A Detailed Survey of Image Steganography Methods

Dayabati Markam
Computer Science and Engineering
TIEIT, RGPV, Bhopal, India

Devashri Deoskar
Computer Science and Engineering
TIEIT, RGPV, Bhopal, India

Amit Saxena
Computer Science and Engineering
TIEIT, RGPV, Bhopal, India

ABSTRACT
Security systems are very popular in many places because technology is getting better and better every day. Information security can be achieved by utilizing encryption and steganography. Cryptography is typically associated with scrambling plain text into cipher ext and back again in today's world. Maintaining the safety of confidential information has always been a major concern, from ancient times to the present. As a result, numerous methods for securely transferring data were developed, one of which is steganography. Steganography takes cryptography one step further by concealing an encrypted message so that no one is aware of its existence. The primary goal of Steganography is to conceal the embedded data's existence. Due to the remarkable advancement in computational power, the steganography technique has enhanced the security of existing methods for hiding data. Steganography system fundamentals, evaluation methods, and security aspects, as well as various spatial and transform domain embedding schemes, are discussed in this article. In addition, a brief overview of various image steganography methods is provided in this paper.

Keywords
Image, steganography, cryptography, DWT, DCT, DWT, IFT, LT

1. INTRODUCTION
Steganography alludes to the approaches to disguising a mystery message into a cover message in a way that its presence is totally covered up [1]. The mystery message can be as a plain text, a image, a code message, or anything which can be addressed as a piece [2]. Once in a while, the implanting system is defined by a stego key (secret key) which should be realized before the mystery message can be recognized and removed. When a message is concealed in a cover message, it is alluded to as a stego-object. Figure 1.1 portrays a general steganographic model [3]. Prior to implanting data in a cover, the source should initially change the mystery message, and afterward control a portion of the pieces of the cover object to shape the stego-object. Process includes a mystery key, the two players (shipper and collector) should have the key preceding the transmission of the stego-object. Watermarking and fingerprinting are the two different strategies that are connected with steganography; however they are not in similar class as they mostly guarantee the security of licensed innovation [4]. Hence, watermarking, fingerprinting, and steganography vary in strength, application and concealing limit. Steganography is by and large utilized in the correspondence of mystery and when complete opportunity is wanted. Correspondence security is vital in both rebuffed and checked environmental factors. Confidential interchanges which can't be gotten through cryptography can be gotten with steganography [5]. In any case, the utilization of steganography with other security systems for the arrangement of layered security as a gatecrasher who prevails at one layer is as yet expected to sidestep different levels to find success. Correspondences in the military and knowledge fields require no block; even with content encryption, the discovery of a sign can bring about an assault on the source on a cutting edge war zone. Such signals can be concealed through steganography. Data that isn't expected to be imparted to anybody can likewise be put away utilizing steganography [6].

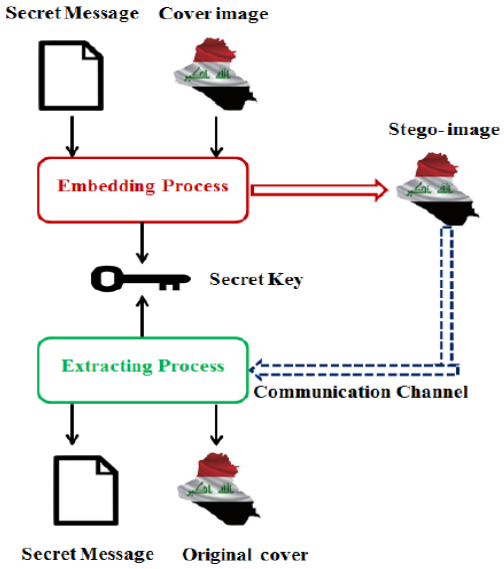

Fig 1.1: Steganography Process.

The stego-object is then sent to the intended recipient via a communication medium. After it is received, the process is reversed to get the hidden information. If additional sensitive information, such as banking data, can be stored on a private computer and concealed in a cover object [7]. To guarantee the safety of data, various steganographic algorithms have been implemented. It is important to keep in mind that not all steganography systems use secret keys; however, applying the Kirchhoff principle can improve the security of steganographic systems. The idea is that an intruder must have the secret key to successfully attack the steganographic system, even if they are aware of its design and implementation. Therefore, when implementing steganographic systems, it might be prudent to incorporate the secret keys—public or private.

As the area of steganography is tremendous, we have confined ourselves to image and video steganography and steganalysis just [8]. The following segment talked about the cutting edge of image and video steganography methods in light of most recent five years writing. The principal point of a steganography strategy is to hide the presence of the information without debasing the nature of the cover object. The fundamental advances associated with the steganography (image/video) method are displayed in the figure 1.2.

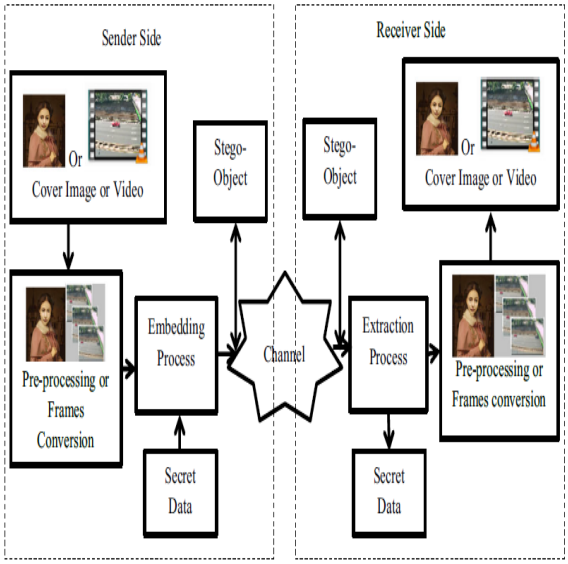

Fig 1.2: Block diagram of steganography process.

2. BASIC REQUIREMENTS FOR STEGANOGRAPHY

A decent steganography strategy or instrument ought to satisfy the essential prerequisites of a steganography framework which incorporates subtlety, limit, heartiness and security. Moreover, there exist different necessities likewise for an improved method, for example, reversibility, encryption, computational intricacy and so on. The fundamental prerequisites are characterized as follows [9]-

2.1 Invisibility

Imperceptibility most importantly, a steganographic procedure should be undetectable, taking into account the point of steganography is to battle off undesirable consideration regarding the transmission of stowed away data. On the off chance that the natural eye thinks that data is covered up, this objective is crushed. In addition, the disguised data might be compromised.

2.2 Imperceptibility

Indistinctness Impalpability alludes to the nature of the stego-objects subsequent to implanting, for example the undetectable corruption of the stego-object. It is the key component of any steganography procedure for concealing restricted information inside a cover object.

2.3 Capacity

Limit or payload alludes to the greatest measure of data concealed in a cover media without visual mutilation. An effective steganography strategy generally has high implanting limit. In any case, high implanting limit some of the time brings about bad quality of the stego-object, which eventually prompts visual mutilation. In this way, a high implanting limit method ought to constantly accept subtlety as one of the primary elements to be analyzed.

2.4 Robustness

Power Strength is one of the fundamental necessities of the steganography procedure. It alludes to the steganography strategy or apparatus strength against assaults. The need of power is on the grounds that occasionally while transmission a few obscure goes after, for example, commotion, scaling, revolution, pressure and so on diminish the nature of the stego-object which prompts the deficiency of mystery message. There is dependably a compromise between limit, intangibility and power, so while fostering a fruitful or productive steganography procedure or device, it should be thought about.

2.5 Security

One more primary component of a fruitful steganography procedure is security, which alludes to the opposition of the stego-objects against steganalysis methods. Thus, a protected steganography procedure is one in which restricted information isn't discernible using any and all means, for example neither by factual instruments nor by the strategies. The point of the steganography strategy is to send data safely over the uncertain transmission channel without admittance to an unapproved individual or framework.

2.6 Reversibility

Reversibility alludes to the specific recovery of cover and privileged information after transmission at the recipient's side. This is essentially utilized in the applications where the lossless recovery of data is required, like in clinical and military applications.

2.7 Encryption

Encryption is utilized to give extra security to the stego-object, which is typically finished by encoding the restricted information utilizing some encryption plan, for example, AES, RSA and so on calculations. Encryption of the restricted information is finished prior to inserting it into cover object. Likewise, in some cases to additionally work on the security, the stego-object is additionally encoded.

2.8 Computational Complexity

Computational Intricacy as far as reality of the steganography procedure or instrument ought to likewise be thought about while fostering another strategy or apparatus. Be that as it may, with the improvement of very good quality processors and supercomputers, the registering power can be expanded.

2.9 Independency from file format

As there is an overflow of different image document designs being utilized on the web, it might draw undesirable doubt that a singular kind of document design is over and again imparted between two gatherings. Be that as it may, assuming a stenographic calculation is strong it ought to have the capacity to implant data in a wide range of record designs.

3. IMAGE STEGANOGRAPHY TYPES

3.1 Text steganography

In this strategy the privileged information can be taken cover behind any message document which can be sent across an unstable channel [10].

Example- Plain Message, which is to send is - Since Evan Can Run, Encoding Text

Unique Message-Since Evan Can Run, Encoding Message

Secret Message-SECRET

3.2 Audio Steganography

In sound steganography strategy restricted information can be taken cover behind any sound media displayed in Figure 1.3

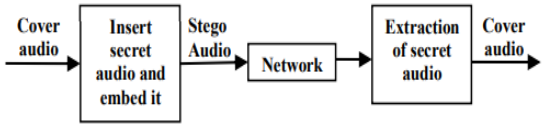

Fig 1.3: Example of audio Steganography.

By and large two kinds of sound are utilized in this procedure. One sound document goes about as cover media while another record is secret message.

3.3 Video Steganography

In this method the privileged information can be taken cover behind a video record with the goal that a lot of data can be taken cover behind as displayed in figure 1.4.

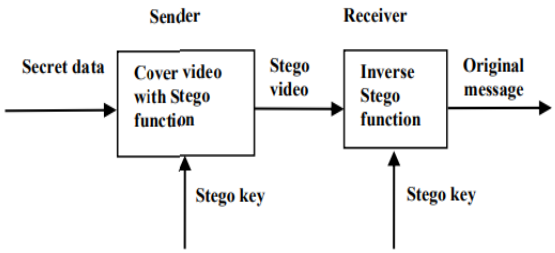

Fig 1.4: Example of video Steganography.

3.4 Image Steganography

In this procedure the restricted information can be taken cover behind any cover image. Secret data exist in text or image structure. Subsequent to inserting the stego image is produced this can be moved over an unstable channel. Figure 1.5 is showing the Image Steganography process [11].

Fig 1.5: Example of image Steganography.

4. DIFFERENCE IN CRYPTOGRAPHY & STEGANOGRAPHY

Cryptography keeps unapproved party from finding the substance of correspondence however Steganography forestalls disclosure of the presence of correspondence (i.e., Cryptography spreads the word about data nonsense and the message passing while Steganography will in general disguise presence of stowed away data and obscure the message passing) [12]. A relative examination of Encryption and Steganography is given in table 1.

Table 1: A comparison Between Cryptography and Steganography

Criteria/Method	Cryptography	Steganography
Objective	Data protection	Secret communication
Input	One	At least two
Output	Cipher tex	Stego file
Key	Necessary	Optional
Carrier	Usually text	Text , Message , Audio , Video , Protocol and DNA
Security Service	Authentication, Confidentiality, Identification, Data Integrity and Non-repudiation	Authentication, Confidentiality, Identification
Visibility	Always	Never
Type of attacks	Cryptanalysis	Steganalysis
attacks	Broken when aggressor can grasp the mystery message. known as Cryptanalysis	Broken when aggressor uncovers that steganography has been utilized, known as Steganalysis
Naked eye	Yes, The secret	No, The secret
identification	message will convert in another way	message will hide within the cover image (Carrier).
Fails	de-ciphered	When it is detected
Secret data	Plaintext	payload
Applications	Information security	Information security
Technology-specific problems	Key distribution	Key distribution (except with keyless

5. A HYBRID COMBINATION OF CRYPTOGRAPHY & STEGANOGRAPHY

Steganography and cryptography have been noted to be independently deficient for complete data security; hence, a more solid and solid component can be accomplished by joining the two strategies [13]. Consolidating these systems can guarantee a better restricted intel security and will meet the prerequisites for security and heartiness for communicating significant data over open channels. Figure 1.6 presents a methodology for the mix of the two strategies.

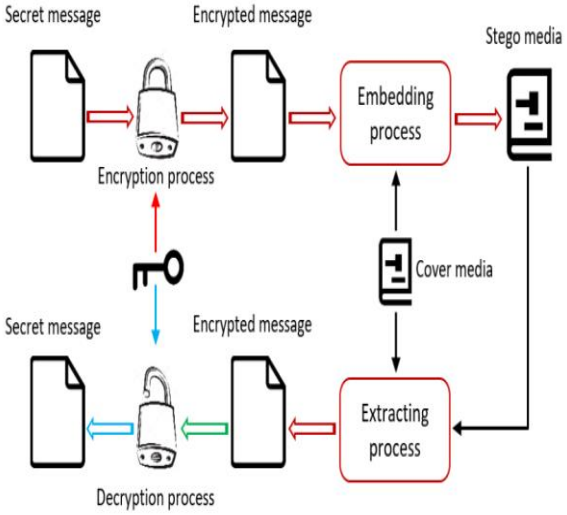

Fig 1.6: Basic diagram of combining steganography and cryptography.

It is noticed that steganography or cryptography alone is deficient for the security of data in all situations. Nonetheless, assuming we join these frameworks, we can produce more dependable and solid frameworks [14]. The mix of these two procedures will work on the security of the restricted intel. This mix will satisfy a few wanted highlights, similar to: memory use, security, and strength for delicate data transmission across an open channel. Likewise, it will be a strong component which empowers individuals to impart without hauling the consideration of busybodies who doesn't actually know about the presence of the privileged intel being sent [15].

6. VARIABLES INCLUDED IN STEGANOGRAPHY

The adequacy of steganography procedure not set in stone by contrasting cover-image and the stego Image [16]. The different variables are:

4.1 Robustness

Vigor alludes to the capacity of inserted information to stay in salvageable shape if the stego-image goes through transformations, like straight and non-direct sifting, honing or

obscuring, expansion of irregular commotion, pivots and scaling, editing or annihilation, lossy pressure.

4.2 Imperceptibility

The subtlety implies imperceptibility of a steganography calculation. Since it is the above all else prerequisite, since the strength of steganography lies in its capacity to be unseen by the natural eye.

4.3 Bit Error Rate

The secret data can be effectively recuperated from the correspondence channel. It should be great yet for the genuine correspondence channel, the mistake comes while recovering secret data and this is estimated by BER. It is the proportion of the quantity of mistakes to the complete no of pieces sent in an image.

4.4 Correlation Coefficient (CR)

The relationship coefficient is utilized in estimating unique image and watermarked image. In ideal case, CR ought to approach 1. In any case, this may not be imaginable, so assuming the worth of CR is almost one, it is alright.

$$C_r = \frac{\sum_m \sum_n (Xi - X')(Yi - Y')}{\sqrt{(\sum_m \sum_n (Xi - X')^2)(\sum_m \sum_n (Yi - Y')^2)}}$$

Where, X' is the first image normal worth and Y' is the watermarked image normal worth.

4.5 Mean Square Error (MSE)

It is figured by performing byte by byte correlations of the two images. The portrayal of pixel with 8 pieces and the portrayal of dark level images upto 256 levels. The mutilation in the image can be estimated utilizing MSE. Allow I to be the cover image, K be the stego image and m*n be the all out number of pixels.

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

4.6 Peak Signal to Noise Ratio (PSNR)

The image steganography framework should implant the substance of stowed away data in the image so the nature of the image shouldn't change. PSNR is normally used to gauge the nature of reproduction of lossy pressure procedures Bigger the PSNR esteem shows the better nature of image for example less twisting. PSNR is the proportion of the most extreme sign to commotion in the stego image [17].

$$\text{PSNR} = 10 * Log_{10} \left(\frac{{MAX_C}^2}{MSE} \right) \ (dB)$$

4.7 Structural similarity index (SSIM)

SSIM looks at two given images of likeness utilizing their designs with values ranges between - 1 and 1. The nearer the SSIM is to 1 the more the likeness between the given two images and it is determined by

$$\text{SSIM}(x, y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

7. CLASSIFICATION OF IMAGE STEGANOGRAPHY TECHNIQUES

The two primary subcategories of steganography techniques are broadly classified as frequency (transform) domain or spatial domain. Researchers investigated number of steganographic approaches that are designed in well-known transform techniques because of the resilience and stability. There are many transformations stego methods as in shown figure 1.7.

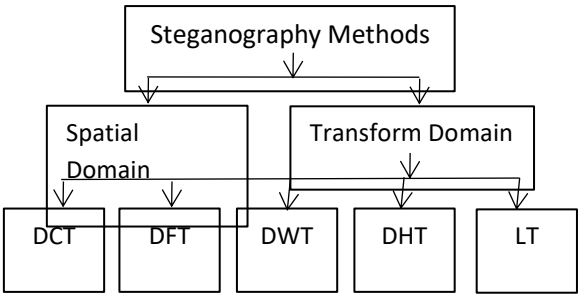

Fig 1.7: Classification of Steganography Methodologies.

7.1 Spatial Domain Techniques

Spatial area based image steganography is finished by controlling direct pixel values for implanting restricted information. The fundamental benefit of spatial space methods is their simple and quick execution which makes it the most used area for steganography 1[8]. There exist different spatial area methods for steganography like Least Huge Piece (LSB), Range based, Pixel Value Differencing (PVD), numerous piece plane based strategies, Histogram moving, and so on. The most widely recognized strategy utilized for steganography in spatial space is implanting in LSB. Late image steganography strategies utilizing LSB and other spatial area based techniques have been examined in this segment.

7.1.1 Least significant bit (LSB) based steganography

LSB strategy is one of the easiest and famous procedures in image steganography as the LSBs comprises of for the most part fragile data or commotion which won't debase the visual nature of the image in the wake of implanting privileged information bits. LSB based steganography has been utilized for high payload limit by keeping up with the great visual nature of the stego-image. Notwithstanding, the security of the LSB based strategies involves worry as due to its simple execution, it is more inclined to steganalysis assaults. Accordingly, to work on the security of the stego-image, scientists have utilized encryption of the mystery message prior to inserting. Figure 1.8 shows us that 11010010 has MSB (Most Huge Piece) and LSB (Least Critical Piece), the primary piece in 11010010 (1) is MSB, and the last Piece in11010010 (0) is LSB.

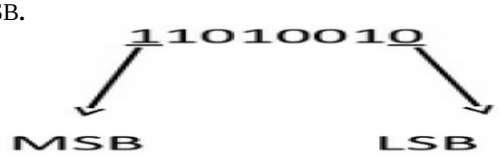

Fig 1.8: LSB and MSB in Steganography.

7.1.2 Pixel value differencing (PVD) Steganography

PVD is one more typical technique in view of spatial area for image steganography in which implanting is finished by contrasting the upsides of continuous pixels. The upside of PVD is that subsequent to implanting it doesn't influence the visual nature of the stego-image; notwithstanding, the installing limit should be worked on further. In writing, it has been seen that half and half implanting procedures perform well with regards to fundamental steganography necessities by joining the advantages of various plans.

7.2 Transform Domain Techniques

In the transform space, implanting is finished in transformed coefficients rather than straightforwardly to the power values. There exists number of various transform space strategies which has been used by the scientists in the cutting edge for

image steganography which incorporates Discrete Fourier Transform (DFT) [19], Discrete Cosine Transform (DCT) [20] and Discrete Wavelet Transform (DWT) [21]. As of late, a portion of the scientists have used various variants of these transforms, for example, Discrete Fourier Transform (DFT) [22], Integer Wavelet Transform (IWT) [23], and Laguerre Transform [24] and so on for image steganography

7.2.1 DISCRETE WAVELET TRANSFORM (DWT)

Discrete Wavelet Transform (DWT) has ended up being the favored area of concentrate in the field of data stowing away. This is for the most part because of its broad usage in the new image pressure standard, JPEG2000, and its capacity to address limit and vigor. The DWT separates pixel values into different recurrence groups known as sub groups. Each sub band can be portrayed as the accompanying [25]:

LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically high pass
HL - Horizontally high pass and vertically low pass
HH - Horizontally and vertically high pass

To keep away from these restrictions, new transform space strategies are there which have been investigated by the analysts in image steganography. One of the strategies is DWT what separates the image into four sub-groups where implanting should be possible autonomously which gives high visual quality to the stego-images. The decay of DWT into one, two and three level is given in figure 1.9 and this disintegration is finished with the series of separating and down examining. The execution aftereffects of first-level and second-level (LL sub-band) 2D DWT decay on an image (512 × 512 goal) are displayed in figure 1.10.

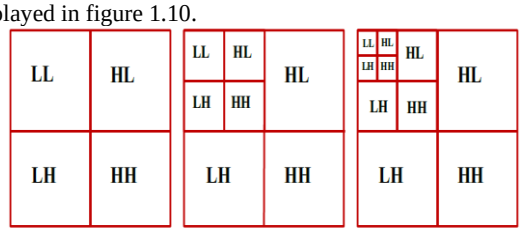

Fig 1.9: Different level decompositions of DWT.

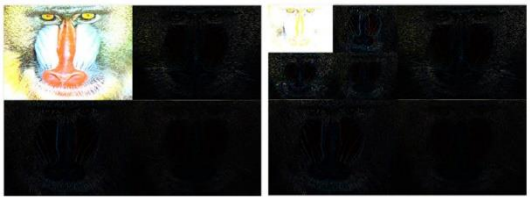

Fig 1.10: Example of 1st and 2nd level DWT decomposition.

To acquire a superior comprehension with regards to how wavelets work the 2-D Haar wavelets will be examined. A 2-layered Haar-DWT comprises of two tasks, an even and an upward one. Activity of a 2-D Haar is as per the following:

Stage 1: First, the pixels are examined from left to right, on a level plane. Then, the expansion and deduction activities are done on nearby pixels. Then, the aggregate is put away on the left and the distinction put away on the right as displayed in figure 1.11.

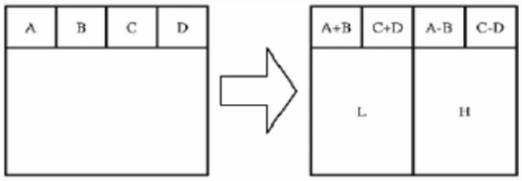

Fig 1.11: Horizontal procedure based on 1st row.

The above interaction is rehashed until every one of the lines is handled. The pixel values totals address the low recurrence component (indicated as image L) while the pixel distinctions address the high recurrence components of the first image (meant as image H).

Stage 2: All pixels are examined through and through in vertical request. Then, expansion and deduction tasks are completed on adjoining pixels, the aggregate is then put away on the top and the thing that matters is put away on the base as displayed in figure 1.12.

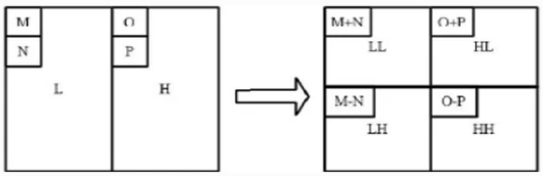

Fig 1.12: Vertical procedure based on 1st row.

The whole interaction made sense of above is known as the first-request 2-D Haar-DWT. The impacts of applying first-request 2-D Haar-DWT on the image "Lena" is displayed in figure 1.13. In contrast with DCT, late examinations have shown that wavelets are considered as being fewer assets escalated and make less twisting an image subsequently why the DWT strategy is turning into a more famous. Also, as DWT is separated into sub-groups, it gives higher adaptability with regards to versatility.

Fig 1.13: Example of 2-D Haar DWT.

7.2.2 DISCRETE COSINE TRANSFORM (DCT)

The DCT is a methodology for transforming a sign into rudimentary recurrence parts. It shows an image as a summation of sinusoids of fluctuating frequencies and sizes. For an information image x, we can work out the DCT coefficients of the transformed result image y, by utilizing Eq. 1. In the accompanying condition x, is an info image have N x M pixels, y(u,v) is DCT coefficient in uth line and vth section of the DCT framework and x(m,n) is the force of the pixel in mth column and nth segment of image grid.

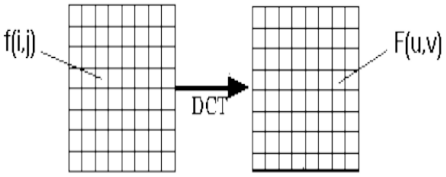

Fig 1.14: DCT transform of an Image.

Because of fitting in general execution, it's been utilized in JPEG standard for image pressure. It is capability addresses a strategy carried out to portrayal pixels in spatial region great technique to change them into recurrence space inside which inactivity may be marked. The one layered DCT be significant in handling single layered pointers comprise of the discourse waveforms. It broke the image into three recurrence groups the low, high, and mid as in figure 1.14.

One-dimensional DCT equation for k data items:

$$F(u)=\alpha(u)\sum_{x=0}^{k-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2k}\right]$$

Where u = 0, 1, 2. . . K-1.

Two dimensional DCT equations for k data item is

$$F(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{k-1}\sum_{y=0}^{K-1}f(x,y)\cos\left[\frac{(2x+1)u\pi}{2K}\right]\cos\left[\frac{(2y+1)u\pi}{2K}\right]$$

Where u,v = 0, 1, 2, . . . , K-1 Here, the input image is of size K × L.
f (i, j)- Pixel intensity
F (u, v) is DCT coefficient.

7.2.3 DISCRETE FOURIER TRANSFORM (DFT)

French mathematician fostered the idea that any capability which returns occasionally can be verbalized as an amount of sine as well as cosine relatives of incalculable frequencies, each increased by a coefficient. This is typified by a total; on the off chance that the equivalent is intermittent, fulfill some logical state or conditions. This summation is called Fourier series. Once more, capabilities which are limited however not intermittent can likewise be portrayed as a fundamental of sine and cosine capabilities duplicated by a weighing capability. The Fourier transform might be one layered or two layered. There might be simple and discrete Fourier transform. We will just consider discrete Fourier transform.
The DFT of a capability f (x, y) of size M × N is given in beneath condition for recurrence space transformation.

$$F(u,v) = 1/\left(\sqrt{MN}\right)\sum\sum f(x,y)\left(\cos 2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)-f(x,y)i\,\mathrm{Sin}2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right)$$

For $u = 0$ to $M-1$ and $v = 0$ to $N - 1$.
It tends to be said to change over the examined capability from its unique space frequently time or position along a line to the recurrence space. The Discrete Time Fourier transforms utilizes the discrete time however it changes over into the ceaseless recurrence. The calculation for figuring the DFT is extremely quick on current PCs. This calculation is known as Quick Fourier Transform for example FFT and it creates a similar outcome as of the DFT by utilizing the Reverse Discrete Fourier Transform.

7.2.4 INTEGER WAVELET TRANSFORM (IWT)

Most data concealing strategies perform installing data by changing the items in a source media. Subsequently, while extraction it causes some mutilation in cover image and in this manner the steganalyser can attempt to remove the privileged data. This can be tried not to by utilize Whole number Wavelet Transform. IWT is a more productive strategy to conceal privileged intel without mutilation. IWT maps whole numbers to whole numbers.

(a) Original image (b) 1st level DWT (c) 2nd level IWT
Fig 1.15: Example of Integer Wavelet Transform in sub band LL.

Though in DWT, assuming the info comprises of numbers, the subsequent result doesn't comprises of whole numbers. Hence it causes trouble in rebuilding of the first image. However, in the event of IWT, coming about result can be totally sorted with whole numbers. In IWT, LL sub-band has all the earmarks of being a nearby duplicate of the first image with more limited size while in DWT the subsequent LL is contorted somewhat, as displayed in figure 1.15.

7.2.5 LAGUERRE TRANSFORM (LT)

Be that as it may, the said transform was addressed in constant structure and thus, couldn't be taken advantage of in that frame of mind as the images are discrete in nature. In 2007, Paul Barry expanded McCully's paper in which he addressed the expressed transform in discrete whole number grid form and its converse inside the setting of outstanding Riordan exhibits. The remarkable Riordan bunch is addressed as a bunch of limitless lower-three-sided whole number networks.
Every matrix is characterized by a couple of producing capabilities

$$u(x) = 1 + u1x + u2x2 + \dots \text{ and}$$
$$v(x) = v1x + v2x2 + \dots [v1 \neq 0]$$

The related matrix is the matrix whose kth section has EGF $u(x)vk(x)/k!$
LT is viewed as the transform with matrix given by

$$Lag = \left[\frac{1}{1-x}, \frac{x}{1-x}\right]$$

The ILT is given by

$$Lag^{-1} = \left[\frac{1}{1+x}, \frac{x}{1+x}\right]$$

General term of LT

$$Lag(n,k) = \frac{n!}{k!}[x^n]((1-x)^{-1}x^k(1-x)^{-k})$$
$$= \frac{n!}{k!}[x^{n-k}]((1-x)^{-1-k}$$
$$= \frac{n!}{k!}\sum_{t=0}^{\infty}\binom{k+t}{t}x^t$$
$$= \frac{n!}{k!}\binom{n}{k}$$

The essential thought of LT is to get a whole number polynomial succession in light of pixel level expansion and augmentation in coefficient portrayal. Rather than the current transforms, the computation of LT is whole number based which makes the activities quicker. Our proposed strategy upholds various image arrangements, for example, BMP, PPM, PGM and Spat and so on other than JPEG. LT doesn't create complex result as DFT and consequently the computational intricacy is decreased to O(nlog(n)). Dissimilar to IWT based conspire, our proposed strategy offers unrivaled outcomes regarding payload and visual clearness (i.e., PSNR and SSIM).

Table 2: Comparison of Image Steganography Technique

Method	Imperceptibility	Robustness	Payload Capacity
LSB	High	Low	High
DWT	High	High	Low
DCT	Medium	Low	Low
DFT	High	Low	Low
IWT	Low	Low	Low
LT	High	High	Low

8. CONCLUSION

Steganography can be used to conceal secret information in images in a wide range of ways. Digital image steganography is a relatively new area of information concealment research. In this area, numerous significant studies have been conducted. We looked at some of the fundamental ideas, performance measures, and other important parameters that have an effect on image steganography in this paper. Although text, digital images, audio, video, and protocol are all possible carrier file formats, digital images are the most widely used because of how frequently they are used online. The paper also provides a brief overview of various steganography methods for secret message detection. In order for researchers who work in steganography and steganalysis to gain prior knowledge in

designing these techniques and their variants, the techniques' strengths and weaknesses are briefly discussed.

9. REFERENCES

[1] K. G. Maheswari, C. Siva, G. Nalinipriya, H. M, J. V and R. R, "An Innovative Model for Secure Environment Using Steganograph", 2022 8th International Conference on Smart Structures and Systems (ICSSS), 2022, pp. 1-5,

[2] A. Sahu, G. Swain and G. Swain, "Dual steganography imaging based reversible data hiding using improved LSB matching", International Journal of Intelligent Engineering and Systems, vol. 12, no. 5, pp. 63-73, 2019.

[3] Dalal, Mukesh & Juneja, Mamta. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications. Douglas, M., Bailey, K., Leeney, M., "An overview of steganography techniques applied to the protection of biometric data", Multimedia Tools & Applications Vol. 77, (2018). https://doi.org/10.1007/s11042-017-5308-3,

[4] J. Bieniasz, P. Bąk and K. Szczypiorski, "StegFog: Distributed Steganography Applied to Cyber Resiliency in Multi Node Environments", IEEE Access, vol. 10, pp. 88354-88370, 2022, doi: 10.1109/ACCESS.2022.3199749.

[5] G. F. Siddiqui, "A Dynamic Three-Bit Image Steganography Algorithm for Medical and e-Healthcare Systems", IEEE Access, vol. 8, pp. 181893-181903, 2020, doi: 10.1109/ACCESS.2020.3028315.,

[6] Chaudhary, Dev & Srivastava, Sandeep & Choudhury, Tanupriya. (2018), "Steganography for Confidential Communication and Secret Data storage" 461-465. 10.1109/ICGCIoT.2018.8753034.

[7] Y. Yang, R. Pintus, H. Rushmeier, and I. Ivrissimtzis, "A 3D steganalytic algorithm and steganalysis-resistant watermarking", IEEE Trans. Vis. Comput. Graphics, vol. 23, no. 2, pp. 10021013, Feb. 2017

[8] Rabie, Tamer & Kamel, I.. (2017). "High-capacity steganography: a global adaptive region discrete cosine transform approach", Multimedia Tools and Applications. vol. 76. 10.1007/s11042-016-3301-x,

[9] Nazari Mahboubeh, Ahmadi Iman Dorostkar, "A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity", Multimedia Tools and Applications 2020 ;79:13693–724. Maheswari, S Uma & D, Jude. (2015), "Discrete ripplet transform based steganography system for imaging applications", International Journal of Reasoning-based Intelligent Systems. 7. 130. 10.1504/IJRIS.2015.070927.

[10] A. Melman and O. Evsutin, "On the Efficiency of Metaheuristic Optimization for Adaptive Image Steganography in the DFT Domain", 2021 XVII International Symposium, Problems of Redundancy in Information and Control Systems, (REDUNDANCY), 2021, pp. 49-54, S. Khashandarag and N. Ebrahimian, "A New Method for Color Image Steganography Using SPIHT and DFT, Sending with JPEG Format", 2009 International Conference on Computer Technology and Development, 2009, pp. 581-586, doi: 10.1109/ICCTD.2009.14.

[11] Mandal, Jyotsna & Ghosal, Sudipta. (2013), "Separable Discrete Hartley Transform Based Invisible Watermarking for Color Image Authentication" (SDHTIWCIA). Advances in Computing and Information Technology (pp.767-776) 2013.

[12] P. Sharma and A. Sharma, "Robust technique for steganography on Red component using 3-DWT-DCT transform", 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1049-1054, doi: 10.1109/ICISC.2018.8398962.

[13] Jothy N, Anusuyya S., "A secure color image steganography using integer wavelet transform". In: 10th international conference on intelligent systems and control (ISCO); 2016. https://doi.org/10.1109/ISCO.2016.7726948.

[14] Baby, Della & Thomas, Jitha & Augustine, Gisny & George, Elsa & Michael, Neenu. (2015), "A Novel DWT Based Image Securing Method Using Steganography", Procedia Computer Science. 46. 612-618. 10.1016/j.procs.2015.02.105.

[15] M. M.; Huy, V. N.; Tuan, N. M., "Some operational properties of the Laguerre transform", AIP Conference Proceedings 1798, 020130 (2017); doi: 10.1063/1.4972722, 2017

[16] G. Mandyam and N. Ahmed, "The discrete Laguerre transform: derivation and applications", in IEEE Transactions on Signal Processing, vol. 44, no. 12, pp. 2925-2931, Dec. 1996, doi: 10.1109/78.553468.

[17] Debnath, L. ,"An application of laguerre transform on the problem of oscillation of a very long and heavy chain", Ann. Univ. Ferrara 9, 149–151 (1959). https://doi.org/10.1007/BF02835444

[18] Sudipta Kr Ghosal, Souradeep Mukhopadhyay, Sabbir Hossain, Ram Sarkar, "Exploiting Laguerre transform in Image Steganography", Computers & Electrical Engineering, Volume 89, 2021, https://doi.org/10.1016/j.compeleceng.2020.106964

[19] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019)

[20] R. Sulaiman, C. Kirana, T. Sugihartono, Laurentinus and F. Panca Juniawan, "RC4 Algorithm and Steganography to Double Secure Messages in Digital Image", 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020, pp. 1-4, doi: 10.1109/CITSM50537.2020.9268833.

[21] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms", 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 86-90, 2017.

[22] R. Sulaiman, B. Isnanto, Hengki and C. Kirana, "Cryptography in (LSB) Method Using RC4 Algorithm and AES Algorithm in Digital Image to Improve Message Security", 2018 International Conference on Computing Engineering and Design (ICCED), pp. 29-34, 2018.