FORM P1

REPUBLIC OF SOUTH AFRICA

PATENTS ACT, 1978

APPLICATION FOR A PATENT AND ACKNOWLEDGEMENT OF RECEIPT

[Section 30 (1)-Regulation 22]

The granting of a patent is hereby requested by the undermentioned applicant on the basis of the present application.

Official Application No.			Applicant's or Agent's Reference
21	01	**2024/06065**	4383LPS

71	Full Name(s) of Applicant(s)

Dr. Himadri Mandal
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
Dr. Amit Phadikar
Santal Bidroha Sardha Satabarshiki Mahavidyalaya PO+PS: Goaltore, Dist: Paschim Medinipur, 721128, India
Dr. Goutam Kumar Maity
Mahishadal Raj College, Garkamalpur, Mahishadal, Purba Medinipur, West Bengal, 721628, India
Dr. Angshuman Majumdar
Department of Electronics and Communication Engineering, Brainware University, Barasat, Kolkata, West Bengal, 700125, India
Dr. Ramkrishna Rakshit
Dr. B.C.Roy Engineering College, Fuljhore, Jemua Road, Durgapur, 713206, India
Dr. Aniruddha Ghosh
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata,West Bengal, 700160, India
Dr. Subhalaxmi Chakraborty
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Atanu Chowdhury
Calcutta Institute of Technology, India
Calcutta Institute of Technology
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
University of Engineering and Management, Kolkata
University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Brainware University
398, Ramkrishnapur Road, Barasat, Kolkata, 700125, India

54	Title of invention

A SYSTEM BASED ON DATA HIDING TECHNIQUE FOR EFFICIENT QUALITY ACCESS CONTROL OF IMAGES AND A METHOD THEREOF

The applicant claims priority as set out on the accompanying Form P.2. The earliest priority claimed is

COUNTRY: NUMBER: DATE:

~~This application is for a patent of addition to patent application No.~~

21	01	

~~This application is a fresh application in terms of section 37 and based on Application No.~~

21	01	

This application is accompanied by:

X	1.	A single copy of a complete specification of 27 pages.
X	2.	Drawings of 6 sheet(s).
X	3.	Publication particulars and abstract(Form P8)
X	4.	A copy of a figure of the drawing (if any) for the abstract
X	5.	Assignment of invention
	6.	Certified priority document(s)
	7.	Translation(s) of the priority document(s)
	8.	Assignment of priority rights
	9.	A copy of the Form P.2 and the specification of S.A Patent Application (if applicable).
X	10.	A declaration and power of attorney on Form P3
X	11.	Statement on the use of indigenous Biological Resource, Genetic Resource, Traditional Knowledge or Use on Form P26

74	Address of Service:

SOUTH AFRICA

Dated this 7th day of August 2024

RECEIVED

Official Date Stamp
..... Registrar of Patents

Digitally signed by :

.....

Signature of Applicant(s)

This is returned to the applicant's address for service as proof of lodging.

FORM P2

REPUBLIC OF SOUTH AFRICA | REGISTER OF PATENTS | PATENTS ACT, 1978

Official application No.	Lodging date: Provisional	Acceptance date
21 01 **2024/06065**	22	47
International classification	**Lodging date: Complete**	**Granted date**
51 G06K	23 2024/08/07	

71 Full name(s) of applicant(s)/Patentee(s):

Dr. Himadri Mandal
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
Dr. Amit Phadikar
Santal Bidroha Sardha Satabarshiki Mahavidyalaya PO+PS: Goaltore, Dist: Paschim Medinipur, 721128, India
Dr. Goutam Kumar Maity
Mahishadal Raj College, Garkamalpur, Mahishadal, Purba Medinipur, West Bengal, 721628, India
Dr. Angshuman Majumdar
Department of Electronics and Communication Engineering, Brainware University, Barasat, Kolkata, West Bengal, 700125, India
Dr. Ramkrishna Rakshit
Dr. B.C.Roy Engineering College, Fuljhore, Jemua Road, Durgapur, 713206, India
Dr. Aniruddha Ghosh
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata,West Bengal, 700160, India
Dr. Subhalaxmi Chakraborty
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Atanu Chowdhury
Calcutta Institute of Technology, India
Calcutta Institute of Technology
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
University of Engineering and Management, Kolkata
University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Brainware University
398, Ramkrishnapur Road, Barasat, Kolkata, 700125, India

71 Applicant substitued:	Date registrered

71 Assignee(s):	Date registrered

72 Full name(s) of inventor(s):

Dr. Himadri Mandal
Dr. Amit Phadikar
Dr. Goutam Kumar Maity
Tien-Lung Chiu

Priority claimed:	Country	Number	Date

54 Title of invention

A SYSTEM BASED ON DATA HIDING TECHNIQUE FOR EFFICIENT QUALITY ACCESS CONTROL OF IMAGES AND A METHOD THEREOF

Address of applicant(s)/patentee(s):

Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316
INDIA
Santal Bidroha Sardha Satabarshiki Mahavidyalaya PO+PS: Goaltore, Dist: Paschim Medinipur, 721128
INDIA
Mahishadal Raj College, Garkamalpur, Mahishadal, Purba Medinipur, West Bengal, 721628
INDIA
Department of Electronics and Communication Engineering, Brainware University, Barasat, Kolkata, West Bengal, 700125
INDIA
Dr. B.C.Roy Engineering College, Fuljhore, Jemua Road, Durgapur, 713206
INDIA
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata,West Bengal, 700160
INDIA
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160
INDIA
Calcutta Institute of Technology
INDIA

Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316 INDIA University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160 INDIA 398, Ramkrishnapur Road, Barasat, Kolkata, 700125 INDIA	
74	Address for service
SOUTH AFRICA Reference No. 4383LPS	

61	Patent of addition No.	Date of any change
Fresh application based on.		Date of any change

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978
COMPLETE SPECIFICATION
[Section 30(1) – Regulation 28]

OFFICIAL APPLICATION NO.		LODGING DATE	
21 01	**2024/06065**	22	2024/08/07

INTERNATIONAL CLASSIFICATION	
51	G06K

FULL NAME(S) OF APPLICANT(S)

71
Dr. Himadri Mandal
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
Dr. Amit Phadikar
Santal Bidroha Sardha Satabarshiki Mahavidyalaya PO+PS: Goaltore, Dist: Paschim Medinipur, 721128, India
Dr. Goutam Kumar Maity
Mahishadal Raj College, Garkamalpur, Mahishadal, Purba Medinipur, West Bengal, 721628, India
Dr. Angshuman Majumdar
Department of Electronics and Communication Engineering, Brainware University, Barasat, Kolkata, West Bengal, 700125, India
Dr. Ramkrishna Rakshit
Dr. B.C.Roy Engineering College, Fuljhore, Jemua Road, Durgapur, 713206, India
Dr. Aniruddha Ghosh
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata,West Bengal, 700160, India
Dr. Subhalaxmi Chakraborty
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Atanu Chowdhury
Calcutta Institute of Technology, India
Calcutta Institute of Technology
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
University of Engineering and Management, Kolkata
University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Brainware University
398, Ramkrishnapur Road, Barasat, Kolkata, 700125, India

FULL NAME(S) OF INVENTORS(S)

72
1. Dr. Himadri Mandal
2. Dr. Amit Phadikar
3. Dr. Goutam Kumar Maity
4. Tien-Lung Chiu

TITLE OF INVENTION

54 **A SYSTEM BASED ON DATA HIDING TECHNIQUE FOR EFFICIENT QUALITY ACCESS CONTROL OF IMAGES AND A METHOD THEREOF**

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978
PUBLICATION PARTICULARS AND ABSTRACT
[Section 32(3)(a) – Regulation 2291)(g) AND 31]

OFFICIAL APPLICATION NO.		LODGING DATE		ACCEPTANCE DATE	
21	01 **2024/06065**	22	2024/08/07	47	

INTERNATIONAL CLASSIFICATION		NOT FOR PUBLICATION
51	G06K	CLASSIFIED BY:

FULL NAME(S) OF APPLICANT(S)

71
Dr. Himadri Mandal
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
Dr. Amit Phadikar
Santal Bidroha Sardha Satabarshiki Mahavidyalaya PO+PS: Goaltore, Dist: Paschim Medinipur, 721128, India
Dr. Goutam Kumar Maity
Mahishadal Raj College, Garkamalpur, Mahishadal, Purba Medinipur, West Bengal, 721628, India
Dr. Angshuman Majumdar
Department of Electronics and Communication Engineering, Brainware University, Barasat, Kolkata, West Bengal, 700125, India
Dr. Ramkrishna Rakshit
Dr. B.C.Roy Engineering College, Fuljhore, Jemua Road, Durgapur, 713206, India
Dr. Aniruddha Ghosh
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata,West Bengal, 700160, India
Dr. Subhalaxmi Chakraborty
University Of Engineering and Management, Kolkata, University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Atanu Chowdhury
Calcutta Institute of Technology, India
Calcutta Institute of Technology
Calcutta Institute of Technology, Banitabla, Uluberia, Howrah, 711316, India
University of Engineering and Management, Kolkata
University Area, Plot No. III, B/5, New Town Rd, Action Area III, Newtown, Kolkata, West Bengal, 700160, India
Brainware University
398, Ramkrishnapur Road, Barasat, Kolkata, 700125, India

FULL NAME(S) OF INVENTORS(S)

72
1. Dr. Himadri Mandal
2. Dr. Amit Phadikar
3. Dr. Goutam Kumar Maity
4. Tien-Lung Chiu

EARLIEST PRIORITY CLAIMED

COUNTRY		NUMBER		DATE	
33		31		32	

TITLE OF INVENTION

54 **A SYSTEM BASED ON DATA HIDING TECHNIQUE FOR EFFICIENT QUALITY ACCESS CONTROL OF IMAGES AND A METHOD THEREOF**

57 **The present invention relates to a system and method based on data hiding technique, for efficient quality access control of images. The present invention discloses a hardware implementation of a data hiding technique for efficient quality access control of images using lifting-based discrete wavelet transformation (DWT). It comprises modules for image storage, DWT/IDWT, dither generation, watermark permutation, embedding, and extraction. A binary watermark is embedded into the DWT coefficients of the host image using adaptive dither modulation, enabling access control. The hardware architecture, designed using power-aware techniques, offers low power consumption of 78.48mW at 130.14MHz for 512x512 images. It achieves high throughput of 23.8MB/s for encoding/decoding, minimal resource utilization, and avoids storing the original image, reducing memory requirements. The invention provides an efficient, real-time, and easily integrable solution for image access control, enabling content protection and commercial benefits for vendors while allowing authorized users to access superior quality.**

PATENT IMAGE

A system based on data hiding technique for efficient quality access control of images and a method thereof

FIELD OF THE INVENTION

The present disclosure relates to hardware implementation of data hiding technique, specifically to a system and method based on data hiding technique, for efficient quality access control of images. In more particular manner the present invention relates to a system with plurality of hardware components, and method for efficient quality access control of images using lifting-based discrete wavelet transformation (DWT). The invention relates to an implementation of FPGA-based low-power hardware architecture of data hiding scheme for efficient quality access control of grayscale images using lifting-based DWT.

BACKGROUND OF THE INVENTION

With the widespread use of the internet and advancements in digital technology, sharing and replicating digital multimedia content (images, documents, videos) has become increasingly easy without loss of quality. This proficiency in accessing digital content poses challenges for commercial vendors and creators who wish to protect their innovative work and derive commercial benefits from it. To address this issue, various access control mechanisms based on data hiding techniques have been proposed to ensure copyright protection and ownership verification.

Numerous approaches have been developed in the literature, including histogram modification, prediction error adjustment (PEA), rational dither modulation (RDM), and dither modulation. These schemes operate either in the spatial domain or in transform domains such as discrete cosine transformation (DCT) or discrete wavelet transformation (DWT).

However, most of the existing access control methods found in the literature are based on software implementations using MATLAB, which can be complex and time-consuming. While some hardware realizations have been proposed, they often face challenges in terms of high power consumption, suboptimal resource utilization, and limited throughput, making them unsuitable for real-time applications and integration with consumer electronic devices.

Specifically, the following drawbacks have been identified in the existing access control schemes and their hardware implementations:

1. High power consumption: Many hardware implementations fail to prioritize power-aware design techniques, resulting in excessive power consumption, which is undesirable for practical applications.

2. Inefficient resource utilization: Some implementations do not optimize the utilization of hardware resources, leading to increased chip area and higher costs.

3. Limited throughput and operational latency: Certain schemes suffer from low throughput and high operational latency, making them unsuitable for real-time processing of digital multimedia content.

4. Lack of integrability: Many hardware designs are not easily integrable with existing consumer electronic devices, limiting their practical applications.

5. High memory requirements: Some schemes require storing the original host image for detection or extraction purposes, increasing memory requirements and system complexity.

6. Software-based implementations: Software-only schemes implemented using MATLAB or similar tools lack the performance, reliability, and power efficiency of dedicated hardware implementations.

To overcome these limitations and provide an efficient, low-power, high-throughput, and easily integrable solution for access control of digital images, a hardware implementation of a data hiding technique using lifting-based discrete wavelet transformation (DWT) is needs to be implemented.

In the view of the foregoing discussion, it is clearly portrayed that there is a need for an efficient a system and method based on data hiding technique, for efficient quality access control of images.

SUMMARY OF THE INVENTION

The present disclosure relates to a system and method based on data hiding technique, for efficient quality access control of images. The present invention introduces a hardware-based method for efficiently controlling access to images while ensuring quality using lifting-based discrete wavelet transformation (DWT). The process involves decomposing the host image into multiple wavelet tiles, and then embedding a binary watermark into high-quality DWT coefficients using an adaptive dither modulation technique, all without suppressing self-noise. This intentional degradation of visual quality serves as a means of access control. On the decoder side, authorized users can extract watermark bits using minimum distance decoding to obtain a superior quality image. The proposed approach utilizes field-programmable gate array (FPGA) hardware for real-time implementation. Experimental results conducted on a variety of benchmark images demonstrate superior performance compared to existing methods in the literature. Notably, the scheme achieves a substantial 89.53% power saving in real-time processing compared to related implementations, along with a high throughput of 23.8 MB/s for both watermarking encoder and decoder operations, at a maximum operating frequency of 130.14 MHz, specifically tailored for (512×512) sized images.

The present disclosure seeks to provide a system based on data hiding technique, for efficient quality access control of images. The system comprises: an encoder module configured for embedding a watermark into an input image using adaptive dither modulation technique, wherein the encoder module comprises: an encoder image random access memory (RAM) module configured to store image pixels and wavelet coefficients; an encoder discrete wavelet transformation (DWT) module configured to perform lifting-based 2D DWT on the image pixels stored in the image RAM module to obtain DWT coefficients; an encoder dither generation and watermark permutation module configured to generate dither sequences and permute a binary watermark; an embedding module configured to modulate the DWT coefficients obtained from the DWT module using the dither sequences and the permuted watermark from the dither generation and watermark permutation module to embed the watermark into the DWT coefficients; an encoder inverse discrete wavelet transformation (IDWT) module configured to perform IDWT on the watermarked DWT coefficients to obtain watermarked image pixels; and an encoder control unit configured to control the operation of the encoder image RAM module,

encoder DWT module, encoder dither generation and watermark permutation module, embedding module, and encoder IDWT module.

In an embodiment, the system further comprises: a decoder module configured for extracting the embedded watermark from the watermarked image using minimum distance decoding technique, wherein the decoder module comprises: a decoder image random access memory (RAM) module configured to store the watermarked image pixels and wavelet coefficients; a decoder DWT module configured to perform lifting-based 2D DWT on the watermarked image pixels to obtain watermarked DWT coefficients; a decoder dither generation and watermark permutation module configured to generate dither sequences; a watermark extraction module configured to extract the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences; a decoder IDWT module configured to perform IDWT on the watermarked DWT coefficients after watermark extraction to obtain the original image pixels; and a decoder control unit configured to control the operation of the decoder image random access memory (RAM) module, decoder DWT module, decoder dither generation and watermark permutation module, watermark extraction module, and decoder IDWT module.

In an embodiment, both encoder image RAM module and decoder image RAM module comprises a dual-port RAM configured to allow simultaneous read and write operations.

In an embodiment, the encoder and decoder DWT modules, and encoder and decoder IDWT module are configured to perform multi-level wavelet decomposition and reconstruction, respectively.

In an embodiment, the encoder dither generation and watermark permutation module and decoder dither generation and watermark permutation module, both are configured to generate dither sequences based on predefined equations and permute the watermark stored in a read-only memory (ROM).

In an embodiment, the embedding module is configured to modulate selected DWT coefficients using an adaptive dither modulation technique based on the generated dither sequences and the permuted watermark.

In an embodiment, the watermark extraction module is further configured to suppress self-noise from the watermarked DWT coefficients based on the extracted watermark bits.

The present disclosure also seeks to provide a method based on data hiding technique, for efficient quality access control of images. The method comprises: encoding an input image with a watermark, wherein the encoding of an binary image includes transmuting and embedding the binary watermark image into high–high DWT coefficients using adaptive dither modulation technique without self-noise suppression; and decoding the watermarked image to extract the embedded watermark, wherein the decoding of watermarked image includes obtaining superior quality image by extracting watermark bits using minimum distance decoding.

In an embodiment, the encoding method comprises: storing image pixels in an image encoder RAM module; performing lifting-based 2D DWT on the stored image pixels using an encoder DWT module to obtain DWT coefficients; generating dither sequences and permuting a binary watermark using an encoder dither generation and watermark permutation module; embedding the permuted watermark into the DWT coefficients by modulating the DWT coefficients using the generated dither sequences and the permuted watermark in an embedding module; performing IDWT on the watermarked DWT coefficients using an encoder IDWT module to obtain watermarked image pixels; and controlling the operation of the image RAM module, DWT module, dither generation and watermark permutation module, embedding module, and IDWT module using the encoder control unit.

In an embodiment, the decoding process comprises: storing the watermarked image pixels in the decoder image RAM module; performing lifting-based 2D DWT on the watermarked image pixels using the decoder DWT module to obtain watermarked DWT coefficients; generating dither sequences using the decoder dither generation and watermark permutation module; extracting the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences in a watermark extraction module; suppressing self-noise from the watermarked DWT coefficients based on the extracted watermark bits in the watermark extraction module; performing IDWT on the watermarked DWT coefficients after watermark extraction using the decoder IDWT module to obtain the original image pixels; and controlling the operation of the decoder image RAM module, decoder DWT module, decoder dither

generation and watermark permutation module, watermark extraction module, and decoder IDWT module using the decoder control unit.

An objective of the present disclosure is to provide a system and method based on data hiding technique, for efficient quality access control of images.

Another objective of the present disclosure is to a hardware-based method for efficiently controlling access to images while maintaining quality using lifting-based discrete wavelet transformation (DWT).

Another objective of the present disclosure is to achieve minimal resource utilization in the hardware architecture, ensuring efficient implementation of the data hiding scheme for (512×512) sized images.

Another objective of the present disclosure is to ensure very low power consumption, with power requirements estimated at only 78.52 mW for the encoder and 78.45 mW for the decoder.

Yet, another object of the present disclosure is to targets a higher embedding rate, achieving throughputs of 23.819 MB/s for the encoder and 23.835 MB/s for the decoder at operating frequencies of 130.094 MHz and 130.191 MHz, respectively.

To further clarify advantages and features of the present disclosure, a more particular description of the invention will be rendered by reference to specific embodiments thereof, which is illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail with the accompanying drawings.

BRIEF DESCRIPTION OF FIGURES

These and other features, aspects, and advantages of the present disclosure will become better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

Figure 1 illustrates a block diagram of a system based on data hiding technique, for efficient quality access control of images in accordance with an embodiment of the present disclosure;

Figure 2 illustrates a flow chart of a method based on data hiding technique, for efficient quality access control of images in accordance with an embodiment of the present disclosure;

Figure 3A and 3B illustrates diagrams representing block diagram of watermark encoder, and watermark decoder, respectively in accordance with an embodiment of the present disclosure;

Figure 4 illustrates a diagram representing the watermark encoder datapath in accordance with an embodiment of the present disclosure; and

Figure 5 illustrates a diagram representing watermark decoder datapath in accordance with an embodiment of the present disclosure.

Further, skilled artisans will appreciate that elements in the drawings are illustrated for simplicity and may not have been necessarily been drawn to scale. For example, the flow charts illustrate the method in terms of the most prominent steps involved to help to improve understanding of aspects of the present disclosure. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having benefit of the description herein.

DETAILED DESCRIPTION:

For the purpose of promoting an understanding of the principles of the invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended, such alterations and further modifications in the illustrated system, and such further applications of the principles of the invention as illustrated

therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the invention and are not intended to be restrictive thereof.

Reference throughout this specification to “an aspect”, “another aspect” or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. Thus, appearances of the phrase “in an embodiment”, “in another embodiment” and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a process or method that comprises a list of steps does not include only those steps but may include other steps not expressly listed or inherent to such process or method. Similarly, one or more devices or sub-systems or elements or structures or components proceeded by "comprises...a" does not, without more constraints, preclude the existence of other devices or other sub-systems or other elements or other structures or other components or additional devices or additional sub-systems or additional elements or additional structures or additional components.

Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. The system, methods, and examples provided herein are illustrative only and not intended to be limiting.

Embodiments of the present disclosure will be described below in detail with reference to the accompanying drawings.

The functional units described in this specification have been labeled as devices. A device may be implemented in programmable hardware devices such as processors, digital signal processors, central processing units, field programmable gate arrays, programmable array logic, programmable logic devices, cloud processing systems, or the like. The devices may also be

implemented in software for execution by various types of processors. An identified device may include executable code and may, for instance, comprise one or more physical or logical blocks of computer instructions, which may, for instance, be organized as an object, procedure, function, or other construct. Nevertheless, the executable of an identified device need not be physically located together, but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the device and achieve the stated purpose of the device.

Indeed, an executable code of a device or module could be a single instruction, or many instructions, and may even be distributed over several different code segments, among different applications, and across several memory devices. Similarly, operational data may be identified and illustrated herein within the device, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices, and may exist, at least partially, as electronic signals on a system or network.

Reference throughout this specification to "a select embodiment," "one embodiment," or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosed subject matter. Thus, appearances of the phrases "a select embodiment," "in one embodiment," or "in an embodiment" in various places throughout this specification are not necessarily referring to the same embodiment.

Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the following description, numerous specific details are provided, to provide a thorough understanding of embodiments of the disclosed subject matter. One skilled in the relevant art will recognize, however, that the disclosed subject matter can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the disclosed subject matter.

In accordance with the exemplary embodiments, the disclosed computer programs or modules can be executed in many exemplary ways, such as an application that is resident in the

memory of a device or as a hosted application that is being executed on a server and communicating with the device application or browser via a number of standard protocols, such as TCP/IP, HTTP, XML, SOAP, REST, JSON and other sufficient protocols. The disclosed computer programs can be written in exemplary programming languages that execute from memory on the device or from a hosted server, such as BASIC, COBOL, C, C++, Java, Pascal, or scripting languages such as JavaScript, Python, Ruby, PHP, Perl or other sufficient programming languages.

Some of the disclosed embodiments include or otherwise involve data transfer over a network, such as communicating various inputs or files over the network. The network may include, for example, one or more of the Internet, Wide Area Networks (WANs), Local Area Networks (LANs), analog or digital wired and wireless telephone networks (e.g., a PSTN, Integrated Services Digital Network (ISDN), a cellular network, and Digital Subscriber Line (xDSL)), radio, television, cable, satellite, and/or any other delivery or tunneling mechanism for carrying data. The network may include multiple networks or sub networks, each of which may include, for example, a wired or wireless data pathway. The network may include a circuit-switched voice network, a packet-switched data network, or any other network able to carry electronic communications. For example, the network may include networks based on the Internet protocol (IP) or asynchronous transfer mode (ATM), and may support voice using, for example, VoIP, Voice-over-ATM, or other comparable protocols used for voice data communications. In one implementation, the network includes a cellular telephone network configured to enable exchange of text or SMS messages.

Examples of the network include, but are not limited to, a personal area network (PAN), a storage area network (SAN), a home area network (HAN), a campus area network (CAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a virtual private network (VPN), an enterprise private network (EPN), Internet, a global area network (GAN), and so forth.

Figure 1 illustrates a block diagram of a system (100) based on data hiding technique, for efficient quality access control of images in accordance with an embodiment of the present disclosure.

Referring to Figure 1, the system (100) includes an encoder module (102) configured for embedding a watermark into an input image using adaptive dither modulation technique, wherein the encoder module (102) comprises: an encoder image random access memory (RAM) module (104) configured to store image pixels and wavelet coefficients; an encoder discrete wavelet transformation (DWT) module (106) configured to perform lifting-based 2D DWT on the image pixels stored in the image RAM module (102) to obtain DWT coefficients; an encoder dither generation and watermark permutation module (108) configured to generate dither sequences and permute a binary watermark; an embedding module (110) configured to modulate the DWT coefficients obtained from the DWT module (106) using the dither sequences and the permuted watermark from the dither generation and watermark permutation module (108) to embed the watermark into the DWT coefficients; an encoder inverse discrete wavelet transformation (IDWT) module (112) configured to perform IDWT on the watermarked DWT coefficients to obtain watermarked image pixels; and an encoder control unit (114) configured to control the operation of the encoder image RAM module (104), encoder DWT module (106), encoder dither generation and watermark permutation module (108), embedding module (110), and encoder IDWT module (112).

In an embodiment, the system (100) further comprises: a decoder module (116) configured for extracting the embedded watermark from the watermarked image using minimum distance decoding technique, wherein the decoder module (116) comprises: a decoder image random access memory (RAM) module (118) configured to store the watermarked image pixels and wavelet coefficients; a decoder DWT module (120) configured to perform lifting-based 2D DWT on the watermarked image pixels to obtain watermarked DWT coefficients; a decoder dither generation and watermark permutation module (122) configured to generate dither sequences; a watermark extraction module (124) configured to extract the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences; a decoder IDWT module (126) configured to perform IDWT on the watermarked DWT coefficients after watermark extraction to obtain the original image pixels; and a decoder control unit (128) configured to control the operation of the decoder image random access memory (RAM) module (118), decoder DWT module (120), decoder dither generation and watermark permutation module (122), watermark extraction module (124), and decoder IDWT module (126).

In an embodiment, both encoder image RAM module (104) and decoder image RAM module (118) comprises a dual-port RAM configured to allow simultaneous read and write operations.

In an embodiment, the encoder and decoder DWT modules (106 and 120), and encoder and decoder IDWT module (112, and 126) are configured to perform multi-level wavelet decomposition and reconstruction, respectively.

In an embodiment, the encoder dither generation and watermark permutation module (108) and decoder dither generation and watermark permutation module (122), both are configured to generate dither sequences based on predefined equations and permute the watermark stored in a read-only memory (ROM).

In an embodiment, the embedding module (110) is configured to modulate selected DWT coefficients using an adaptive dither modulation technique based on the generated dither sequences and the permuted watermark.

In an embodiment, the watermark extraction module (124) is further configured to suppress self-noise from the watermarked DWT coefficients based on the extracted watermark bits.

Figure 2 illustrates a flow chart of a method (200) based on data hiding technique, for efficient quality access control of images in accordance with an embodiment of the present disclosure.

Referring to **Figure 2**, the method (200) includes pluralities of steps as mentioned below,

At step (202), the method (200) includes encoding an input image with a watermark, wherein the encoding of an binary image includes transmuting and embedding the binary watermark image into high–high DWT coefficients using adaptive dither modulation technique without self-noise suppression.

At step (204), the method (200) includes decoding (204) the watermarked image to extract the embedded watermark, wherein the decoding of watermarked image includes obtaining superior quality image by extracting watermark bits using minimum distance decoding.

In an embodiment, the encoding method comprises: storing image pixels in an image encoder RAM module (104); performing lifting-based 2D DWT on the stored image pixels using an encoder DWT module (106) to obtain DWT coefficients; generating dither sequences and permuting a binary watermark using an encoder dither generation and watermark permutation module (108); embedding the permuted watermark into the DWT coefficients by modulating the DWT coefficients using the generated dither sequences and the permuted watermark in an embedding module (110); performing IDWT on the watermarked DWT coefficients using an encoder IDWT module (112) to obtain watermarked image pixels; and controlling the operation of the image RAM module (104), DWT module (106), dither generation and watermark permutation module (108), embedding module (110), and IDWT module (112) using the encoder control unit (114).

In an embodiment, the decoding process comprises: storing the watermarked image pixels in the decoder image RAM module (118); performing lifting-based 2D DWT on the watermarked image pixels using the decoder DWT module (120) to obtain watermarked DWT coefficients; generating dither sequences using the decoder dither generation and watermark permutation module (122); extracting the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences in a watermark extraction module (124); suppressing self-noise from the watermarked DWT coefficients based on the extracted watermark bits in the watermark extraction module (124); performing IDWT on the watermarked DWT coefficients after watermark extraction using the decoder IDWT module (126) to obtain the original image pixels; and controlling the operation of the decoder image RAM module (118), decoder DWT module (120), decoder dither generation and watermark permutation module (122), watermark extraction module (124), and decoder IDWT module (126) using the decoder control unit (128).

Figure 3A and 3B illustrates diagrams representing block diagram of watermark encoder, and watermark decoder, respectively in accordance with an embodiment of the present disclosure.

The purpose of watermark embedding is to insert a watermark into the host image to enable quality access control. Conversely, the decoder's role is to extract the embedded watermark and subsequently eliminate self-noise, resulting in an improved quality host image.

Watermark Encoding:

Figure 2A illustrates the image encoding process. In this method, a binary watermark (W) of size (n × n) undergoes a transmutation process via an XOR operation using a 2-D random key (K). The W' represents the output after the XOR operation. Subsequently, the host image (m × m) undergoes a 3-level 2D-DWT transformation using a lifting scheme. From the resulting sub-bands (low–low (LL), high–low (HL), low–high (LH), and high–high (HH)), a group of 24 coefficients is selected for embedding the 1-bit watermark. Specifically, four coefficients are chosen from LL, HL3, LH3, and HH3 each, four coefficients from HH2, and the remaining 16 coefficients from HH1 sub-band.

These selected coefficients are then grouped into 'g' number of categories (g = 5 in the present invention). Consequently, 'g' different step sizes (ΔS) are chosen to calculate binary dither sequences, with the smallest step size utilized for modulating the LL sub-band due to its containing the most visual information of the image. Conversely, the largest step size (ΔL) is used for the HH sub-band. Intermediate step sizes (ΔL to ΔS) are chosen for modifying the other sub-bands accordingly. Based on the step size value (ΔS), dither sequences are generated for quantization index modulation (QIM). The transmuted watermark (W') is then embedded into the different sub-bands of DWT coefficients. Finally, inverse DWT (IDWT) is performed on the watermarked coefficients to regenerate the watermarked image.

Watermark Decoding:

The decoding process, depicted in Fig. 2B, is essentially the reverse of the encoding process and operates on the principle of minimum distance decoding. Specifically, it calculates the distance between the dither sequences $d_{g,q}(0)$ and $d_{g,q}(1)$. The permuted watermark bit $\tilde{W}(i, j)$ is then decoded, where a larger distance between SA and SB indicates a lower probability of decoding error, thus ensuring better quality access control for the digital image.

Subsequently, $\tilde{W}(i, j)$ is subjected to an XORed operation with 'K' to recover the decoded version of the watermark ($\hat{W}$). Finally, the process involves eliminating self-noise to achieve the final, improved quality version of the decoded watermark.

The increasing demand for low-power portable communication systems necessitates new low-power techniques, particularly for FPGA (Field-Programmable Gate Array) designs. Despite FPGA-based designs consuming more power than fixed logic FPGAs, they remain an attractive option for designers due to their cost-effectiveness and reconfigurability. The proposed hardware design aligns with both the international technology roadmap for semiconductors (ITRS) and the power-aware hardware description language (HDL) technique to achieve low power consumption.

Below given description describes the proposed data paths of the DWT (lifting)-based quality access control encoder and decoder.

The data paths of the access control encoder and decoder are designed using the very high-speed integrated circuit hardware description language (VHDL) and implemented on the Xilinx Zynq (XC7Z020-CLG484-1) FPGA platform. The architecture is constructed by configuring different modules separately, with the encoder and decoder architecture being symmetrically designed.

The proposed encoder module comprises:

- 'Image_RAM': for storing image data

- Lifting-based DWT/IDWT (Discrete Wavelet Transform/Inverse DWT): for image transformation

- 'Dither Generation and Watermark Permutation': for generating dither sequences and permuting the watermark

- 'Embed_block': for embedding the watermark into DWT coefficients

- Finite-state machine (FSM)-based 'Control Unit': for synchronization and timing control

Similarly, the decoder module includes:

- 'Image_RAM': for storing image data

- Lifting-based DWT/IDWT: for image transformation

- 'Dither Generation': for generating dither sequences

- 'W_Extraction': for extracting the watermark

- FSM-based 'Control Unit': for synchronization and timing control

Each hardware component is designed, tested, and optimized separately before integration for encoding and decoding operations. During implementation, it's crucial to ensure that individual components are activated only when necessary; otherwise, they should remain disabled to conserve power.

Figure 4 illustrates a diagram representing the watermark encoder datapath in accordance with an embodiment of the present disclosure.

Referring to **Figure 4**, the watermark encoder data path involves several key steps:

1. Image Preloading: Initially, the encoder assumes that the image (N × N) pixels are preloaded into the 'Image_RAM.' This acts as the starting point for the encoding process.

2. External Input Interface: Additionally, the user has the option to include an external input bus as an interface at 'Image_RAM,' allowing for real-time implementation and data input.

3. Storage of Watermark and Random Keys: The watermark and random keys are stored in separate read-only memories (ROMs), which serve as inputs to the encoder. These keys are essential for the encoding algorithm.

4. 2-D DWT Transformation: The next step involves performing a lifting-based 2-D Discrete Wavelet Transform (DWT) on each (512 × 512) sized image block. This transformation decomposes the image into its frequency components, generating DWT coefficients.

5. Storage of DWT Coefficients: The resulting DWT coefficients are then stored back into the 'Image_RAM.' This storage step is crucial for further processing and manipulation of the image data.

6. Adaptive Dither Modulation: Selected coefficients from the 'Image_RAM' undergo modulation using an adaptive dither modulation technique, as described in Algorithm 1. This

modulation process embeds the watermark into the DWT coefficients, integrating the external information into the host image.

This detailed sequence of operations forms the core data path of the watermark encoder, ensuring the efficient and effective embedding of the watermark into the host image while maintaining data integrity and quality. Each of these mentioned key steps are further elaborated in the description given below.

The hardware architecture detailed below comprises several crucial components and operations designed for efficient image processing and watermark embedding.

The "Image_RAM" module functions as a dual-port random-access memory (RAM) designed using VHDL programming techniques based on power-aware design principles. It is specifically tailored to store image pixels, intermediate Discrete Wavelet Transform (DWT) coefficients, and Inverse DWT (IDWT) pixels. Configured for (512×512) pixels with an 8-bit depth per pixel, this module facilitates simultaneous reading and writing operations at different memory cells. Two separate address buses enable efficient selection of addresses for read and write operations, controlled by a dedicated 'wr_en' line. Input and output 8-bit data buses ('pixel_in' and 'pixel') manage data storage and retrieval. During prototype implementation, image pixel data is loaded into 'Image_RAM' from a text file, ensuring a streamlined process. The module is designed to accommodate real-time implementation and can integrate with an external image sensor module for added functionality, although this aspect is not considered in the prototype implementation for simplicity.

The "DWT/IDWT Block," it forms a critical part of both the encoder and decoder modules. This block implements a lifting-based 2-D DWT, a key operation in the encoding and decoding processes. The lifting-based DWT reduces implementation complexity, enhancing efficiency by minimizing arithmetic operations and memory accesses. Utilizing VHDL language and FPGA-based implementation, the block's hardware design is optimized for resource utilization, speed, and power consumption. It operates at a frequency of 174.630 MHz, performing the DWT of the (512×512) image. The IDWT, which reverses the DWT process, is also implemented seamlessly within this block.

Within the "Dither Generation and Watermark Permutation Block," dither sequences are generated alongside the permutation of the watermark. These sequences and the permuted watermark, derived from a pre-stored watermark in 'watermark_ROM' within the block, are then processed for watermark embedding using DWT coefficients modulation. This process is pivotal for embedding the watermark into the image data effectively.

The "Embed Block" functions to modulate selected coefficients as per the watermark embedding algorithm. Once modified, these watermarked coefficients are then transferred back to the 'Image_RAM' for storage and further processing.

Lastly, the "Encoder Control Unit Block" orchestrates the watermark embedding process. Utilizing a Finite State Machine (FSM), it provides synchronization and timing signals to ensure sequential watermark embedding at selected DWT coefficients. The control unit follows a defined sequence of states, from initializing the DWT to modulating coefficients, and finally computing the IDWT. Each state is meticulously designed to access 'Image_RAM' for reading and writing operations, maintaining efficiency throughout the watermark embedding process.

Figure 5 illustrates a diagram representing watermark decoder datapath in accordance with an embodiment of the present disclosure.

In accordance to the **Figure 5**, a detailed description of the decoding process is given below.

The process of decoding the watermark involves reversing the embedding process to extract the watermark information accurately. The decoding algorithm outlines the steps for extracting the watermark from the watermarked image. Initially, the watermarked image undergoes a three-level Discrete Wavelet Transform (DWT). Subsequently, different combinations of dither sequences ('D0' and 'D1') are generated on-chip based on various step sizes. The "W_Extraction" block then calculates the minimum distance between incoming dither sequences to predict the watermark bit accurately. The extracted watermark is stored in 'W_RAM' for further processing. Following this, an Inverse DWT (IDWT) is performed on the extracted coefficients to retrieve the original image pixels. The data path for the watermark extraction block mirrors the embedding data path, ensuring a symmetrical decoding process.

The "Watermark Decoding Control Unit Block" is responsible for managing the timing and control signals for each component of the decoder module. Utilizing a Finite State Machine (FSM), the decoding process is structured into fourteen distinct states. The decoding process initiates with a 'start' trigger pulse. The FSM follows a sequence of states similar to the encoder control unit, except for one state in which, the watermark bit extraction is performed by computing S_A(S_A= [image_ram] - [(Y| [[image_ram] + (D0)]/Y|) - D0];) and S_B(S_B= [image_ram] - [(Y| [[image_ram] + (D1)]/Y|) - D1];) and determining the presence or absence of self-noise in the DWT coefficient based on the extracted bit (0 or 1). The processed DWT coefficients are then stored back into the corresponding location in 'Image_RAM.' The extracted watermark is reverse-permuted and stored in 'W_RAM.' Subsequently, the IDWT is computed and upon the completion of computation of IDWT, the program control transitions to an idle state. Throughout the decoding process, the dual-port 'Image_RAM' is efficiently managed, ensuring proper read and write control signals at each state for seamless operation.

A performance evaluation was conducted using a CPU, operating at 1.7 GHz with 8 GB of RAM, running a 64-bit operating system. The simulations were carried out using simulation software for e.g MATLAB and the hardware design was implemented using Xilinx tools, specifically ISE Design Suite 14.5 and Vivado 2014.2 design suite. Initially, the effectiveness of the quality access control scheme was tested through software simulations. Subsequently, a prototype hardware design was implemented on an FPGA to further assess the performance of the scheme.

The evaluation of the quality access control scheme involved testing it on a variety of benchmark images, including popular ones like Lena, Baboon, Boat, and Pepper, all sized at (512×512) pixels with 8-bit grayscale. The scheme used three levels of DWT decomposition and a dither length of 24, with specific step sizes for different sub-bands. Performance was assessed using peak-signal-to-noise ratio (PSNR), mean structural similarity index measure (MSSIM), and Kullback–Leibler distance (KLD) for distortion and security measurements.

From the PSNR and MSSIM values for the four popular test images, it is observed that the Lower PSNR values indicated poorer image quality for unauthorized users. However, the KLD values demonstrated high security against noise. On the other hand, authorized users with the correct key could decode images with good PSNR values.

Additionally, it is observed that the image quality variation after self-noise elimination for different watermark sizes, averaged over multiple experiments. The scheme's robustness was tested against various image processing operations and noise additions, with results showing that the scheme performed well against 'Salt & Pepper' and 'Speckle' noise compared to Gaussian noise, indicating robustness to noise additions.

Furthermore, it is observed that NCC values increases with JPEG quality factor, demonstrating robustness, PSNR values improves after decoding, highlighting the scheme's robustness. A comparative analysis of embedding methods, domains, fidelity, capacity, and hiding techniques, emphasizes the proposed scheme's robustness despite lower capacity compared to other techniques.

In summary, the software simulation results showcased the scheme's effectiveness in quality access control, robustness to various image processing operations and noise additions, and its security against unauthorized access.

In an implementation, a hardware realization is carried out of the proposed system for encoding and decoding, wherein implementation is carried out on Xilinx Zynq (XC7Z020-CLG484-1) series FPGA target board. The timing simulations were conducted using the Xilinx ISE simulator, while the design underwent characterization in the Vivado 14.2 design suite with various synthesis constraints. The VLSI implementation specifically focused on watermark embedding and extraction for 8-bit grayscale images of different sizes. This design framework is adaptable for larger images (N × N) to facilitate real-time applications, either through full parallel processing or a combination of parallel and pipelined architectures. The architectural cost assessment in FPGA involved evaluating fundamental components such as slice flip-flops, LUTs, multiplexers (MUX), and BRAMs. However, the encoding and decoding operations have occurred separately. The encoder and decoder efficiency in terms of data rate is calculated.

The hardware implementation of the (512×512) image encoder and decoder achieved an impressive embedding rate of 23.819 Mbps and a decoding rate of 23.835 Mbps, respectively. The power consumption analysis revealed that the system operated at a remarkably low power level, with static power being dependent on design resources and dynamic power influenced by effective capacitance, resource utilization, and switching activity.

Using the Xilinx X power analyzer (XPA), the total power consumption for encoding and decoding was calculated to be 78.52 mW and 78.45 mW, respectively, indicating efficient power utilization in the proposed architecture. Throughput analysis demonstrated competitive performance, with a throughput of 23.827 MB/s, comparable to other FPGA-based implementations.

Resource utilization and power consumption were significantly lower compared to related work, with the proposed DWT-based access control hardware saving 89.536% and 22.29% of power compared to other hardware-based implementations. The design operated at a frequency of 130.14 MHz and consumed only 78.48 mW of power.

Trade-offs among area, power, and frequency were evaluated, showcasing an increase in effective power consumption and area with higher frequencies. The simulated web form illustrated the encoding and decoding processes, emphasizing the system's low power consumption, high throughput, and minimal FPGA resource utilization.

Overall, the hardware implementation demonstrated efficient power management, competitive throughput, and minimal resource utilization, making it an attractive option for low-power reconfigurable access control applications.

The drawings and the forgoing description give examples of embodiments. Those skilled in the art will appreciate that one or more of the described elements may well be combined into a single functional element. Alternatively, certain elements may be split into multiple functional elements. Elements from one embodiment may be added to another embodiment. For example, orders of processes described herein may be changed and are not limited to the manner described herein. Moreover, the actions of any flow diagram need not be implemented in the order shown; nor do all of the acts necessarily need to be performed. Also, those acts that are not dependent on other acts may be performed in parallel with the other acts. The scope of embodiments is by no means limited by these specific examples. Numerous variations, whether explicitly given in the specification or not, such as differences in structure, dimension, and use of material, are possible. The scope of embodiments is at least as broad as given by the following claims.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and

any component(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or component of any or all the claims.

CLAIMS:

1. A system (100) based on data hiding technique for efficient quality access control of images, comprising:

an encoder module (102) configured for embedding a watermark into an input image using adaptive dither modulation technique, wherein the encoder module (102) comprises:

an encoder image random access memory (RAM) module (104) configured to store image pixels and wavelet coefficients;

an encoder discrete wavelet transformation (DWT) module (106) configured to perform lifting-based 2D DWT on the image pixels stored in the image RAM module (102) to obtain DWT coefficients;

an encoder dither generation and watermark permutation module (108) configured to generate dither sequences and permute a binary watermark;

an embedding module (110) configured to modulate the DWT coefficients obtained from the DWT module (106) using the dither sequences and the permuted watermark from the dither generation and watermark permutation module (108) to embed the watermark into the DWT coefficients;

an encoder inverse discrete wavelet transformation (IDWT) module (112) configured to perform IDWT on the watermarked DWT coefficients to obtain watermarked image pixels;

an encoder control unit (114) configured to control the operation of the encoder image RAM module (104), encoder DWT module (106), encoder dither generation and watermark permutation module (108), embedding module (110), and encoder IDWT module (112);

a decoder module (116) configured for extracting the embedded watermark from the watermarked image using minimum distance decoding technique, wherein the decoder module (116) comprises:

a decoder image random access memory (RAM) module (118) configured to store the watermarked image pixels and wavelet coefficients;

a decoder DWT module (120) configured to perform lifting-based 2D DWT on the watermarked image pixels to obtain watermarked DWT coefficients;

a decoder dither generation and watermark permutation module (122) configured to generate dither sequences;

a watermark extraction module (124) configured to extract the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences;

a decoder IDWT module (126) configured to perform IDWT on the watermarked DWT coefficients after watermark extraction to obtain the original image pixels; and

a decoder control unit (128) configured to control the operation of the decoder image random access memory (RAM) module (118), decoder DWT module (120), decoder dither generation and watermark permutation module (122), watermark extraction module (124), and decoder IDWT module (126).

2. The system (100) of claim 1, wherein both encoder image RAM module (104) and decoder image RAM module (118) comprises a dual-port RAM configured to allow simultaneous read and write operations.

3. The system (100) of claim 1, wherein the encoder and decoder DWT modules (106 and 120), and encoder and decoder IDWT module (112, and 126) are configured to perform multi-level wavelet decomposition and reconstruction, respectively.

4. The system (100) of claim 1, wherein the encoder dither generation and watermark permutation module (108) and decoder dither generation and watermark permutation

module (122), both are configured to generate dither sequences based on predefined equations and permute the watermark stored in a read-only memory (ROM).

5. The system (100) of claim 1, wherein the embedding module (110) is configured to modulate selected DWT coefficients using an adaptive dither modulation technique based on the generated dither sequences and the permuted watermark.

6. The system (100) of claim 1, wherein the watermark extraction module (124) is further configured to suppress self-noise from the watermarked DWT coefficients based on the extracted watermark bits.

7. A data hiding technique-based method (200) for efficient quality access control of images, comprising:

encoding (202) an input image with a watermark, wherein the encoding of an binary image includes transmuting and embedding the binary watermark image into high–high DWT coefficients using adaptive dither modulation technique without self-noise suppression; and

Decoding (204) the watermarked image to extract the embedded watermark, wherein the decoding of watermarked image includes obtaining superior quality image by extracting watermark bits using minimum distance decoding.

8. The method as claimed in claim 7, wherein the encoding method comprises:

storing image pixels in an image encoder RAM module (104);

performing lifting-based 2D DWT on the stored image pixels using an encoder DWT module (106) to obtain DWT coefficients;

generating dither sequences and permuting a binary watermark using an encoder dither generation and watermark permutation module (108);

embedding the permuted watermark into the DWT coefficients by modulating the DWT coefficients using the generated dither sequences and the permuted watermark in an embedding module (110);

performing IDWT on the watermarked DWT coefficients using an encoder IDWT module (112) to obtain watermarked image pixels; and

controlling the operation of the image RAM module (104), DWT module (106), dither generation and watermark permutation module (108), embedding module (110), and IDWT module (112) using the encoder control unit (114).

9. The method as claimed in claim 7, wherein the decoding process comprises:

storing the watermarked image pixels in the decoder image RAM module (118);

performing lifting-based 2D DWT on the watermarked image pixels using the decoder DWT module (120) to obtain watermarked DWT coefficients;

generating dither sequences using the decoder dither generation and watermark permutation module (122);

extracting the embedded watermark from the watermarked DWT coefficients by computing minimum distances between the watermarked coefficients and the generated dither sequences in a watermark extraction module (124);

suppressing self-noise from the watermarked DWT coefficients based on the extracted watermark bits in the watermark extraction module (124);

performing IDWT on the watermarked DWT coefficients after watermark extraction using the decoder IDWT module (126) to obtain the original image pixels; and

controlling the operation of the decoder image RAM module (118), decoder DWT module (120), decoder dither generation and watermark permutation module (122), watermark extraction module (124), and decoder IDWT module (126) using the decoder control unit (128).

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

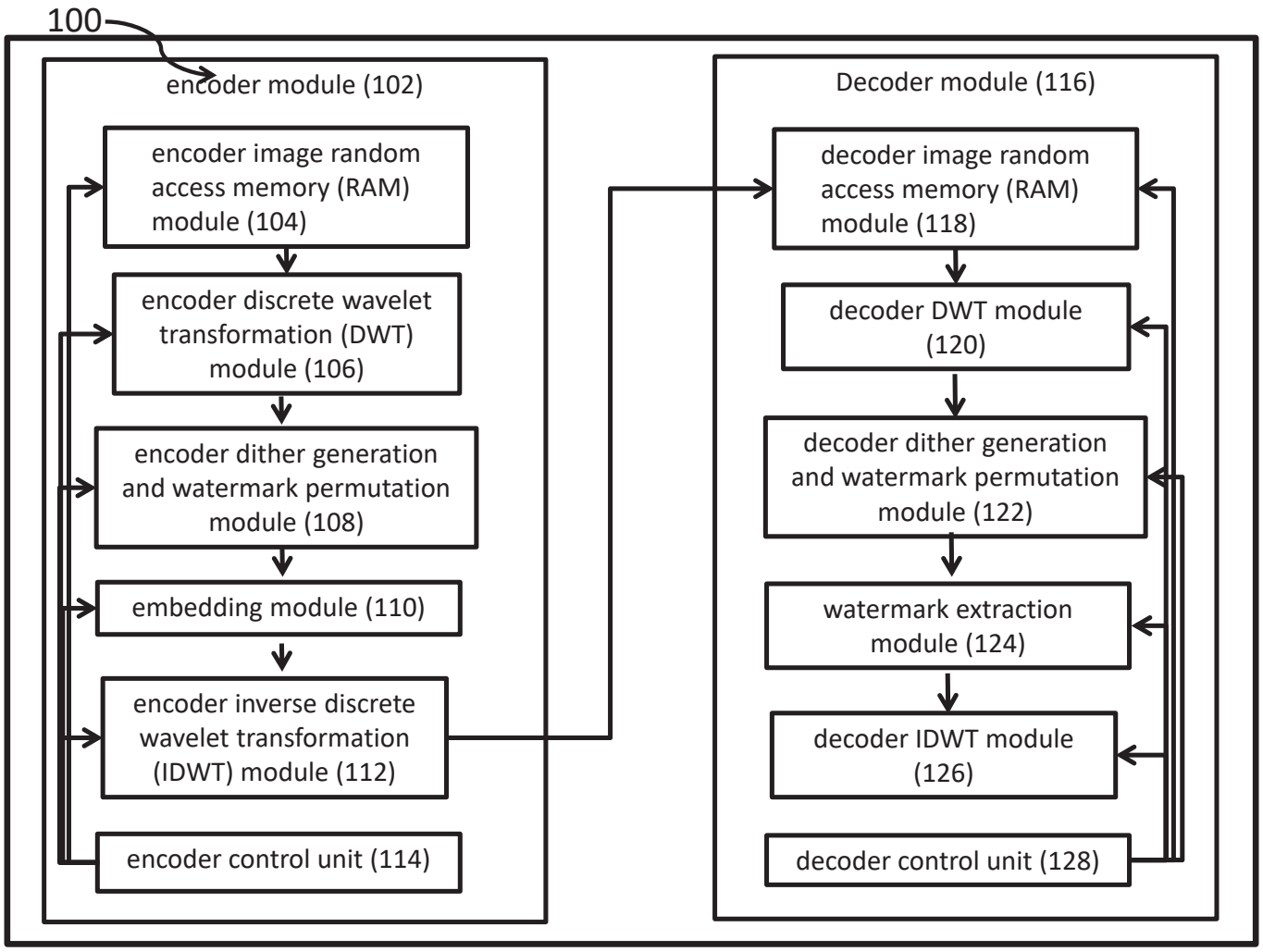

Figure 1

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

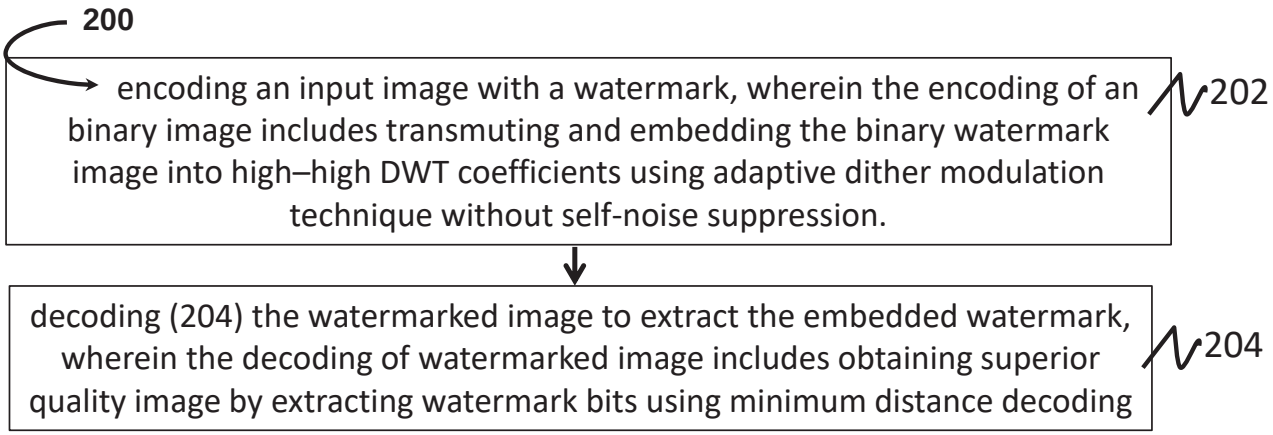

Figure 2

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

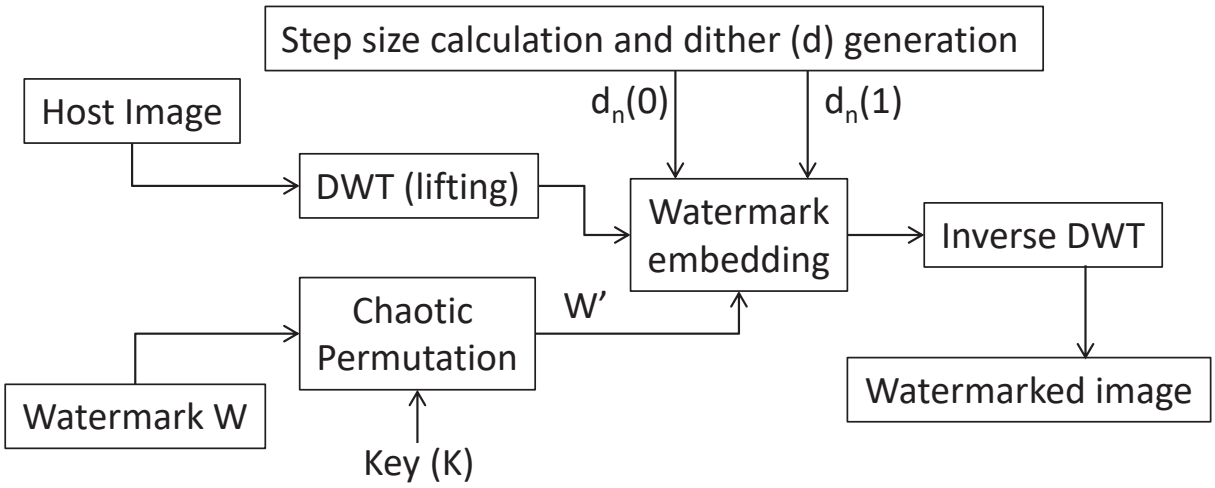

Figure 3A

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

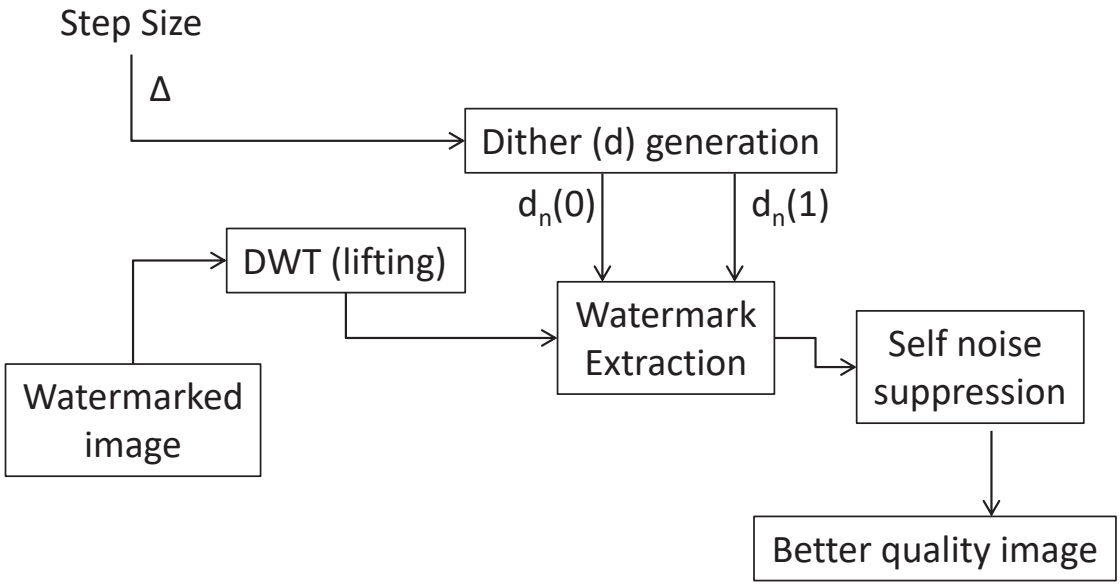

Figure 3B

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

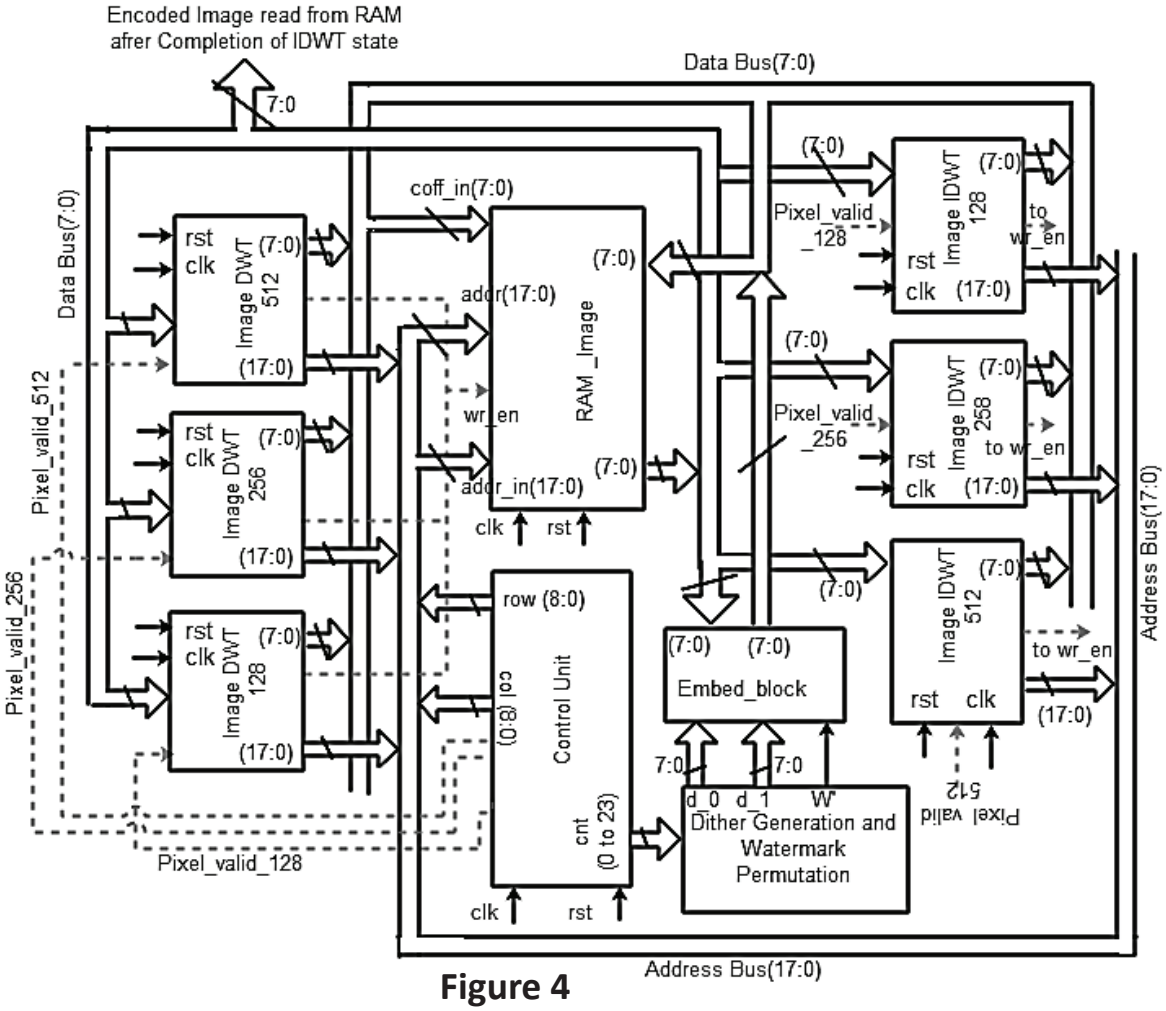

Figure 4

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR;
DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR;
DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH;
DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY;
CALCUTTA INSTITUTE OF TECHNOLOGY;
UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA;
BRAINWARE UNIVERSITY

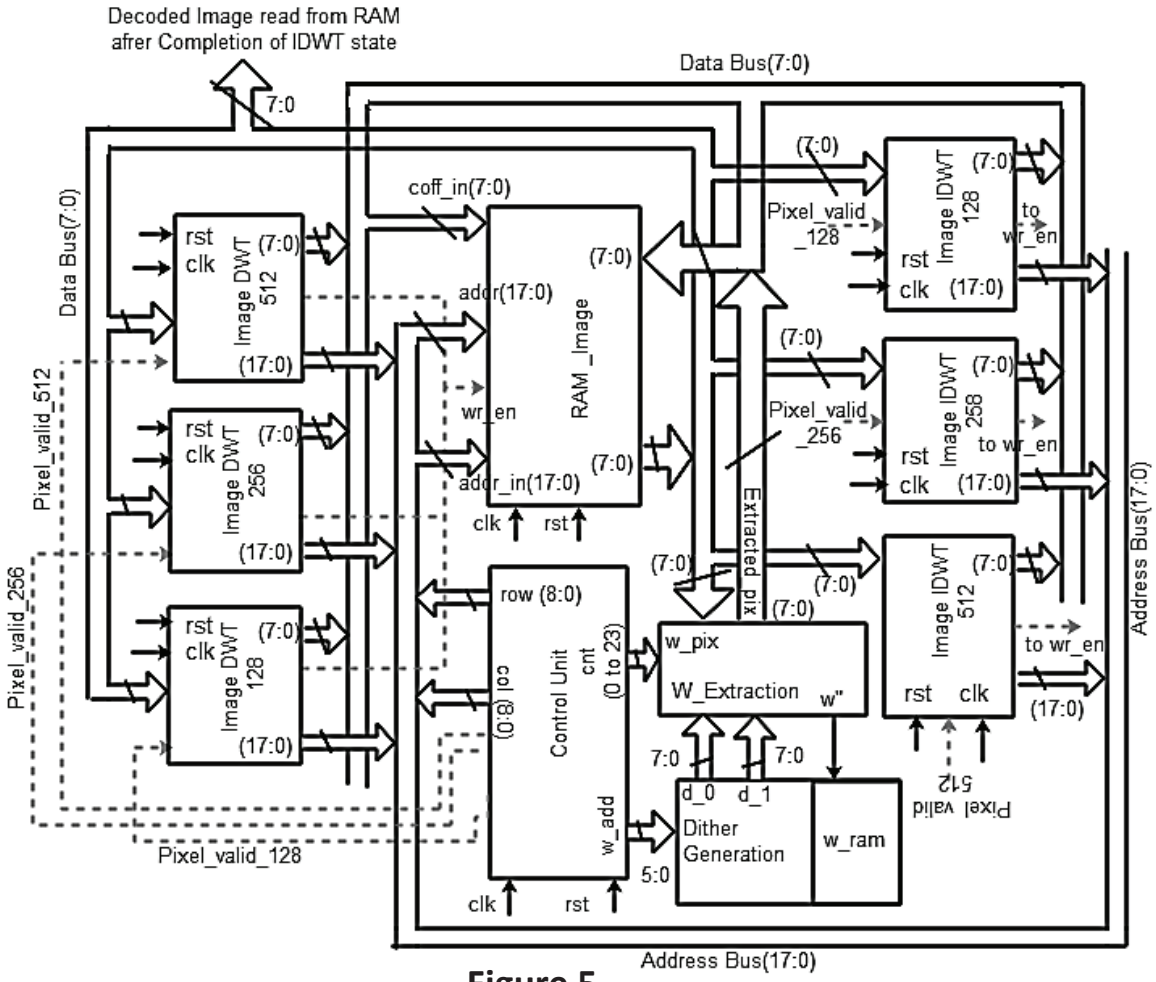

Figure 5

REPUBLIC OF SOUTH AFRICA

REPUBLIEK VAN SUID AFRIKA

PATENTS ACT, 1978

CERTIFICATE

In accordance with section 44 (1) of the Patents Act, No. 57 of 1978, it is hereby certified that:

DR. HIMADRI MANDAL; DR. AMIT PHADIKAR; DR. GOUTAM KUMAR MAITY; DR. ANGSHUMAN MAJUMDAR; DR. RAMKRISHNA RAKSHIT; DR. ANIRUDDHA GHOSH; DR. SUBHALAXMI CHAKRABORTY; ATANU CHOWDHURY; CALCUTTA INSTITUTE OF TECHNOLOGY; UNIVERSITY OF ENGINEERING AND MANAGEMENT, KOLKATA; BRAINWARE UNIVERSITY

Has been granted a patent in respect of an invention described and claimed in complete specification deposited at the Patent Office under the number

2024/06065

A copy of the complete specification is annexed, together with the relevant Form P2.

In t[illegible]ony thereof, the seal of the Patent Office has been affixed at Pretoria with effect from the 26th day of **February 2025**

.....

Registrar of Patents