fig 1. Characteristics of digital watermarking [6]

e) **Capacity:** Limit portrays what number of data bits can be settled. It addresses additionally the likelihood of embeddings different watermarks in one record in parallel. Restrict require always exertion against two other fundamental things, that is, fancy and liberality. A higher purpose of imprisonment is ordinarily gotten to the impediment of either vitality quality or trickiness, or both.

Computerized watermarking is a procedure which is utilized as a part of the advanced flag handling of implanting shrouded data into interactive media information. This data is not typically unmistakable, just devoted locator or extractor can seen and removes that data. Advanced Image Watermarking use computerized picture for implanting the shrouded data, subsequent to inserting the watermarked picture is produced and the watermarked picture is stronger against assaults [7]. Figure 1.2 shows the important classification of the watermark.

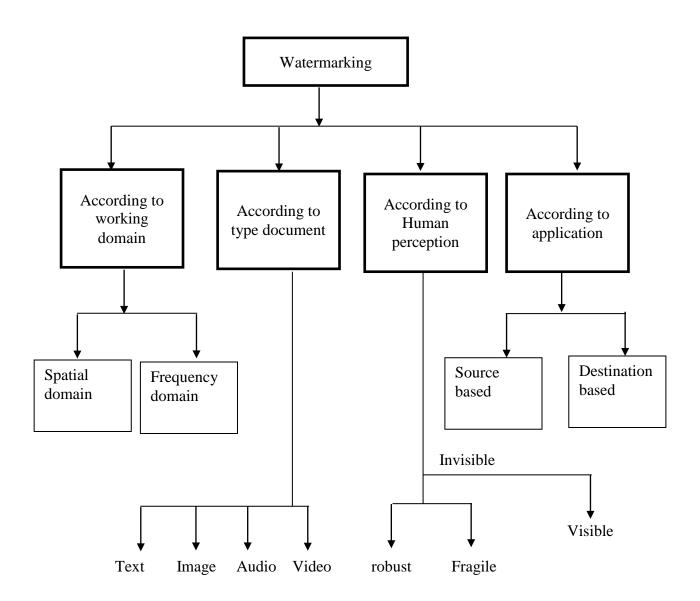


Fig. 1.1 Classification of Watermarking [7]

Some of the important types of watermarking based on different watermarks are given below:

1.4 Types of digital watermarks

Some of the important types of watermarks are given below [8]:

a) Visible watermarks

Visible watermarks are in the terms of logos. Such watermarks are relevant to pictures as it were. These logos are decorated into the picture however they are straightforward. Such watermarks can't be expelled by editing the middle some portion of the picture. Further, such watermarks are ensured against, for example, measurable investigation. The disadvantages of obvious watermarks are debasing the nature of picture and location by visual means as it were. In this way, it is unrealistic to distinguish them by committed projects or gadgets. Such watermarks have applications in maps, design and programming UI.

b) Invisible watermark

Intangible watermark is concealed in the substance. It can be perceived by an affirmed association so to speak. Such watermarks are used for substance as well as maker affirmation and for recognizing unapproved copier.

c) Fragile Watermark

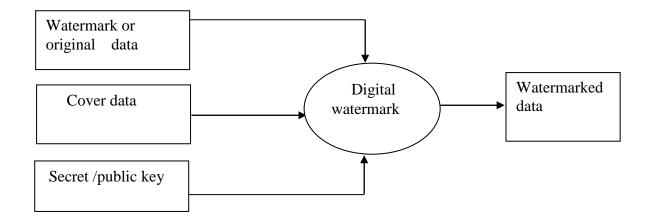
Delicate watermarks are those watermarks which can be easily crushed by any attempt to upset them. Sensitive watermarks are pounded by data control. In the going with figure an instance of fragile watermarking the primary address the principal picture, the second is the balanced picture and the third the recognized adjustment. Other than watermark force, watermark can in like manner sorted into evident and vague sorts, perceptible watermarks are noticeable to a watcher. On the other hand, imperceptible watermarks are unclear and don't change the visual of the photos. In our wander, we are enthusiastic about indistinct watermarks since they have a more broad extent of employments appeared differently in relation to recognizable watermarks.

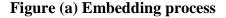
- d) **Robust Watermarks**: -These watermarks can't be broken easily as they withstand many banner get ready strikes. Capable watermark should remain set up forever in the embedded banner with the true objective that attempts to empty or annihilate the solid watermark will degenerate or even may wreck the way of the photo. This system can be used to ensure copyright security of the banner.
- e) **Blind Watermarks:** -These watermarks recognize the introduced information without the usage of one of a kind banner. They are less effective to any attacks on the banner.

1.4 Embedding and extraction process of digital watermarking

The way toward implanting data into another protest or flag can be named as watermarking. Watermarking is for the most part utilized for duplicate insurance and copyright-security [5-6]. Watermarking has been utilized to send delicate data covered up in another flag. Watermarking has its applications in picture/video copyright security. Advanced watermarking can characterized as to embed a mystery message or logo into the first media source by utilizing signal handling strategy.

Figure 1.3 (a)-(b) show the general watermarking embedding and extraction process respectively. The watermark introducing structure takes as data the watermark bits, the photo data, and on the other hand a puzzle or open key. The yield of the watermark embeddings system is the watermarked picture. The watermark extraction structure takes as data a photo that conceivably contains watermarks and maybe a riddle or open key. Dependent upon the sort of watermarking system used, it may in like manner take as information the main picture or the watermark. The watermark extraction structure chooses if a watermark is accessible or missing in the photo. It may in like manner yield a sureness measure that exhibits the probability with which the watermark is accessible in the photo.





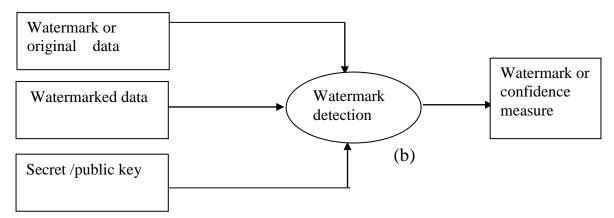


Figure 1.2 Watermark (a) embedding and (b) extraction process

1.4.1 Applications of digital watermarking

The important applications of digital watermarks are discuss below [9]

a) Owner Identification

The use of watermarking to which he made is to see the proprietor of any media. Some paper watermark is sufficiently exhausted by some little exercise of aggressors. So the modernized watermark was shown. In that the watermark is the inner piece of forefront media with the target that it can't be feasibly seen and cleared.

b) Copy Protection

Unlawful copying is furthermore foreseen by watermarking with copy secure piece. This security requires repeating contraptions to be consolidated with the watermark perceiving equipment.

c) Broadcast Monitoring

Broadcasting of Television openings and radio news is similarly checking by watermarking. It is generally completed with the Paid media like recreations convey or news is imparted.

d) Medical applications

Helpful media and reports in like manner precisely affirmed, having the information of patient and the meeting experts. These watermarks can be both evident and imperceptible. This watermarking helps experts and therapeutic applications to affirm that the reports are not changed by illegal means.

e) Fingerprinting

A fingerprinting is a procedure by which a work can be doled out a unique recognizing verification by securing some propelled information in it as watermark. Perceiving the watermark from any unlawful copy can incite the recognizing verification of the person who has discharged the principal substance.

f) Information Validation

Approval is the strategy of perceive that they got substance or data should be right as it was sent. There should be no changing completed with it. So consequently sender embedded the propelled watermark with the host data and it would be removed at the recipients end and checked.

1.4.2 Classification of digital watermarking techniques

Advanced watermarking can be extensively partitioned into vigorous and delicate watermarking. Hearty watermarking is utilized to appoint copyright data of the computerized works, the inserted watermark can oppose the different picture preparing lossy compression and watermark is not devastated after the procedure of assault and it will be distinguishable to give the accreditation of the first substance. Delicate watermarking is basically for honesty security, which might be touchy to shift changes in the flag [8-9].

Digital watermarking can be partitioned into picture watermarking, video watermarking, sound watermarking, and content watermarking and realistic watermarking in light of the appended media. Picture watermarking alludes to including watermark in still picture. Video watermarking includes computerized watermark in the video stream to control video applications Content watermarking implies adding watermark to PDF, DOC and other content record to anticipate changes of content. Realistic Watermarking is installing watermark to two-dimensional or three-dimensional PC produced representation to demonstrate the copyright.

Digital watermarking can be separated into visual watermarking and visually impaired watermarking as indicated by the discovery procedure. Visual watermarking needs the first information in the testing course, it has more grounded power, yet its application is constrained. Dazzle watermarking does not require unique information, which has wide application field, yet requires a higher watermark innovation.

The watermarks can be classified on the basis of permanency, visibility, detection and domain. According to domain watermarking techniques can be classified as spatial domain and frequency domain techniques [8].

Table 1: classification	of watermark and	l their description [7]
-------------------------	------------------	-----------------------	----

S.N	Criteria	Description	
1	Watermark Type	Noise: pseudo noise, Gaussian random and chaotic sequences Image: Any logo, Stamp Image etc.	
2	Robustness	Fragile: Easily Manipulated. Semi-Fragile: Resist from some type of Attacks Robust: not affected from attack	
3	Domain	Spatial: LSB, Spread Spectrum Frequency: DWT, DCT, DFT, SVD	
4	Perceptivity	Visible Watermarking: Channel logo Invisible Watermarking: like Steganography	
5	Host Data	Image Watermarking Text Watermarking Audio Watermarking	

1.4.3 Stages in general watermarking systems

Figure beneath demonstrates the phases of advanced watermarking. Fundamentally working of computerized picture watermarking can be partitioned in three phases:

a. Embedding Stage

The inserting stage is the main stage in which the watermark is implanted in the first picture by utilizing the installing calculation and the mystery key. At that point the watermarked picture is created. So the watermarked picture is transmitted over the system.

b. Distortion/Attack Stage

In this stage, when the information is transmitted over the system. Either some commotion is included with the watermarked picture or a few assaults are performed on the watermarked picture. In this way, our watermarked information is either adjusted or demolished.

c. Detection/Retrieval Stage

In the location organize, the watermark is identified or extricated by the committed indicator from the watermarked picture by applying some identification calculation and by utilizing mystery key. Furthermore, commotion is likewise detected.Fig3. Demonstrates the idea of computerized watermarking system.

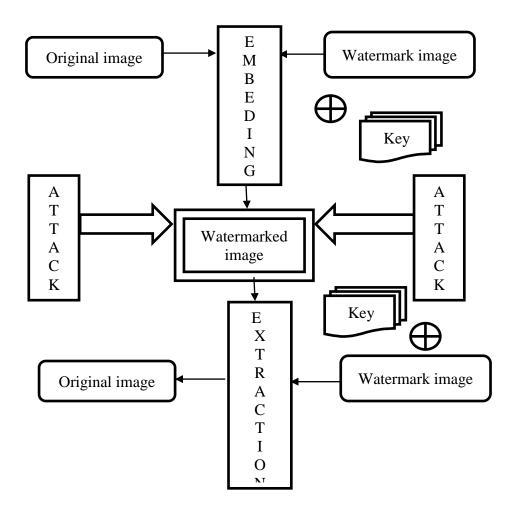


Fig1.3 Digital watermarking framework

1.5 Spatial and transform domain techniques

According to working domain, watermark techniques can be classified into two important techniques, spatial and transform domain.

1.5.1 Spatial Domain Watermarking [10]: -It works by implanting watermark by adjusting estimations of pixels. It is straightforward procedure and requires less time and computational multifaceted nature. In any case, this system is less vigorous against assaults. Different spatial area strategies are:

- a) Least significant bit (LSB): It is ordinarily utilized spatial area system in which haphazardly pixels of cover picture are chosen and watermark is inserted in slightest critical bits.
- b) Correlation-Based Techniques:-In this strategy a pseudo-irregular clamor is added to a picture and amid interpreting a relationship between's two is found. On the off chance that connection esteem surpasses some edge level watermark is discovered else it is definitely not.
- c) SSM-Modulation-Based Technique: These method are connected in the water stamping calculations with a connected data and appended to the first picture with pseudo commotion flag, it's regulated by the watermark.

Spread-go methodologies are strategies in which imperativeness made no less than one discrete recurrence is intentionally spread or passed on in time. SSM based watermarking estimations embed information by straightforwardly joining the host picture with a little pseudo bustle hail that is balanced by the embedded watermark.

e) Texture mapping coding Technique

This procedure is useful in quite recently those photos which have some surface part in it. This strategy hides the watermark in the surface some bit of the photo. This estimation is sensible for those zones with far reaching number of self-selfassured surface pictures (hindrance), and is unthinkable normally. This methodology covers data inside the constant self-assertive surface cases of a photograph.

f) Patchwork Algorithm

Interlaced is data hiding strategy made by Drinking binge et alii and disseminated on IBM Frameworks Diary, 1996. It relies on upon a pseudorandom, real model. Interlaced unobtrusively inserts a watermark with a particular estimation using a Gaussian allocation. A pseudo aimlessly decision of two patches is finished where the first is An and the second is B. Settle A photo data is lit up where as that of settle B is darkened.

g) Correlation-Based Technique

In this framework, a pseudorandom no. (PN) outline says W(x, y) is added to cover picture I(x, y). Iw(x, y) = I(x, y) + k*W(x, y) Where K address the get component, Iw address watermarked picture underground creepy crawly position x, y and I address cover picture. Here, if we augment the get segment then regardless of the way that it fabricates the energy of watermark yet the way of the watermarked picture will decrease.

1.5.2 Transform domain techniques

These calculations shroud the watermarking information in change coefficients, in this manner spreading the information through the recurrence range [1] making it difficult to recognize and solid against many sorts of flag preparing controls. The most utilized changes are: Discrete cosine transform (DCT) [1], discrete wavelet transform (DWT) [6] and discrete lifting transform (LWT) [7].

- a) Discrete Cosine Transform (DCT):- The Discrete Cosine Transform (DCT) calculation is notable and normally utilized for picture pressure. DCT changes over the pixels in a picture, into sets of spatial frequencies. The DCT work by isolating pictures into the parts of various frequencies. Amid a stage called Quantization, where parts of pressure really happen, the less imperative frequencies are disposed of, consequently the utilization of the lossy. At that point the most vital frequencies that remain are utilized recover the picture in disintegration prepare. Thus, recreated picture is contorted. Contrasted with other information subordinate changes, DCT has many points of interest Fig 1.5 shows discrete cosine transform [6]:
 - a. It has been executed in single incorporated circuit.
 - b. It can pack most data in least coefficients.
 - c. It limits the square like appearance called blocking relic that outcomes when limits between sub-pictures.

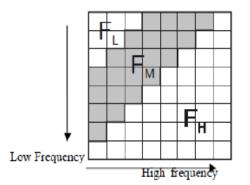


Figure 1.4 Discrete Cosine Transform Region

In this method picture is separated into non-covering pieces. At that point forward DCT is connected to every one of these pieces. The main change coefficient is called DC coefficient and all others are air conditioning coefficients. In the wake of applying some square determination and coefficient choice criteria. Watermark is inserted by altering chose coefficient with watermark. After that converse change is connected to change over picture into spatial area. In DCT, for implanting the watermark, picture is partitioned into various recurrence groups [8].

Formulae of 2-D DCT

$$F(m,n) = \sum_{i=0}^{N-1} \sum_{J=0}^{N-1} C(m)c(n)f(i,j)\cos\left[\frac{\prod(2i+1)}{2N}\right] * \cos\left[\frac{\prod(2i+1)}{2N}\right]$$
(1)

b) Discrete Wavelet Transform (DWT): DWT of cutting edge picture gives multi-assurance depiction of a photo which helps in unraveling picture information. It changes the two-dimensional propelled picture into four quadrants of different frequencies i.e. LL, LH, HL, HH. The low repeat part can be part again into more quadrants of high and low frequencies until the banner is totally rotted. DWT also a repeat zone picture change strategy that is used to part the information of any propelled media into gauge sub signal (used to show the pixel regard) and organized sub hail (used to exhibit the vertical, level and corner to corner purposes of intrigue). The crucial focus of DWT procedure is to cover data as coefficients. DWT is examined on channel bank. Fig 1.6 shows the discrete wavelet transform.

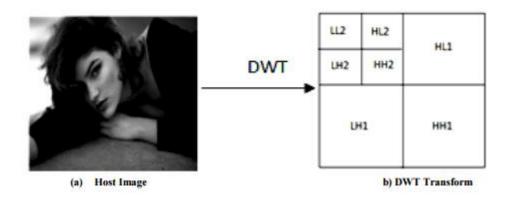


Figure 1.5 Two level DWT decomposition of host image

The DWT is connected on the host picture to deteriorate the picture into four non covering multi determination coefficient sets. The coefficients are:

$$W_{LL}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y)$$
$$W_{LH}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y)$$
$$W_{HL}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y)$$
$$W_{HH}^{J} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} h(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y)$$

c) Discrete Fourier Transform (DFT):DFT gives strength against different geometrical assaults. It is additionally partitioned into two systems which are immediate inserting and layout based implanting. In direct implanting DFT size and stage coefficients are adjusted while inserting watermark. In layout based installing present's formats which are characterized as structure implanted in DFT space for the estimation of change component. After the change of picture, this change component is utilized perceive picture and afterward locator can be utilized to extricate inserted spread range watermark. The discrete Fourier change is a standout amongst the most

essential changes utilized as a part of flag preparing and picture handling. For a 1-D periodical succession of tests $\{u(n), n=0, ..., N-1\}$.

	Advantages	Disadvantages
LSB	Simple to execute and get it.	It needs essential
	Low corruption	vigor
	High perceptual	Helpless against
	straightforwardness	clamor
		Helpless against
		editing, scaling
Correlation	Pick up component can be	Picture quality gets
	expanded bringing about	diminished because
	expanded vigor	of high increment in
		pick up element.
DCT	The watermark is	Piece adroit DCT
201	installed into the center	devastates the
	recurrence, so the	invariance properties
	deceivability of picture	of the system
	won't get influenced and	2
	the watermark won't be	Certain higher repeat
	evacuated by any sort of	parts tend to be
	assault.	smothered in the
	Pixels themselves don't	midst of the
	influence each other	quantization step
DWT	Permits great limitation	Cost of processing
	both in time and spatial	might be higher.
	recurrence area	
		Longer pressure time
	Higher pressure	
	proportion which is	Clamor/obscure
	applicable to human	close edges of
	discernment	pictures or video
		outlines.

Table 1.1 Comparison between various watermarking techniques

c) Singular Value Decomposition (SVD): SVD is the factorization of An into the consequence of three frameworks A = UDV T where the areas of U and V are orthonormal and the system D is awry with positive bona fide entries. It decays structure of host picture into 3 rectangular systems i.e. U, S and transpose (T) of V. S is corner to corner network whose to one side entries are single values and are in diving demand. U and V are orthogonal square matrices in which segments are left and right specific vectors. Let I is square system then SVD can be addressed as:

S.N	Spatial domain	Frequency domain
Computational cost	Low	high
Robustness	Fragile	More robust
Perceptual quality	High control	Low control
Capacity	High (depends on the size of t he image)	Low
Example of application	Mainly authentication	Copyrights

 Table 1.2 Comparison between Spatial and Frequency domain watermarking [5]

1.6 Analysis & Quality Performance Measures

To define the quality parameters are described below [9]:-

The quality execution of the watermarked pictures, there are some quality measures, for

example, PSNR, MSE, NC and BER

a) Peak to Signal Ratio (PSNR)

It is utilized to quantify the intangibility of a watermarked picture, i.e. closeness between the first picture and watermarked picture. It can likewise be utilized to contrast unique watermark and the removed watermark. It is communicated as quality measure. Higher the PSNR esteem higher is the security. It itself utilizes Mean Square Blunder (MSE) for its calculation. PSNR can be spoken to as:

$$PSNR = 10 \log \left[\frac{255^2}{MSE}\right]$$
(2)

PSNR is the proportion between greatest conceivable energy of a flag and the energy of degenerate commotion. Here 255 is most extreme conceivable pixel esteem (of the cover picture). MSE is processed as:

$$MSE = \sum_{I=1}^{N} \sum_{I=1}^{N} \frac{(X(i,j) - i^{w}(i,j))^{2}}{N^{2}}$$
(3)

Where, N speaks to number of lines and sections (here considered same esteem), X(i,j) is the first picture pixel esteem and Xw (i,j) is the watermarked picture pixel esteem.

b) Normalized Cross Correlation

The normalized cross correlation (NCC) is utilized to quantify the closeness between the cover picture and the watermarked picture and also unique watermark and recouped watermark. Higher the estimation of NCC will bring about better method. It is figured by the equation:

$$NCC = \frac{\sum i \sum j}{\sum i \sum j} \frac{[I(i,j) - I\omega(i,j)]}{[I(i,j) - I\omega(i,j)]}$$
(4)

Where, I (i, j) is the original image pixel value and Iw (i,j) is the watermarked image pixel value.

c) Bit Error Rate:-It is characterized as a proportion between number of inaccurately decoded bits and aggregate number of bits. It is utilized to assess the unwavering quality of the content watermark. In this manner bring down piece blunder rate, better is the execution of watermarking calculation. The bit error is computed as

Bit error rate = $\frac{\text{Incorrectly decoded bit}}{\text{total number of bit}}$

1.7 Distribution and Attacks:

The transmission media can realize some incident in the banner recommending in a hurt substance. These ambushes may be consider or accidental. Ponder attacks use each open resource for destroy or adjust the watermark making it hard to focus it, the techniques by and large used are: banner planning systems, cryptanalysis, steganalysis. On the other hand, coincidental strikes are unavoidable, in light of the way that each photo taking care of or transmission racket may exhibit twisting [10].

These assaults are named takes after:-

- a) Simple Attacks: These attacks change the information of the cover picture without endeavoring to focus on the watermark area. Case: Noise expansion, trimming, change to simple and wavelet-based pressure.
- **b) Disabling Attacks**: The objective of these attacks is to endeavor to break the connection between's the watermark and the cover picture, making extraction unimaginable. Case: Geometric bends, pivot, trimming and inclusion of pixels.
- c) Ambiguity Attacks: These attacks confound the receptor installing a fake watermark, making it difficult to find which the first implanted stamp in the cover picture was.
- d) Removal Attacks: In this type of an investigation of the watermark is done, assessing the watermark substance and endeavoring to separate it from the host picture. Case: Certain non-direct channel operations and assaults custom-made to a particular watermark calculation.

CHAPTER 2

Recent Survey on data hiding techniques

Lie et al. [10] proposed a double insurance strategy through picture watermarking for JPEG picture. At first, the cover picture is separated into various channel and the delicate watermark is installing into the cover picture. Advance, the delicate watermark is removed through a two-organize technique. The trial comes about built up that the strategy is vigorous and great verification rates for various flag handling assaults at adequate visual nature of the watermarked picture. Notwithstanding that the strategy likewise addresses the false positive issue and the vigor execution of the strategy is superior to other announced methods. Hawlader et al. [11] presents a SVD based strong and secure twofold stages watermarking philosophy for copyright affirmation. The technique utilized two proposed methods essential watermark and optional watermark. The partner watermark takes the data of central watermark and support to essential watermark for different ambushes, security points of interest and fundamental watermark emptied utilizing a mystery scaling technique. A DWT SVD based new philosophy was started, the cover picture is decayed by DWT and the SVD is related on each of the four sub-get-togethers. In the watermark embeddings get ready, SVs of watermark were installed into the SVs of each sub social affairs and brought into SVs of cover picture by utilizing a scaling section. The methodology proposes the imperative guide, Arnold's catlike guide and particular respect separating .The framework delineates the Ascertained manual for introduce a mixed up course of action for embeddings the crucial watermark for the security in the particular zone. The essential watermark is encoded by utilizing discovered guide with puzzle parameters. The test happens demonstrates that the essential watermark is encoded by utilizing figured guide with the puzzle parameters and this system gives the extensive quality power against different ambushes than other SVD based strategies.

Karla et al. [12] proposed a powerful visually impaired watermarking calculation. The strategy in view of Double encryption procedure and discrete wavelet change. The visually impaired watermarking is actualized which is hearty to safe assaults .The DWT change over the cover pictures into their separate recurrence area. In this technique it utilizes lifting wavelet and Henon for the encryption of watermark. The technique is undetectable and vigorous for some typical assaults like JPEG, editing, including, and sifting. The watermark execution of the picture in view of PSNR and higher the estimation of PSNR smoothness and the nature of picture can be embraced. The visually impaired watermarking plan in view of quick ICA and the wavelet tree structure which expands the security and semi delicate picture watermarking system in view of the shape wavelet and it is acknowledged at the level of substance verification and Arnold change used to build the security. Mohananthini et al. [13] proposed procedure is examination of various watermarking frameworks in light of Discrete Wavelet Change and Specific Regard Breaking down using Innate computation. The SVD-based watermarking figuring's add the watermark information to the singular estimations of the inclining system finishing energy necessities. The upgrade is to expand the execution of PSNR and NC in various watermarking strategies using genetic counts. The various watermarking techniques results of composite watermarking achieve high PSNR when differentiated and dynamic and divided watermarking method. The composite watermarking technique gained more power for sharpening, spot tumult, trim ping, JPEG weight and smoothing. Test comes to fruition watched that the various watermarking methods achieve more power when differentiated and the single watermarking. Najih et al. [14] presented Advanced picture watermarking in light of edge quantization in discrete form let change. Advanced picture watermarking calculation was suggested that is a mix of discrete CT and quantization file tweak calculation and after that taking contourlet, the coefficients are isolated into three quadrants by utilizing the symmetric property of the shape let coefficients, then the edge coefficients are adjusted for each of three focuses. In this strategy PSNR is high that speaks to the high impalpability of the watermarked picture and the standardized connection values right around one shows high vigor for this predefined calculation The outcomes uncover that mix of discrete CT and QIM in watermarking calculations brings about more hearty calculation against assaults. Shen et al. [15] familiar a lone watermark with twofold watermarking this technique watermarks were introduced in both multi assurance and spatial

individual fields. The primary picture was first rotted by 5/3 wavelet deterioration. Pixels with high constrain were browsed medium zone frequencies. Watermarked picture was modified by inverse 5/3 wavelet crumbling. Twofold watermark computation uses the improved pixel based covering model and other is the pseudodiscretionary progression based piece substitution the pixels with high shine is decided to LSB2 substitution with the check to get the last results of watermarked picture. The essential favored outlook of this watermarking is to overcome and hindrance of each individual watermark. Bhatnagar et al. [16] proposed a strong dim scale logo watermarking in wavelet space. The watermark utilized for inserting is a dark scale logo picture, which is considerably littler in size contrasted with the host picture. In the watermark extraction watermark logos are removed and are consolidated by the components expecting that the twists in the encompassing pixels and the level of sub-band of the relating piece. The picture disintegrated into recurrence sub groups utilizing wavelet change installing in chose sub groups of gotten by crisscross arrangement. In this technique the utilized watermark is the 8-bit dim scale logo of size 32×32 and the watermark picture quality measuring PSNR values. The test comes about uncover better visual intangibility to make this against purposeful or un-deliberate assortment of assaults. Rani et al. [17] proposed a picture copyright insurance conspire by scrambling mystery information with the host picture. In this method the utilization of discrete cosine change and particular esteem disintegration to extraction procedure of host picture in the particular space. The copyright insurance plot experiences two stages possession enlistment and proprietorship recognizable proof stage. In the paired logo strategy the mystery key is to be encoded with for host picture for copyright assurance. In this technique it assessed the two measures PSNR and Standardized relationship. Trial comes about demonstrate that the power of the calculation against different signs handling and geometrical attacks. Run-purposeful assortment of assaults. Bhatnagar et al. [18] presented another powerful flexible logo watermarking plan. The required strategy is to enhance the loyalty and nature of the watermarked picture. The technique depended on FRWPT, quadratic deposits and SVD. The strategy is to change have picture utilizing FRWPT by the inserting of watermark in chosen by all sub-groups. SVD is connected to FRWPT sub-groups and a dim scale watermark is inserted by adjusting the particular qualities. The sizes of the first dark scale picture F and dim scale watermark picture are of size $M \times N$ and $m \times n$ ($M \ge m$ and $N \ge n$). The after effects of indistinct watermark and quality are figured by watermarking installing prompts intangible visual corruption of the picture. The exploratory outcomes demonstrate that strength is measured by a few of assaults in this area.

Lei et al. [19] Presented Haar Wavelet Change watermarking calculation for twofold pictures. The calculation used to figure the more flappable pixels in paired pictures instead of basic strategy. Haar wavelet calculation contains two coefficients and in the wavelet change every pixel can be utilized once and no pixel reiteration amid the calculation of the procedure. This strategy figures the change of twofold pictures with the assistance of dynamic stride estimate watermarking can be against different scaling assaults, clamor assaults and JPEG pressure. The strategy can be connected to identify unapproved get to or secure copyright utilization of watermarked parallel pictures and reports like marks, archives, examining and so forth.Bouslimi et al. [20] presented a joint encryption/watermarking calculation with the end goal of ensuring restorative pictures. The watermarking calculation for medicinal pictures in view of the converging of a stream figure calculation. In joint unscrambling/watermarking, watermark inserting is built up amid the decoding procedure. The aftereffects of uprightness and legitimacy with the end goal of confirm the picture dependability in the spatial space and also in the encoded area. The two substitutive strategies ought to be utilized the Slightest Huge Piece substitution Strategy and the Quantization File Regulation. The Trial comes about demonstrate that the strategy gives a high corresponding rate and limiting picture mutilation for ultrasound picture.

Nabhani et al. [21] proposed Powerful watermarking calculation for advanced pictures utilizing discrete wavelet and probabilistic neural system. Discrete wavelet change with a Haar channel to implant a paired watermark picture in chose coefficient pieces. A probabilistic neural system is utilized to extricate the watermark picture in the particular area .The hearty visually impaired watermarking calculation in light of the PNN in the wavelet space. PNN used to keep up the connection amongst watermark and watermarked picture. The PSNR used to quantify the intangibility of the watermark and the watermarked picture. Trial comes about set up that the watermarking calculation indicates watermarked pictures with subjective subtlety and power to normal assaults, for example, JPEG pressure, turn, Gaussian clamor, trimming, and middle channel.

Table 2.Summary the some reported watermarking techniques					
S.N O	Author's name	Techniques Used	Size of Watermark/ Cover Image	Results (Highest values)	
1.	Lie et al.[10]	DCT technique and inform Embedding algorithm	JPEG image 512*512 16*16 binary logo image	PSNR =40.21dB JPEG quality factor =20% Global authentication rate=62.11%	
2.	Hawladar et al.[11]	Fusion of DWT & SVD	Binary Watermark image of size = 128*128 Gray scale lemma image size 256*256	PSNR=38.77dB NC=1	
3.	Karla et al.[12]	DWT and Dual encryption Technique	Watermark image of size =1024*1024	Depth =10% PSNR =33.90dB NC=0.9901	
4.	Mohananthini et al.[13]	DWT and SVD Technique	512 × 512 image sizes of Lena 48 × 48 size color logo	PSNR = 43.8860 dB NC=1	
5.	Najih et al. [14]	contour let transform and DWT & SVD	512 × 512 image of pixels	PSNR= 61.9914 NC = 1.0000	
6.	Shen et al.[15]	DCT and DWT technique	Watermark image of size =512*512 Lena 64*64 logo image of size	PSNR=28.5127dB	
7.	Bhatnagar et al.[16]	DWT technique and Arnold transform	Watermark gray scale logo image of size = 128*128 Gray scale image of size = 512*512	PSNR=41.0695dB JPEG compression ratio=0.9391	
8.	Rani et al.[17]	DCT and SVD technique	Watermark binary logo Image of size 128*128 Gray scale image - 512*512	PSNR=30.17dB NC=0.9954	
9.	Bhatnagar et al.[18]	DWT technique	Gray scale image of size 256*256 8 bit gray scale logo of size 32*32	PSNR =57.7460dB	

Table 2.Summary the some re	ported watermarking techniques
1 abic 2.5ummary the some re	por teu water marking teeningues

10.	Lei et al.[19]	Haar wavelet transform and Wu algorithm	Image size for text =300*300 pixels Image size for picture=384*384 pixels	ELD total /N= 3.5816 for text And 2.5217 for image
11.	Bouslimi et al.[20]	DCT and DWT technique and dual watermarking algorithm	medical ultrasound gray level of size 576*690 pixels 64*64 logo image	PSNR =49.374dB Entropy of encrypted watermarked image=7.9996
12.	Nabhani et al.[21]	DWT technique	512*512 pixels(Lena Barbara and boat) Watermark images (UN logo and cameraman)64*64 pixels	PSNR for Lena=68.27 dB NC=0.9779

CHAPTER 3

A novel technique for text watermarking using LSB

Abstract

The Steganography keeps up the security of data transmitted over the two social events by covering the nearness of the surrendered data. It sets the ensured transmission of the data over the framework. In this method, we uses LSB with Huffman coding to focus the base no. of bits embedded in the required transporter movement remembering the true objective to essential the steganography.

3.1 STEGANOGRAPHY

The expression "inserting" is used to delineate the strategy used by steganography to cover the puzzle data in any intelligent media report, for instance, video, picture, sound, et cetera. The word steganography gets its essentialness from the Greek words "stegos" and "grafia" which imply "cover" and "creating", independently. The idea behind the use of steganography is to cover data that is ought to have been kept puzzle, inside another sort of data with the end goal that no undesired recipient can perceive its proximity or can have passage to it. The impacting frameworks organization range today gives better ways to deal with complete ensured and secure steganography. The interminable framework structure fills in as a quick medium where riddle data is concealed inside media substance like pictures, sound and video using diverse embedding strategies which guarantee transmission of data in an ensured and secure.

a) **Text Steganography**: This kind of steganography is realized by disguising a byte of puzzle data inside the nth letter of each word in the text or file that is being sent as a sight and sound substance or by controlling the substance in the record in courses with the ultimate objective that the control can be used to address the

riddle data. There are different techniques that can be used execute content steganography, for instance, Line Move System, Include Method, Word Move Procedure, and Void region Control Strategy.

- b) **Image Steganography**: For picture steganography, a photo is used as a transporter in which data is embedded. The idea used here is to change the pixel constrains by a minor variable to such a degree, to the point that it can pass on secret data without being on a very basic level deformed. The system used to portray a photo contains broad number of bits which can be changed in accordance with fulfill picture based steganography.
- c) **Video Steganography**: Video is a social event of pictures and a typical video record will have .mov, .mp4, .avi, et cetera development. In this kind of steganography the secret data is concealed in the photos which all in all make a video. The most broadly perceived procedure used to realize it is changing the qualities using discrete cosine change (DCT).
- d) Audio Steganography: This kind of steganography uses sound records, for instance, .mp3, .wav composes as transporters to embed data into. The unmistakable methodologies used to execute this sort are: Low Piece Encoding, Resound Stowing without end, and Spread Range.

3.2 Least Significant Bit

LSB is a spatial space system substitution is standard clear approach to manage embedding being developed in a cover picture. The LSB of some all extraordinary bytes inside a photo is supplanted with bit of shrouded message. The LSB is the easiest spatial area watermarking procedure to install a watermark at all huge bits of some haphazardly chose pixels of the cover picture. Case of minimum noteworthy piece watermarking [25].

Image:

10010101 00111011 11001101 01010101....

Watermark:

1010.....

Watermarked Picture:

10010101 00111010 11001101 01010100.....

The means used to insert the watermark in the first picture by utilizing the LSB:

1) Change over RGB picture to dim scale picture.

2) Make twofold exactness for picture.

3) Move most noteworthy bits to low critical bits of watermark picture.

4) Make slightest noteworthy bits of host picture zero.

5) Include moved adaptation (step 3) of watermarked picture to altered (stride 4) have picture. The primary favorable position of this strategy is that it is effortlessly performed on pictures

3.3 Adaptive Huffman coding: Adaptive Huffman coding which have Huffman tree yet it fabricated the vacant tree toward the start and updations are in like manner when the new image arrives.

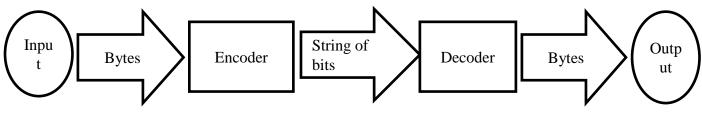


Fig 3 Flowchart for adaptive Huffman coding

3.4 IMPLEMENTATION USING HUFFMAN CODING ALGORITHM

Huffman coding is a quantifiable data pressure method which gives the diminishment in ordinary code length used to address the pictures of letters all together. Huffman coding is a lossless data pressure figuring. This suggests no loss of data happens when this weight estimation is used. Right when Huffman coding is associated with a course of action of data sources, codes of variable length are delivered and distributed to each character of the data set dependent upon their frequencies. To the extent bits, it suggests that lower number of bits is used to encode data that happens more in many cases and more number of bits for data that happens less routinely.

These variable length codes are consigned with the end goal that the code of one character is not the prefix of whatever other character along these lines ensuring no dubiousness happens while decoding the data. The doled out codes are kept in a code book which is made for each photo or a plan of pictures. In order to translate the data the code book ought to be given the encoded data. In figure 3.1 shows the flowchart for Huffman coding.

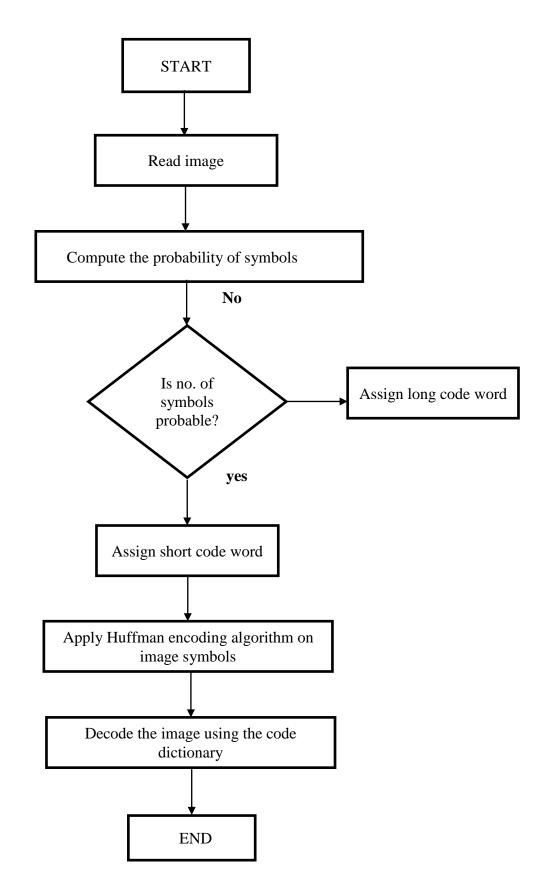


Fig 3.1 Flowchart for Huffman coding

3.5 Algorithm for Data Embedding for huffman coding

Fig 3.2 shows that data embedding algorithm. The major steps for the algorithm are given below:

STEP 1. Read the cover image from the database.

STEP 2. Convert the image in to grey scale format from RGB format.

STEP3. Apply LSB on cover image

STEP4. Enter the text to hide in to the selected cover image.

STEP5. Convert ASCII code conversion of the text.

STEP6. Apply Huffman Encoding on ASCII code of the text data.

STEP7. Convert the ASCII code to the binary format.

STEP 8. Embed binary data of the text watermark into the least significant coefficients of the cover image.

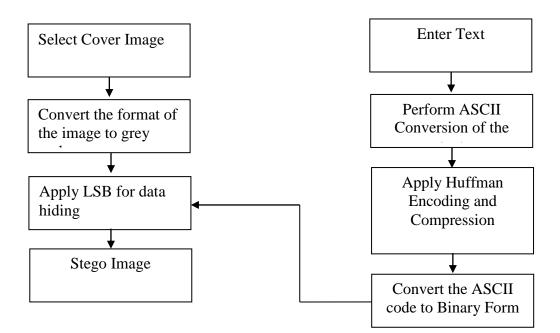


Figure 3.2 Data embedding

3.6 Algorithm for Data Extraction for huffman coding

STEP 1. Select the Stego image.

STEP 2 Apply extraction algorithm using inverse LSB (iLSB) to extract the text watermark.

STEP3. Convert the data to the decimal format.

STEP4. Apply Huffman decoding and decompression technique to the data.

STEP 5.Convert the format of the string.

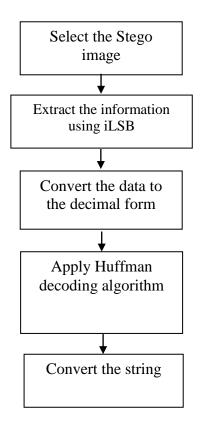


Figure 3. 3 Data extraction

Algorithm steps for data embedding algorithm

Encoding

STEP 1. Input an image from a file:

Temp=Imread ('Image.jpg');

If layer==3;

Image=rgb2gray(temp);

Else

Image=temp;

End

STEP 2.Enter the text to hide in image.

Convert data into uint8

Data=uint8 (double (data));

STEP 3.Perform Huffman encoding

[compress data]=adaptive Huffman (data, 'encoding');

STEP 4.Perform data hiding

STEP 5.Calculate performance parameters:

$$PSNR = 10 \log \left[\frac{255^2}{MSE}\right]$$
(1)

$$BER = Eb/NO$$
(2)

Algorithm steps for Data extraction

Decoding

STEP 1.Perform decoding

[Decode data]= Data_extractor (Image,x,y);

Convert data into uint8

Decode data=uint8(double(decdata));

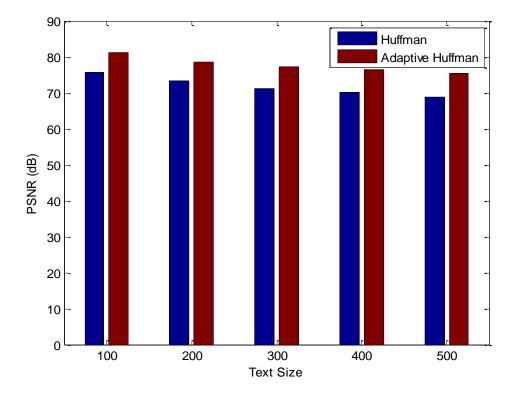
[Info Data]=adaptiveHuffman(DecodeData, 'Decoding');

STEP 2.Decoded Text

The results for the adaptive Huffman and Huffman coding by using different parameters using text size ,image size, and different values of gain factors and other Gaussian ,salt and pepper ,IPEG or resize attacks to. In this table it shows the result with vary with its different text sizes.

S.N	Text Size	BER	PSNR(db)
1.	100.0000	0.0123	81.1411
2.	200.0000	0.0127	78.5583
3.	300.0000	0.0130	77.1835
4.	400.0000	0.0131	76.3518
5.	500.0000	0.0133	75.4444

Table 3. Adaptive Huffman coding with different text size results



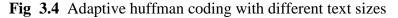


Figure 3.4 represents the graph of the PSNR and BER value with different size of the text with respective to the adaptive Huffman coding. It shows the value of different size of text and it attains the value according to the text size. In this table it shows the text vary with its different text size gives the value of BER and PSNR. The PSNR and BER attains the good results at its quality factors

S.N	Text Size	BER	PSNR(db)
1.	100.0000	0.0132	75.6695
2.	200.0000	0.0136	71.3415
3.	300.0000	0.0141	71.0604
4.	400.0000	0.0143	70.0352
5.	500.0000	0.0145	68.8239

Table 3.1 Huffman coding with different text size results

In the Figure 3.1 the figure represents the value of PSNR and the value of BER values. Which represents the value of different size of text by applying the Huffman coding to the text gets the value of BER and PSNR. In this table it shows the Huffman coding by taking the value of different text size.

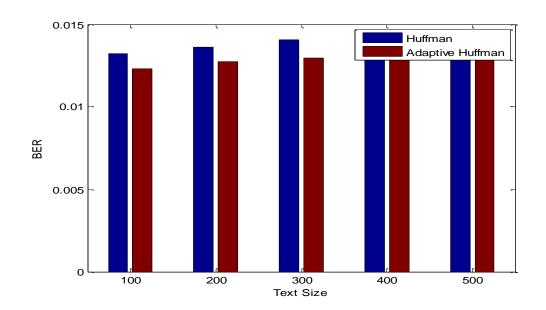


Fig 3.5 Huffman coding with different text of size

S.N	Image Size	BER	PSNR(db)
1.	128 X128	0.0142978	69.9408
2.	256 X 256	0.0129425	77.2647
3.	384 X 384	0.0123948	80.6793
4.	512 X 512	0.0119749	83.5081
5.	640 X 640	0.0117486	85.1163

Table 3.2 Adaptive Huffman coding with different image size results

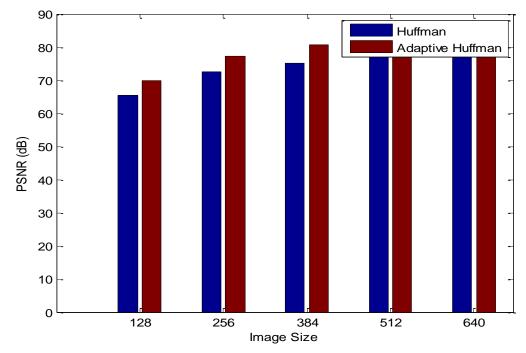


Fig 3.6 Adaptive Huffman with different image size

Table 3.3 Huffman coding with different	image size
---	------------

S.N	Image Size	BER	PSNR(db)
1.	128 X128	0.0152764	65.4606
2.	256 X 256	0.013777	72.5849

3.	384 X 384	0.0133225	75.0607
4.	512 X 512	0.012828	77.9546
5.	640 X 640	0.0126821	78.8511

Figure 3.6 shows the results for Huffman coding by applying Huffman coding and the Table 3.3 shows the value of PSNR and BER at different size of the image and get the better results

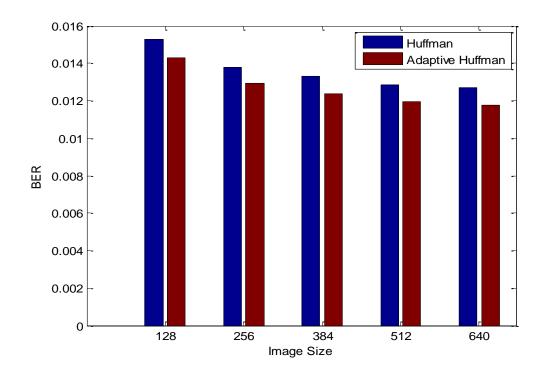


Fig 3.7 Huffman coding with different image size

Table 3.4 Adaptive Huffman with different Attack	S
--	---

S.N	ATTACKS	BER	PSNR(db)
1.	Salt & Pepper	0.0212353	47.0914
2.	Gaussian	0.0367418	27.217
3.	Rotation	0.0332765	30.0512
4.	JPEG	0.0110899	90.172
5.	Resizing	0.0235235	42.5108

Figure 3.7 shows the results for adaptive huffman coding .It represents the performance with different attacks applied on the image.The table 3.4 shows the results of adaptive huffman by applying different attacks to check the performance.

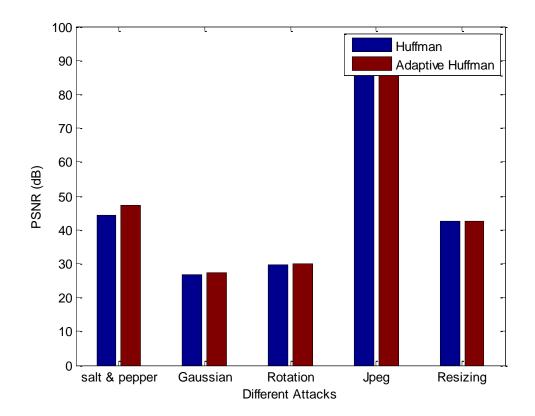


Fig 3.8 Adaptive Huffman with different types attacks

S.N	ATTACKS	BER	PSNR(db)	
1.	Salt & Pepper	0.02264	44.1696	
2.	Gaussian	0.0371914	26.8879	
3.	Rotation	0.0336112	29.752	
4.	JPEG	0.0110899	90.172	
5.	Resizing	0.0235773	42.4137	

Fig 3.8 shows the adaptive Huffman coding by applying different types i.e. Gaussian ,salt and pepper, resizing various type of attacks to show the robustness in the image Figure 3.9 shows the results for huffman coding .Table represents the performance with different attacks applied on the image.

The table 3.5 shows the results of adaptive huffman by applying different attacks to check the performance.

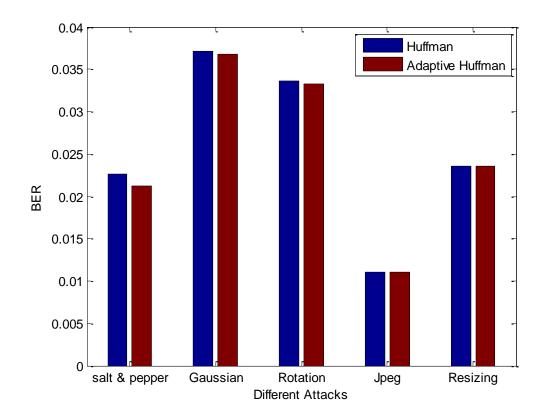


Fig 3.9 Huffman with different types of attacks

Figure 3.9 shows the results for huffman coding .Table represents the performance with different attacks applied on the image.The table 3.5 shows the results of adaptive huffman by applying different attacks to check the performance.

S.N	Gain factor	BER	PSNR(db)
1.	0.1000	0.0139	72.1579
2.	0.2000	0.0142	70.4452
3.	0.3000	0.0146	68.5610
4.	0.5000	0.0153	65.2847
5.	0.7000	0.0159	62.7452

Table 3.6 Adaptive Huffman with different Gain Factor

Figure 3.9 shows the results for adaptive huffman coding at different gain factors and it represents the BER and PSNR .It checks the value of gain factors at different levels

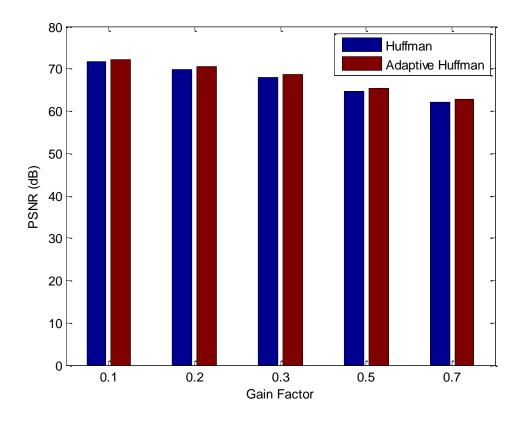


Fig 3.9.1 Adaptive Huffman with different gain factors

Table 3.7 Huffman with different gain factors

S.N	Gain factor	BER	PSNR(db)

1.	0.1000	0.0139	71.6938
2.	0.2000	0.0143	69.9116
3.	0.3000	0.0147	67.9678
4.	0.5000	0.0155	64.6259
5.	0.7000	0.0161	62.0571

Fig 3.9.1 represents the value of gain factors at different levels .It shows the value BER and PSNR by applying Huffman coding .The table 3.7 represents the results of gain factors at different values in terms to check the better results.

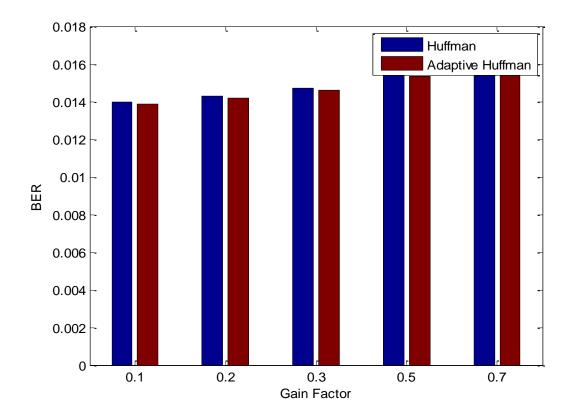


Fig 3.9.2 Huffman v	with different	gain	factors
---------------------	----------------	------	---------

Table 3.8 Adaptive Huffman	with different	size of images
----------------------------	----------------	----------------

S.N	IMAGE	BER	PSNR(db)
1.	Barbara	0.0130288	76.7532

2.	Desert	0.0130919	76.3833
3.	Lena	0.013192	75.8034
4.	Penguin	0.0129425	77.2647

Figure 3.9.2 represents the adaptive Huffman by applying the different size of images. Table 3.8 represents the different images and its values in terms of BER and PSNR. In this table it uses the various images to check e.g. Barbara PSNR 76.7532 shows better results using adaptive Huffman coding.

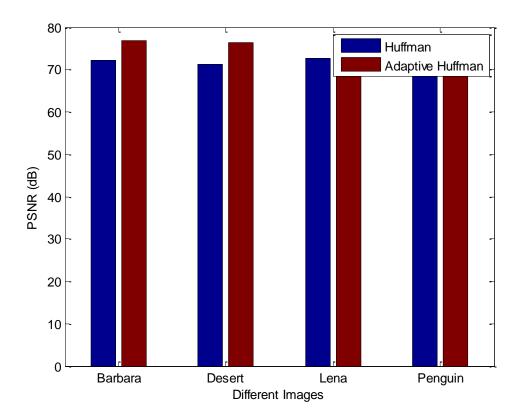


Fig 3.9.3 Adaptive Huffman with different size of images

S.N	IMAGE	BER	PSNR(db)
1.	Barbara	0.0138479	72.2132

2.	Desert	0.0140309	71.2713
3.	Lena	0.0137485	72.7353
4.	Penguin	0.013777	72.5849

Figure 3.9.3 represents the value of different images in order to shows the values of PSNR and BER.Table 3.9 shows the results by using different images of size to calculate the BER and PSNR.

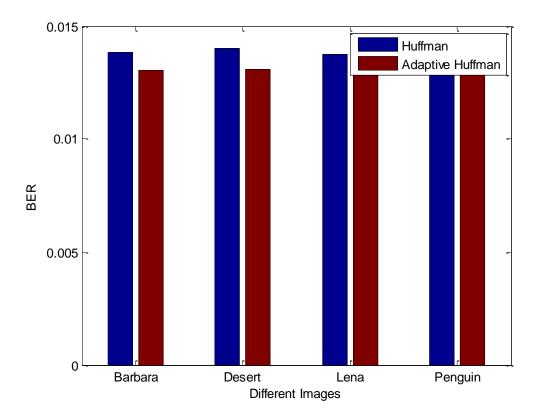


Fig 3.9.4 Huffman with different size of image

S.N	Text size	Adaptive Huffman coding		Huffman coding	
		BER	PSNR(db)	BER	PSNR(db)

1.	100.0000	0.0123	81.1411	0.0132	75.6695
2.	200.0000	0.0127	78.5583	0.0136	71.3415
3.	300.0000	0.0130	77.1835	0.0141	71.0604
4.	400.0000	0.0131	76.3518	0.0143	70.0352
5.	500.0000	0.0133	75.4444	0.0145	68.8239

Table 3.10. Comparison between Adaptive Huffman and Huffman coding text size

Table 3.10 shows the comparison between adaptive Huffman and Huffman the comparison value of PSNR in adaptive is greater than Huffman coding for vary in text size

Table 3.10 shows the difference between adaptive Huffman and Huffman coding by using the same size of text.

Table 3.10 shows the result for both BER and PSNR in terms of adaptive and Huffman coding to shows the better results. Adaptive Huffman uses the better results as compared to Huffman coding to calculate the value of BER and PSNR.

Table 3.11 shows the comparison between Adaptive and Huffman coding by taking the Different image size and check the value of BER and PSNR.It checks the images of different size. Adaptive Huffman shows better results than Huffman coding. In terms to check the performance.

S.N Image size	Image size	Adaptive Huffman coding		Huffman coding	
	BER	PSNR(db)	BER	PSNR(db)	
1.	128×128	0.0142978	69.9408	0.0152764	65.4606
2.	256 ×256	0.0129425	77.2647	0.013777	72.5849
3.	384×384	0.0123948	80.6793	0.0133225	75.0607

Table 3.11 Comparison between Adaptive Huffman and Huffman coding Image size

4.	512×512	0.0119749	83.5081	0.012828	77.9546
5.	640×640	0.0117486	85.1163	0.0126821	78.8511

Table 3.12 Comparison between Adaptive Huffman and Huffman coding of different type of attacks

S.N	Attacks	Adaptive Huffman coding		Huffman coding	
		BER	PSNR(db)	BER	PSNR(db)
1.	Salt & Pepper	0.0212353	47.0914	0.02264	44.1696
2.	Gaussian	0.0367418	27.217	0.0371914	26.8879
3.	Rotation	0.0332765	30.0512	0.0336112	29.752
4.	JPEG	0.0110899	90.172	0.0110899	90.172
5.	Resizing	0.0235235	42.5108	0.0235773	42.4137

Table 3.12 shows the comparison between the various attacks salt and pepper and Gaussian and other JPEG in order to check the robustness of the image at both parts it shows the robustness method when different methods applied on the image. Comparison shows the performance of Adaptive is better than Huffman coding in the given results.

S.N	Gain Factor	Adaptive Huffm	Adaptive Huffman coding Huffman coding			
		BER	PSNR(db)	BER	PSNR(db)	

Table 3.13 Comparison of Adaptive Huffman and Huffman coding at different gain factors

		_			_
		BER	PSNR(db)	BER	PSNR(db)
1.	0.1000	0.0139	72.1579	0.0139	71.6938
2.	0.2000	0.0142	70.4452	0.0143	69.9116
3.	0.3000	0.0146	68.5610	0.0147	67.9678
4.	0.5000	0.0153	65.2847	0.0155	64.6259
5.	0.7000	0.0159	62.7452	0.0161	62.0571

Table 3.13 shows the comparison between both adaptive and Huffman coding .In order to calculate the difference between in terms of gain factor at both coding techniques.

S.N Image		Adaptive Huffman coding		Huffman coding	
		BER	PSNR(db)	BER	PSNR(db)
1.	Barbara	0.0130288	76.7532	0.0138479	72.2132
2.	Desert	0.0130919	76.3833	0.0140309	71.2713
3.	Lena	0.013192	75.8034	0.0137485	72.7353
4.	Penguin	0.0129425	77.2647	0.013777	72.5849

Table 3.14 Comparison between Adaptive Huffman and Huffman coding with different size of images

Table 3.14 shows the comparison between adaptive and Huffman coding with different size of images. It shows the results of BER and PSNR. Adaptive Huffman coding shows the better results as compared to the Huffman coding by applying different images to illustrate the performance.

Figure 3.9.5 shows (a) cover image (Barbara) (b) adaptive Huffman (Barbara) (c) Huffman coding (Barbara)

Results

Figure 3.9.6 shows (a) cover image (Desert) (b) adaptive Huffman (Desert) (c) Huffman (Desert)





(b)



(a)

Figure 3.9.5 (a) cover image(Barbara) (b) stego image adaptive huffman (Barbara) (c)stego image huffman (Barbara)



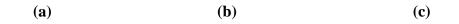


Figure 3.9.6 (a) cover image(Desert) (b) stego image adaptive huffman (Desert) (c)stego image huffman (Desert)



Figure 3.9.7 (a) cover image(Lena) (b) stego image adaptive huffman (Lena) (c) stego image huffman (Lena)

Results

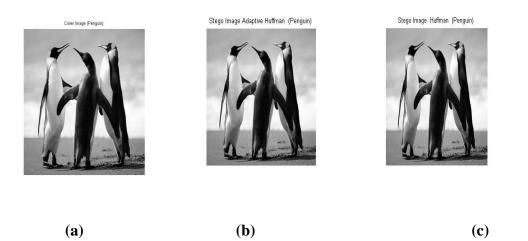


Figure 3.9.8 (a) cover image (Penguin) (b) stego image adaptive huffman (Penguin) (c) stego image huffman (Penguin)

CHAPTER 4 Implementation

4.1 About MATLAB

Short for matrix laboratory" developing MATLAB in the late 1970s by Cleve Moler, the chairperson of the computer science department at the University of New Mexico. He give the entrance to the two understudies LINPACK and EISPACK without them learning FORTRAN. MATLAB soon spread to different colleges and found a solid gathering of people and individuals inside the connected arithmetic group. These revised libraries were known as JACKPAC. In 2000, MATLAB was changed to utilize a more current arrangement of libraries for framework control.MATLAB used in various fields of education, in particular associated with the linear algebra and various mathematical and as well as numerical operations of mathematics.

MATLAB code sometimes called M –code or simply M.The simple way is to execute MATLAB is to type at the prompt >>, in the command window, one of the elements in the desktop. In this way MATLAB can be used as an interactive mathematical or programming shell.

There are various windows in MATLAB

- a) Editor window
- b) Command window
- c) Command history
- d) Workspace
- e) Command history

Editor window is used for coding command window to display output and Command window is used to display output.

Table 4.Commands for managing Variables

Command	Description
clear	Removes all variables from the memory.
clear x, y, z	Clears/removes only variables \mathbf{x} , \mathbf{y} and \mathbf{z} from the memory.
who	Lists the variables currently in the workspace

4.2 Introduction to the Digital Image

A Digital picture is a made out of pixels which can be considered as little spots on the screen .A computerized picture is a direction to how to shading every pixel.

How about we have a picture of arrangement 512-by-1024 pixels .This implies the information for the picture must contain data around 524288 which requires typically a considerable measure of memory space. Subsequently compacting picture is basic for better outcomes for the picture preparing

4.3 The following image formats in MATLAB

- a) .BMP (Microsoft Windows Bitmap)
- b) .HDF (Hierarchical Data Format)
- c) .JPEG (Joint Photographic Experts Group)
- d) .PCX (Paintbrush)
- e).TIFF ((Tagged Image File Format)
- f) .PNG (Portable Network Graphics)

4.4 WORKING FORMAT IN MATLAB

At the point when a picture is put away as JPEG picture we initially read it into MATLAB .so as to begin working with in a picture. For instance perform Wavelet change on the picture we should need to change over into various configurations.

a) Intensity image (gray scale image)

It speaks to the picture as a network where each component has an esteem comparing to how brilliant/dark the pixel at the relating position ought to be colored. There are two approaches to speak to the number that speaks to the splendor of the pixel. The twofold class in the vicinity of 0 and 1 to every pixel. The esteem 0 compare to dark and esteem 1 relate to white

b) Binary image

This picture design likewise stores a picture as a framework however can just shading a pixel dark or white.it doles out 0 for dark and 1 for white.

c) Indexed image

A filed picture store a picture as two networks .the primary lattice is same size as the picture and other one number for each pixel. The second framework is known as the shading guide and its size be unique in relation to the picture.

d) **RGB image**

This is the another organization to shading pictures .it speaks to the picture three grid of size coordinating the picture design Each framework compares to one of the hues Red green and blue.

e) Multi frame image

This is extremely basic which is utilized as a part of medicinal and natural imaging where you may concentrate an arrangement of cell.

4.5 Principal operations

The accompanying table demonstrates to change over between various arrangements. Every one of the summons utilizing picture handling tool kit.

The mat2gray is helpful on the off chance that you have grid speaking to a picture however the esteem speaking to the dark scale running in the vicinity of 0 and 1000.

Table 4.1 Functions for image format conversion

S.N.	Operations	MATLAB commands
1.	Convert between intensity /indexed /RGB format to binary format	Dither()
2.	Convert between intensity format to indexed fomat	Gray2ind()
3.	Convert between indexed format to intensity format	Ind2gray()
4.	Convert between indexed format to RGB format	Ind2rgb()
5.	Convert regular matrix to intensity matrix by scaling	mat2gray()
6.	Convert between RGB format to indexed format	rgb2ind()
7.	Convert between RGB format to intensity format	Rgb2gray()

4.6 Conversion between double and uint8

When you store a picture, you ought to store it as uint8 picture since this requires far less memory than twofold .When you are handling a picture you change over into it twofold

I=im2double(I); Converts a picture named I from Uint8 to twofold.

I=im2uint8(I);Converts a picture named I from twofold to uint8.

Loading and sparing factors in MATLAB

In this clarifies how stacking and putting away factors in MATLAB it is done through charges spare and load.

S.NO.	OPERATION	MATLAB COMMAND
1	Save the variable X	Save X
2	Load the variable X	Load X

Table 4.2 Saving and loading variables in MATLAB

4.7 Some limitations

The dialect demonstrates a blended legacy with at times whimsical language structure.

For example in MATLAB the DFT is characterized with the DC part at file 1 rather than file 0.which is not reliable with the standard meaning of DFT.

MATLAB doesn't bolster references which make it hard to actualize information structures that contain indirections, for example, hash tables, connected records tress and different other basic software engineering information structures.

CHAPTER 5

Conclusion and Future direction

The essential part of this strategy is to give three levels of security, rather than covering the message bits particularly in cover picture, pixels are made subjectively through pseudo discretionary number generator after that riddle data is concealed behind a cover picture using modified LSB strategy. Trial consider raises that the proposed structure is better than basic LSB technique with respect to higher visual quality as appeared by the high PSNR advantages of covering radiate message bits in the photo in this way diminishes the likelihood of the private message being distinguished and engages secret correspondence. For future work we will create discretionary number through cell automata as further securing system and use other sort of cover-question for hiding the data. In this we uses the Huffman and adaptive Huffman to check in the various size of domains. Supplementing the riddle message, second by stowing ceaselessly supplemented puzzle message in cover picture pixels that are picked self-assertively by using pseudo subjective number generator, third by using modified piece LSB method as stenographic framework rather than clear LSB, thusly, diminishes the shot of the covered message being recognized. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two essential quality estimations to check qualification between the cover-picture and the stego-picture.

Chapter 1 presents the basic concepts of data hiding techniques and their importance in recent applications. Characteristics of watermarking system, major classifications of watermark and define the peak-signal-to noise ratio (PSNR), bit error rate (BER) as some metrics to determine the performance of the watermarking method (s) are also described in this chapter. Watermarking techniques are divided into spatial and transform domain techniques. Various spatial, transform domain techniques are described briefly in this chapter.

Chapter 2 presents the state-of-the-art watermarking methods and compares the performance of some recent techniques in tabular form.

In chapter 3, we have proposed a watermarking algorithm based on LSB and Huffman compression technique using text watermark. The performance of the method is tested in terms of PSNR and BER. The method is also robust for different attacks.

The introduction of our simulation tool (MATLAB) and its important functions are presented in Chapter 4.

Conclusion and future directions of the work is presented in Chapter 5.

LIST OF PUBLICATION

From this thesis work I have submitted by one of paper in the publication

(1)Neha sharma ,Amit Kumar Singh "Information Hiding Techniques for Consumer Applications –A Technical Survey", International conference on innovations and development in Mechanical Engineering"(Accepted)

References

[1] Sumit Kumar Prajapati, Amit Naik , Anjulata Yadav, "Robust Digital Watermarking using DWT-DCT-SVD"International Journal of Engineering Research and Applications (IJERA) Vol. 2, 2012.

[2]Aniruddha Singh,Abhishek Vaish, Pankaj Kumar Keserwani "Issues and Challenges of Wireless Networks" International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4 February 2014.

[3] Chauhan Usha, Singh Rajeev Kumar," Digital Image Watermarking Techniques and Applications", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, March 2016.

[4] Vaishali, Priyanka, "A Survey: Digital Image Watermarking Techniques", International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 05; May 2016.

[5] Sandeep Kumar Jatav ,Dhiiraj Nitnawre, "Performance Analysis of various Image Watermarking Techniques using different Image Quality Parameters"International Journal of Computer Applications, Volume 102 September 2014.

[6] Gaurav Chawla, Ravi Saini, Rajkumar Yadav, "Classification of Watermarking Based upon Various Parameters" International Journal of Computer Applications & Information Technology Vol. I, September 2012.

[7] Lalit Kumar Saini, Vishal Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications" (IJCST) Volume 2, May-Jun 2014.

[8]Md. Maklachur Rahman, "A DWT, DCT AND SVD based Watermarking Technique To Protect the image piracy". International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT) Vol. 4, June 2013.

[9]Mohan Durvey, Devshri Satyarthi, "A Review Paper on Digital Watermarking"International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Volume 3, August 2014

[10] Wen-Nung Lie, Member, IEEE, Guo-Shiang Lin, and Sheng-Lung Cheng, "Dual Protection of JPEG Images Based on Informed Embedding and Two-Stage Watermark Extraction Techniques" IEEE Transactions on information forencies and security Vol.1 No.3 September 2006.

[11] Md. Abul Kayum Hawlader, Md. Moniruzzaman and Md. Feisal Hossain, "SVD Based Robust and Secure Dual Stages Watermarking Scheme for Copyright Protection" Khulna University of Engineering and Technology, IEEE 2014.

[12]Gursharanjeet Singh Karla, Dr. Rajneesh Talwar, Dr. Harsh Sadawarti, "Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique", International Conference on Computational Intelligence, Communication Systems and Networks, IEEE 2011.

[13] N. Mohananthini, G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms", Journal of Electrical Systems and Information Technology 3 2016.

[14]Abdulmawla Najih, S.A.R.Al-Haddad, Abd Rahman Ramli,S.J. Hashim, Mohammad Ali Nematollahi, "Digital image watermarking based on angle quantization in discrete contourlet transform" Journal of King Saud University Computer and Information Sciences 2016.

[15] Hong Shen, Bo Chen, "From single watermark to dual watermark: A new approach for image watermarking" China Electronics Technology Group Cooperation, China, Elsevier 2012.

[16]Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "Robust grayscale logo watermarking in wavelet domain", University of Windsor, Ontario, Canada, Computer Electr Eng. 2012.

[17]Asha Rani,Balasubramanian Raman, "An image copyright protection scheme by encrypting secret data with the host image" Multimedia Tools Applications Springer Science Business Media New York 2014.

[18] Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "A new robust adjustable logo watermarking scheme", University of Windsor, Windsor, Ontario, Canada, Computer Electrical Eng. 2012.

[19] Ju Lei, Sui Zhiyuan, ChiYaping, FangYong "A Haar Wavelet Transform Based Watermarking Algorithm for Binary Images", Beijing Electronic Science and Technology Institute china, ESEP 2011.

[20] Dalel Bouslimi, Gouenou Coatrieux, Christian Roux,"A joint encryption/watermarking algorithm for verifying the reliability of medical images Application to echo graphic images",Telecom Bretagne, Department Image et Traitement Information, France 2012.

[21] Yahya AL Nabhani, Hamid A. Jalab , Ainuddin Wahid, Rafidah Md Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network", Journal of King Saud University – Computer and Information Sciences 2015. [22] Mohan Durvey and Devshri Satyarthi, "A Review Paper on Digital Watermarking," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014, pp. 099-105.

[23] Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil and Teddy surya Gunawan, "Properties DigitalImage Watermarking," IEEE 9th International Colloquium on Signal processing and its Applications, 8-10 Mac. 2013, kuala Lumpur, Malaysia, pp. 235-240.

[24] Pooja Mishra and Biju Thankachan, "Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique," International Journal of Science and Research (IJSR), India, Volume 2 Issue 7, July 2013, pp. 347-350.

[25]Frank Hartung and Martin kutter, "Multimedia Watermarking Techniques," Proceedings of the IEEE, Volume. 87, No. 7, July 1999, pp. 1079-1107.

[26] Mrugesh Prajapati "Transform Based Digital Image Watermarking Techniques for Image Authentication,"International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 5, May 2014, pp. 144-151.

[27]Mohan Durvey and Devshri Satyarthi, "A Review Paper on Digital Watermarking," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014, pp. 99-105.

[28] Saraju P. Mohanty "Digital Watermarking : A Tutorial Review," IIT Banglore, 1999, pp. 1-24.

Ming Yang, Nikolaos Bourbakis and Shujun Li, "Data, Image and Video Encryption" IEEE POTENTIAL, Vol. 23, Issue. 3, August/September 2004, pp. 28-34.

[29]R. Gayathri and Dr. V. Nagarajan, "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme," IEEE ICCSP conference, 2015, pp.0118-0123.

[30]B. Nassiri, R.Latif, A.Toumanari and F.M.R. Maoulainine, "Secure transmission of medical images by watermarking technique," IEEE International Conference on Complex Systems (ICCS), 2012, pp. 1-5.

[31]Madhuri Rajawat and D S Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT," IEEE Fifth International Conference on Communication Systems and Network Technologies, 2015, pp.638-642.

[32]Md. Moniruzzaman, Md. Abul Kayum Hawlader and Md. Foisal Hossain, "Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication," IEEE 17th International Conference on Computer and Information Technology (ICCIT),2014, pp.374-378.

[33] Saeid Bakhtiari et al. in [5], "JPEG Image Encryption with Elliptic Curve Cryptography," IEEE International Symposium on Biometrics and Security Technologies (ISBAST),2014, pp. 144-149.

[34]Preeti Gupta in, "Cryptography based digital image watermarking algorithm to increase security of watermark data," International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012, pp. 1-4.

[35]Jasdeep Singh Bhalla and Preeti Nagrath, "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm," International Journal of Scientific & Engineering Research Publications, Volume 3, Issue 4, April 2013, pp. 1-6.

[36]Sukhpal Kaur and Madan Lal, "An Invisible Watermarking Scheme Based on Modified Fast Haar Wavelet Transform and RSGWPT," Proceedings of IEEE 2015 RAECS UIET Panjab University Chandigarh 21-22nd December 2015, pp. 1-5.

[37]Ali Al-Haj, Noor Hussein and Gheith Abandah, "Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images" IEEE 2nd International Confrence on Information Management (ICIM), 2016, pp. 40-46.

[38] Mohamed OUSLIM, Ahmed Sabri and Hassan MOUHADJER, "Securing biometric data by combining watermarking and cryptography" IEEE 2nd International Conference on Advances in Biomedical Engineering, 2013, pp. 179-182.

[39]Anusree K and Dr Binnu G S "Biometric Privacy using Visual Cryptography, Halftoning and Watermarking for Multiple Secrets" IEEE National Confrence on Communication, Signal Processing and Networking (NCCSN), 2014, pp. 1-5.

[40]Yanyan Han, Wencai He, Shuai Ji and Qing Luo,"A Digital Watermarking Algorithm of Colour Image based on Visual Cryptography and Discrete Cosine Transform" IEEE Ninth International Conference on P2P, Parallel Grid, Cloud and Internet Computing, 2014. pp. 527-530.

[41]Sudip Ghosh, Sayandip De, Santi Prasad Maity and Hafizur Rahaman, "A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography Using Extended Hamming Code" IEEE Proceedings of International Conference on Electrical Information and Communication Technology (EICT 2015), 2015, pp. 167-172.

[42]Sanjay Kumar and Ambar Dutta"A Novel Spatial Domain Technique for Digital Image Watermarking Using Block Entropy" IEEE Fifth International Conference on Recent Trends in Information Technology, 2016, pp. 1-4.

[43]Meeta Malonia and Surendra Kumar Agarwal, "Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression" IEEE Students's Conference on Electrical, Electronics and Computer Science (SCEECS), 2016, pp. 1-6.

[44]Pooja Dabas and Kavita Khanna "A Study on Spatial and Transform Domain Watermarking Techniques," International Journal of Computer Applications (0975 – 8887) Volume 71– No.14, May 2013, pp. 38-41.

[45]Preeti Parashar and Rajeev Kumar Singh, "A Survey: Digital Image Watermarking Techniques,"International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 7, No. 6,2014, pp. 111-124.

[46]Amit Kumar Singh, Nomit Sharma, Mayank Dave and Anand Mohan "A Novel Technique for Digital Image Watermarking in Spatial Domain," 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 497-501.