Asian Journal of Applied Science and Technology (AJAST)

(Peer Reviewed Quarterly International Journal) Volume 3, Issue 1, Pages 298-306, Jan-March 2019

A Brief Survey of Image Authentication Methods by DFT, DWT and QFT with Hashing Technique

Anitha.D[1], Dr.N.Suguna[2] & Ms.P.Sowkarthiga[3]

[1]*ME (Computer Science), Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore.*
[2]*Professor, Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore.*
[3]*Assistant Professor, Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore.*

Article Received: 30 August 2018 Article Accepted: 29 December 2018 Article Published: 27 March 2019

ABSTRACT

Because of the development of interactive media applications, the assurance of this sight and sound information turns into a critical issue of correspondence and capacity; particularly when it is exchanged over an uncertain station, where separated from forestalling illegal information get to and the images are utilized in numerous fields, for example, medicinal science and military. Along these lines there is a need of image authentication. In this work, a novel information installing method in recurrence space has been proposed for image authentication and verified message transmission dependent on concealing a huge volume of information into dim pictures. Image authentication is finished by inserting message/picture in recurrence area by picking picture squares of size 2 × 2, called veil, from the source picture in line significant request and change it into the recurrence space. The study is performed for picture validation and the techniques like Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Quantum Fourier Transform (QFT) and the outcomes are looked at. Three bits of confirming message/picture are created inside the genuine piece of every pixel, barring the main pixel of each sub framework where the position is picked utilizing a hash work. The procedure is rehashed for each sub grid on column significant request to embed confirming message/picture content and 128 bits Message Digest (MD-5), created from verifying message/picture. Converse is performed on inserted information to change installed recurrence part to spatial segment. So as to keep the quantum esteem positive and non negative in spatial space, a solid and sound strategy is consolidated principally on the main recurrence part and now and then on other segment relies on circumstances. The unraveling is finished by applying the invert calculation.

Keywords: Image Security, Authentication, DFT, DWT, DFT, MD-5.

1. INTRODUCTION

Correspondence over Internet has turned out to be inconceivably prominent and advanced media are widely utilized for exchanging data. Steganography is a critical method to secure fragile data during transmission through open systems. Steganography is the specialty of concealing data into image or other media so that nobody can separate it from the sender and planned beneficiary even understands that there is shrouded data [2]. Image transmission by means of the web has some issue, for example, data security, copyright insurance, Originality and so forth. Verified correspondence is conceivable with the assistance of encryption strategy which is a cluttered and confounding message that makes sufficiently suspicious to assault busybodies. Without making any exceptional consideration of aggressors, steganographic techniques defeat the issue by concealing the discharge data behind the source image. Image dealing over the system is expanding step by step team to the multiplication of internetworking. Image authentication is expected to forestall unapproved access in different online business application regions. This security can be accomplished by concealing information inside the image. Information covering up in the image has turned into an essential system for image verification and recognizable proof. Subsequently, military, medicinal and quality control pictures must be ensured against endeavors to controls. For the most part advanced image verification plots for the most part falls into two classes' spatial space and recurrence area methods. Along these

CITE THIS ARTICLE: Anitha.D, N.Suguna & P.Sowkarthiga, "A Brief Survey of Image Authentication Methods by DFT, DWT and QFT with Hashing Technique", *Asian Journal of Applied science and Technology*, Volume 3, Issue 1, Pages 298-306, Jan-March 2019

lines, advanced image verification system has turned into a testing research region concentrated on doing combating to keep the unapproved or illicit access and sharing [6]. Steganographic method is strategies to accomplish validation of images and emit correspondence between two gatherings that are embedded and secluded from everything, the substance of discharge message/picture yet additionally go about as conveying it. To this point, steganography calculations implant the discharge data into various kinds of common spread information like sound and images. The subsequent adjusted information is alluded to as stego-information and it must be perceptually unclear from its characteristic spread. Along these lines, steganography is the craft of discharge correspondence. Security is a major worry in cutting edge image dealing over the system. Security can be accomplished by concealing information inside the image. Information covering up in the image has turned into an essential method for image validation and distinguishing proof. Possession confirmation and verification is the real assignment for military individuals, look into foundation, and researcher. Image verification is a method for embeddings data into an image for distinguishing proof and validation. Image confirmation innovation is winding up progressively vital because of the expansion of advanced pictures on the WWW and in web based business. Thus, data security and image validation has turned out to be critical to shield computerized image report from unapproved get to. These are apparatuses and methods used to secure the creativity and to guarantee the validness of the image record [3].

Information concealing alludes to the imperceptible installing of data inside a host informational index as the message, picture, and video. In steganographic applications, the concealed information might be emitting message or discharge 3D image or discharge video whose insignificant nearness inside the host informational index ought to be imperceptible. The information covering up speaks to a valuable option in contrast to the development of a hypermedia record or image, which is exceptionally less advantageous to control. The objective of steganography is to shroud the message/picture in the source image by some key systems as the outcome onlooker has no information of the presence of the message/picture and it is not normal for cryptography where the objective is to verify correspondences from an eavesdropper by making the information non-reasonable. In certain circumstances, sending encoded data will excite doubt while imperceptible data won't do as such. To conceal a message inside an image without changing its noticeable properties the source picture might be modified.

This work introduces a calculation to embed expansive volume of messages/picture information along the MD-5 key created from confirming message/picture into the source image for image confirmation and furthermore to transmit verified message inside the image. It performs verification process by spreading the bit example of the document in spatial area. The proposed procedure actualizes the validation procedure utilizing hash work in recurrence space which has solid probability in confirmation. The techniques like Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Quantum Fourier Transform (QFT) are taken and the outcomes are analyzed. The majority of the works use bits of source image for inserting in time area, yet the proposed system installs bits of verifying message/picture in recurrence space. The plan utilizes proficient addition inside a byte,

which may comply with legitimate confirmation and distinguishing proof of the image just as mystery message transmission.

2. RELATED WORK

Mitchell D, et al., in the year 1996 proposed a procedure of powerful information covering up for images with encoding additional data in a image by making little adjustment to its pixels [1], the principal strategy depicts spatial veiling and information spreading to shroud data by changing image coefficients. The second technique utilizes recurrence veiling to alter image otherworldly parts. Mauro Barni proposed an answer for the issue of copyright assurance of media information in an arranged situation by computerized watermarking [2], it makes conceivable to immovably connect an advanced report with a code permitting the distinguishing proof of the information maker, proprietor, approved purchaser, etc.

In the year 2005 Rongrong Ni, et al., proposed a semi-blind system [3] to validate through installing the image with a parallel copyright image pursued by Arnold cycle change for building the watermark to expand the security. The safe image versatile watermark is implanted in the element hinders by adjusting DCT center recurrence coefficients. This recognition and extraction is a semi-dazzle since it needn't bother with the first image however the individuals who have the first watermark and the key can identify and separate the correct watermark, which gives the high-security level. In 2007 Guillaume Lavoué introduced a non-dazzle watermarking plan for subdivision surfaces [4]. Jawline Chen Chang around the same time proposed reversible covering up in DCT-based packed images [5], in this plan, the two progressive zero coefficients of the medium-recurrence segments in each square were utilized to conceal the mystery information, and the plan alters the quantization table to keep up the nature of the stego-picture.

In 2008 Haohao Song, et al., proposed a contourlet based versatile system that disintegrates a image into low-recurrence (LR) sub-band and a high-recurrence (HR) sub-band by Laplacian pyramid (LP). In this plan, the LF sub-band is made by separating the first image with a 2-D low-pass channel and the HF sub-band is made by subtracting the orchestrated LF sub-band from the first picture, at that point mystery message/picture inserted into the contourlet coefficients of the biggest detail sub-groups of the image.

3. MATERIALS AND METHODS

3.1 Discrete Fourier Transform (DFT)

The work accentuates on data and image assurance against unapproved access in recurrence area. The recurrence area is where the simple image of ceaseless flag lives. When the consistent flag gets inspected and quantized they get into a spatial area where the portrayal of the image is in discrete structure [7]. The most widely recognized sort of flag entering the Discrete Fourier Transformation (DFT) is made out of tests taken at customary interims of time. In the example "genuine part" signifies the cosine wave amplitudes while "nonexistent part" signifies the sine wave amplitudes. The DFT of a capacity (image) f(x, y) of size M x N is given in condition underneath for recurrence area change.

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\left(\frac{2\Pi ux}{M}\right) - f(x,y)\, j \sin\left(\frac{2\Pi vy}{N}\right)$$

For u = 0 to M – 1 and v = 0 to N-1.

The factors u and v are the recurrence factors and x, y are the spatial or image factors. So also backwards discrete Fourier change, where the recurrence area gets changed over to the spatial space, computerized image might be composed as in condition underneath for change from recurrence to spatial area.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u,v) \cos\left(\frac{2\Pi ux}{M}\right) + F(u,v)\, j \sin\left(\frac{2\Pi vy}{N}\right)$$

For u = 0 to M – 1 and v = 0 to N-1.

The Image Authentication in Frequency Domain utilizing Discrete Fourier Transformation Technique (IAFDDFTT) gives security by inserting the confirming message/picture in recurrence space. Before installing, the computerized image is changed from time area to recurrence space portrayal utilizing DFT system.

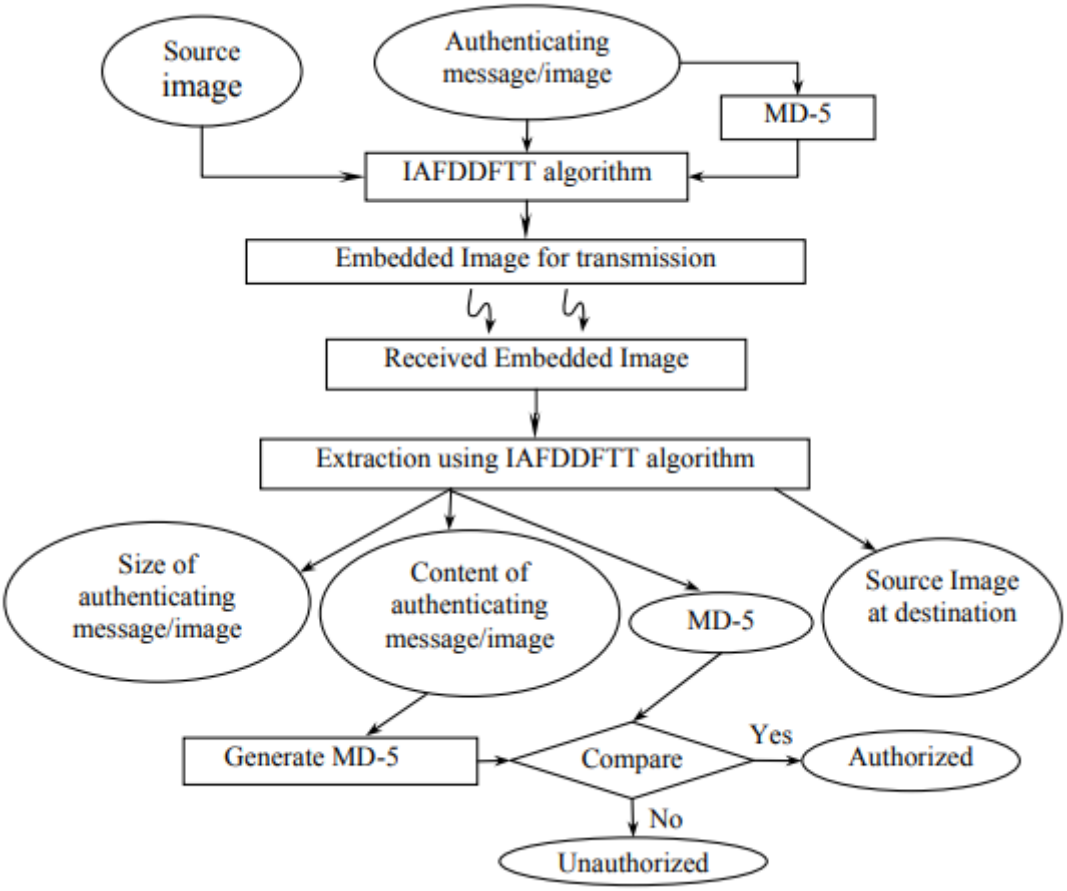


Figure No: 1 Framework of IAFDDFTT Method

 Online ISSN: 2456-883X

In IAFDDFTT to create changed qualities utilizing DFT a 2 x 2 sub network has been taken from source image grid as a window and confirming message/picture bits are implanted inside the genuine piece of the changed information (barring the first pixel in every 2 x 2 sub lattice) of the window. One MD-5 key has been created from confirming message/picture utilizing surely understood message digest 5 techniques. The size and substance of validating message/picture and MD-5 key is installed to the changed source image. In the side of inserting, reverse DFT as given in condition has been performed on the installed image to change the implanted image from recurrence to spatial area. The reverse task is performed at the less than desirable end, and separating bits of validating message/picture and MD-5 key for confirmation at goal and it is given in figure 1.

3.2 Discrete Wavelet Transform (DWT)

The Image Authentication in Frequency Domain utilizing Discrete Wavelet Transformation Technique (IAFDDWTT) is partitioned into four stages. Forward change of spread image is performed toward the start to change over the image from spatial space to recurrence utilizing DWT, which is registered by progressive low pass and high pass separating of the discrete time-area flag. After the change, implanting stage rushes to insert "t" number of bits into every byte of spread image in fluctuating positions chose through hash work. Loyalty alteration is done on the implanted image to improve the nature of the image without hampering the embedded data bits [8].

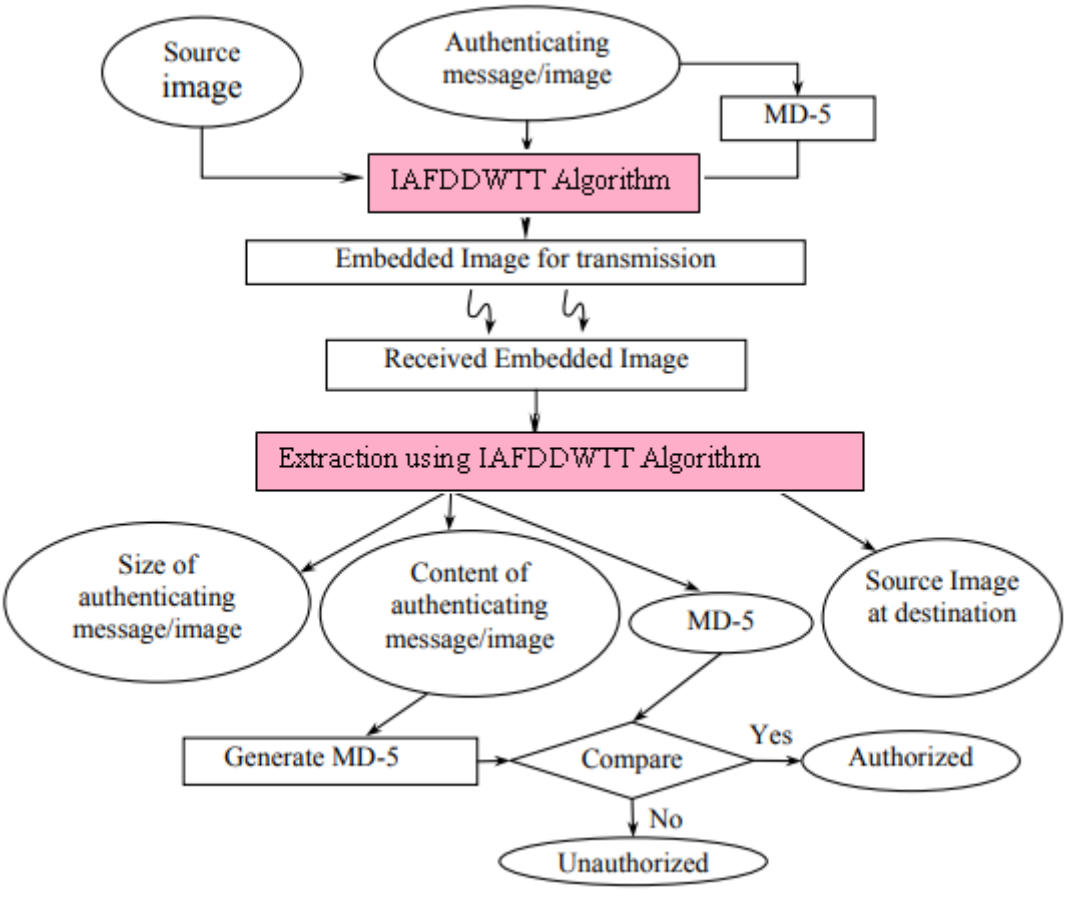


Figure No: 2 Framework of IAFDDWTT Method

A switch change is executed as a conclusive advance of inserting which create the implanted image. At goal, the obtained picture goes through forwarding change utilizing DWT and dependent on same hash work, mystery message/picture bits are separated to reproduce the message/picture. On looking at separated mystery message/picture with a unique secret message/picture, the obtained picture at goal is confirmed. One MD-5 key has been created from confirming message/picture utilizing surely understood message digest 5 techniques. The size and substance of validating message/picture and MD-5 key are implanted to the changed source picture. In the wake of implanting, reverse DWT has been performed on the installed picture to change the inserted picture from recurrence to spatial space. The reverse task is performed at the less than the desired end, and removing bits of confirming message/picture and MD-5 key for confirmation at goal and it is given in figure 2.

3.3 Quantum Fourier Transform (QFT)

Quantum Fourier changes are the utilization of established discrete Fourier change to the quantum states [9]. The QFT change of an orthonormal premise set |0|, |1|, ..., |N − 1| can be characterized as pursues:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle$$

Where $N = 2^n$ and orthonormal basis set is |0|, |1|, ..., |2 n − 1|. The |x| state can be written in binary form as $x = x_0, x_1,...x_{N-1}$. The |x| state is transformed into the phase as results of the QFT transform.

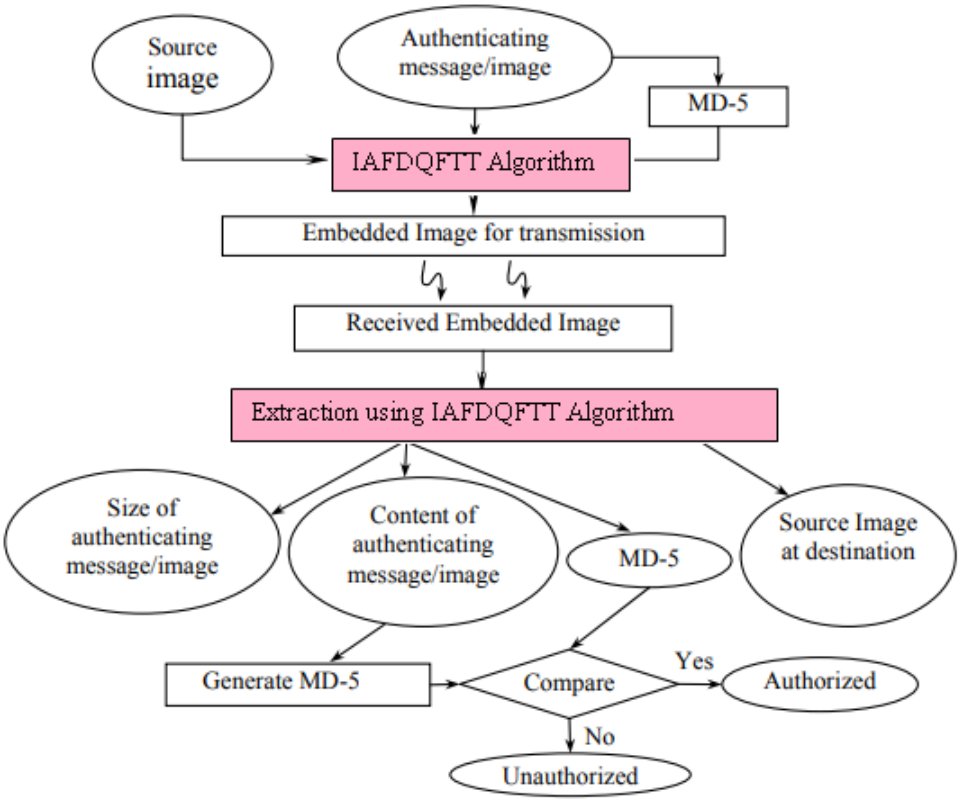


Figure No: 3 Framework of IAFDQFTT Method

Online ISSN: 2456-883X

The security of Image Authentication in Frequency Domain utilizing Quantum Fourier Transformation Technique (IAFDQFTT) of quantum images is recommended by utilizing the Quantum Fourier Transform (QFT) with hashing capacities. In the convention, QFT and keys are utilized to impart mark to beneficiaries. So all individuals know just their hashing data will be the encoded yield of the QFT. This improves the security of the convention. Also, the security of the convention is furnished by utilizing reorder QFT yield with change of the MD-5 calculation. One MD-5 key has been created from validating message/picture utilizing understood message digest five strategy. The size and substance of verifying message/picture and MD-5 key is installed to the changed source image. Subsequent to installing, backwards QFT has been performed on the inserted image to change the implanted image from recurrence to spatial area. The switch activity is performed at the less than desirable end, and separating bits of validating message/picture and MD-5 key for confirmation at goal and it is given in figure 3.

4. RESULTS AND DISCUSSION

In this section, a comparative study has been made between IAFDDFTT, IAFDDWTT and IAFDQFTT in terms of peak signal to noise ratio and image fidelity. Gold coin is embedded as secret image of dimension 128x128. The results are shown in table 1.

Original Image	Original Coin

Table No: 1 Original Image Representation

The embedding through IAFDDFTT, IAFDDWTT and IAFDQFTT and the extraction through IAFDDFTT, IAFDDWTT and IAFDQFTT are shown in table 2.

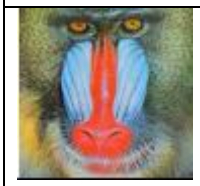
Embedding through IAFDDFTT	Embedding through IAFDDWTT	Embedding through IAFDQFTT	Extraction through IAFDDFTT	Extraction through IAFDDWTT	Extraction through IAFDQFTT
					

Table No: 2 Embedding and Extraction through IAFDDFTT, IAFDDWTT and IAFDQFTT

The peak signal to noise ratio and the image fidelity values are calculated for all the methods and the results are shown in table 3 and figure 4.

Methods	PSNR	IF
IAFDDFTT	37.54	0.99948
IAFDDWTT	30.92	0.99912
IAFDQFTT	30.10	0.99905

Table No: 3 PSNR and IF Values

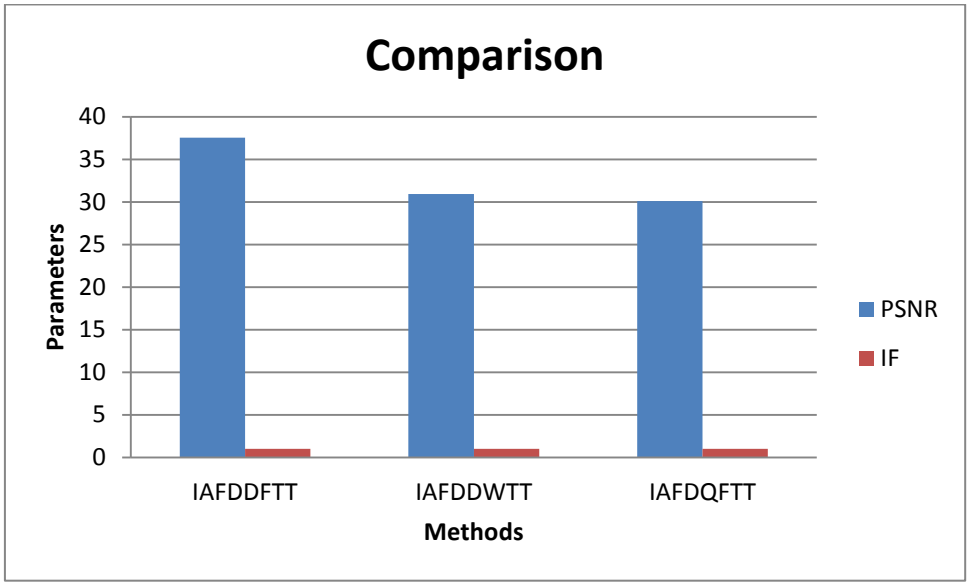


Figure No: 4 PSNR and IF Values

The methods like IAFDDFTT, IAFDDWTT and IAFDQFTT are compared. In IATFDDFT the average bytes with higher average PSNR values 37.54 and completely recoverable the authenticating message/image.

5. CONCLUSION

In every one of the procedures the PSNRs are low, imply bit-mistake rate are high yet in the IAFDFTT plot and more bytes of confirming information can be implanted and the PSNR esteems are essentially high, and implies bit-blunder rate is low. In DCT based plan, it doesn't insert in each and every square of the image. Here specifically pick the districts that don't produce obvious mutilation for inserting, in this manner diminishing the validating information estimate. In QFT based remuneration it enables the inserting to be undetected regardless of whether its quality is high. For low-pressure factor, it can't totally recuperate the installed message. IATFDDFT procedure is a image confirmation process in recurrence area to upgrade the security contrasted with the current calculations. In contrast with DCT and QFT based method, this calculation is pertinent for a shading images validation and quality is high. First recurrence segment in each veil is utilized for re-changing. The control method is connected to streamlined the commotion expansion accordingly PSNR is expanded and IF is closer to 1. In the proposed IATFDDFT confirmation is done in recurrence area without changing the visual property of the verified image. In IATFDDFT perversion of image and change of constancy (like sharpness, brilliance and so on) is unimportant.

6. REFERENCES

[1] Mitchell D. Swanson, el at., "Transparent robust image watermarking" Image Processing, 1996. Proceedings., on International Conference, Vol 3, print ISBN: 0-7803-3259-8, DOI 10.1109/ICIP.1996.560421, Sep 1996.

[2] Mauro Barni, et al., "A DCT-domain system for robust image watermarking", doi:10.1016/S0165-1684(98)00015-2, Volume 66, Issue 3, 28 May 1998, Pages 357-372.

[3] Rongrong Ni, et al., "Secure semi-blind watermarking based on iteration mapping and image features", Pattern Recognition, Volume 38, Issue 3, Elsevier Science Inc. New York, NY, USA, ISSN: 0031-3203, Pages 357-368, March 2005, doi>10.1016/j.patcog.2004.08.006.

[4] Guillaume Lavoué, et al., "Subdivision surface watermarking", Computers & Graphics, Volume 31, Issue 3, Pages 480-492. ISSN: 0097-8493, June 2007.

[5] Chin-Chen Chang, et al., "Reversible hiding in DCT-based compressed images", Information Sciences, ISSN: 0020-0255, doi:10.1016/j.ins.2007.02.019 Volume 177, Issue 13, 1 July 2007, Pages 2768-2786.

[6] Nameer N. EL-Emam, Hiding a large Amount of data with High Security Using Steganography Algorithm, Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.

[7] Ghoshal N., Mandal, J. K. A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT), Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, pp. 24-32, 2008.

[8] Madhumita Sengupta, J. K. Mandal, N. Ghoshal, An Authentication Technique in Frequency Domain through Wavelet Transform (ATFDWT), Association for the Advancement of Modelling and Simulation Techniques in Enterprises.

[9] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "Neqr: a novel enhanced quantum representation of digital images," Quantum Inf Process, vol. 12, pp. 2833–2860, 2013. [Online]. Available: https://doi.org/10.1007/s11128-013-0567-z.