Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 30 No. 4 (2023)

Mathematical Model of Enhanced Aerial Image Quality and Security through Wavelet-Based Dynamic Range Compression and Watermarking Techniques

Dr. Akash Saxena [1], Gaurav Kumar Das[2], Pragati Modi [3]

[1] Professor, Department of Computer Science, Compucom Institute of Technology and Management, Jaipur- Rajasthan (India)

[2]Assistant Professor, Department of Computer Science, Compucom Institute of Technology and Management, Jaipur- Rajasthan (India)

[3] M. Tech. Scholar, Department of Computer Science, Compucom Institute of Technology and Management, Jaipur- Rajasthan (India)

Email: akash27jaipur@gmail.com, gaurav.rush22002@gmail.com, Pragatimodi10@gmail.com

Article History:

Received: *24-08-2023*

Revised: *04-10-2023*

Accepted: *28-10-2023*

Abstract:

This research introduces a novel wavelet-based dynamic range compression system tailored for improving the visual quality of digital photographs taken in high dynamic range environments with non-uniform lighting. Primarily designed for aerial photography in defense and security applications, this method excels in preserving local contrast and tonal rendition while efficiently managing dynamic range, making it highly suitable for aviation industry video streaming. A key advancement of this research is the development of an algorithm capable of enhancing aerial images to a quality that surpasses direct human observation in terms of clarity and robustness. Additionally, the research presents an innovative watermarking technique utilizing Local Binary Patterns (LBP) and Discrete Wavelet Transform (DWT). This approach employs the LBP operator in conjunction with wavelet approximation coefficients to generate a resilient binary watermark. The focus is on establishing more reliable watermarking methods to ensure enhanced security and resilience of embedded information. The study explores the application of public watermarking to facilitate easy access and comprehension of copyright and patent information, highlighting the technology's efficacy in protecting sensitive image data. The research further investigates the enhancement of neural network performance in watermarking applications using Gray Level Co-occurrence Matrix (GLCM) and Principal Component Analysis (PCA) algorithms. PCA is utilized for image selection, while GLCM aids in feature extraction from the original image. The performance of the PCA algorithm is assessed based on its implementation's scaling factor.Through simulations, the proposed algorithm demonstrated impressive results, especially in terms of Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and correlation coefficients, confirming its potential in improving image quality and security in aerial photography and related applications. This study represents a significant advancement in the fields of image processing and digital security, offering new tools and methodologies for enhancing the quality and protection of aerial imagery.

Keywords: Image Processing, PSNR, Image Watermarking, Image Enhancement, Discrete Wavelet Transform, Discrete Cosine Transform, LBP, GLCM, PCA.

1. INTRODUCTION

The processing of images is known as the input images production process at a specific location. It is comprised of metric and topological edges to examine and crack the edges for structure building between image pixels. The captured amplitude is different from the tiny surrounding pixel border. In this image, processing this pixel boundary is a very significant concept. The image is visible from sinkhole and image processing is completely knowledge-based and implemented. The choices are made by using an information-driven system of human cognition. The degradation percentage is determined by evaluating image quality. Two factors decide the quality of the image:

- Subjective for TV technology
- Objective quantitative assessment techniques for our purposes are more appealing

Similar images are very important because they help images from the appropriate database to be retrieved. The captured or the original is destroyed and degraded by sounds in the background. This occurs during image capture, material transfer. The understanding of human facial color is another important layer for researching the characteristics of electromagnetic radiation to address the physical appearance of humans. The client and the server are transmissible. It also stores graphical information and the processing parameter is shown in each graph node.

The image processing goals can be broken down into five groups:

- Hallucination (monitor not visible objects)
- Restore and sharpen photos (for better photo creation.)
- Photo repossession (photo search).
- Pattern measurement (measures a variety of items in a picture).
- Recognition of images (distinguish objects in an image)

Various methods for the transfer of image data are implemented, one of which is the imaging system. Mostly however, people use their pictures on many social applications, from which some unauthorized users can copy and hack them. For a better use of such applications, people use them on their computers or on mobile phones. These frames either use or combine the encryption process or the stenographic process. There are numerous encoding methods available, which are specifically designed to secure images from hackers. As a large [5] amount of data is traceable. The data can be protected from being hacked by numerous authentication or security features.

1. **Encryption:** Transforms the simple text into cipher text with the aid of the secret key. The image can be converted into encrypted format with the secret key. This converted encrypted image is sent out to the unsecured medium at its desired place.
   - Cryptography: Original images are translated to other images in this type of image encryption such that someone else can hardly understand and maintain confidentiality among users. It uses an encoded and transformed simple text form that uses an unreadable digital key, and that entire process is called Cryptography
   - Cryptography with secret key: it adopts an individual encryption key. This allows the sender to encrypt messages with this single key, and the recipient to decrypt the information with that specific key on the receiving end.
   - Public Key Cryptography (CPK): In this type of cryptography, it includes two types of cryptosystems used to establish a sender-receiver-source communication via unprotected network forms. In order to perform encryption, n these different keys are used and hence are known as asymmetric cryptosystems. Public and private keys [7] that communicate publicly and privately are available.

- Hash Functions (HFs): It is implemented to check the completeness of messages in order to ensure the message is not altered or compromised by any virus. An image is also an essential part of the details.

2. Steganography: Steganography is used to interact invisibly. The initial images are filled with masks from intrusion or contact with the intruder / hacker, and the filled image is then called the stego image.

3. Watermarking: There are many watermarking applications including content archiving, temperature tracking, copyright protection, meta-data insertion and broadcast monitoring, both visual and secret signatures in this case are incorporated.[31]

Watermarking is one of the most effective images processing techniques. It has many different applications and some of them are listed below:

- **Defense of copyright:** copyright material is used for the integration of information into a new development. If there is some conflict about ownership, the watermark can be withdrawn and the proprietor is expected to provide proof.
- **Content Authentication:** authentication of content is necessary for. It prevents unauthorized access to the watermark by an unauthorized user.[12]
- **Broadcast monitoring:** The use of the content as a deal between the advertising agency and the client is made more regular in advertising.
- **Owner Identify:** Conventional approaches are used to verify the owner with visual markings. Some sophisticated software that can change the images can be easily overcome.
- **Fingerprinting:** Consumer security is based on fingerprinting. The transaction is focused on the integration of a single, robust watermark of each recipient when the customer obtained a legal copy of any product, and he started selling it illegally on the market. Those who redistribute the commodity can easily be marked and the watermark retrieved by the owner.
- **Medical applications:** in the medical industry, watermarking plays an important role. This is used to secure the sensitive reports that any unauthorized party receives from the patient. In the event of a patient losing them, t can be used to locate all details and reports about every patient. t preserves medical image copyright. In tele medicine, where images easily spread over the internet, this security and authentication are very common.

2. LITERATURE REVIEW

[Mahbuba Begum, et-al 2020] proposed that digital image watermarking is an attractive research field because it provides protection against unauthorized access to multimedia images. In this paper an overview of existing digital hybrid image watermarking techniques has been presented. Initially, we presented a standard structure for the creation of a hybrid solution to ensure basic watermarking design criteria for different applications. Contrasted and evaluated in a tabular form the sophistication of many hybrid approaches that occur after a brief literary analysis. There are also the drawbacks and uses of these techniques. **[Shrinivas, et-al 2020**]proposed that suggested copyright-based digital picture watermarking (DCT) technique for transform-(DWT) and discrete cosine (DCT).Here we can encrypt the watermark picture with the Arnold framework and can calculates block-based DCT of transform.DWT LL sub band that offers better visual output of the human eye image. The watermark is built into this DCT coefficient into the host infrequency image. It is also a versatile framework for different attacks performs better than a DCT-based solution. **[Challa, et-al 2020**]proposed the technology for hybrid watermarking based on SVD-DWT. On DWT. The fusion algorithm of the Wavelet is used here using DWT and SVD to insert the watermark there is a sturdy and imperceptible device. With capability enhancement converting the lifting wavelet in the analysis (LWT) and DCT. **[Wazid, et-al 2020**] proposed that there is telemedicine technology medical data to be transferred as network medical data management. This paper uses a hybrid approach of robustness and protection DWT and DCT are combined. The medical host picture is here divided into two parts: Non-Interest Area (NROI) and Interest area (ROI). More pictures are watermarks incorporated in the ROI part, the word watermark is built into part of the NROI. **[Noor Zaman, et-al, 2018]** has developed a lightweight security authentication model that provides security against multiple attacks such as IOT attacks by Impersonation, middle attackers, and unknown IOT-based key share attacks. Applications based on IOT-based e-health groupings presented a secure Lightweight Authentication Scheme. The proposed model offers an IOT-based authentication, energy efficiency method and healthcare measurement. This uses the ECC principle, which defines the characteristics of the model proposed. **[Muhammad NaveedAman, et-al, 2017]** has an effective stable IOT systems authentication protocol. In order to provide protection, the proposed protocol uses an unexpected physical feature. The proposed protocol is not only effective in preventing various attacks, but also in managing memory, computations, energy and communication. The author implemented a shared IOT device authentication protocol. **[Mehdi Bahrami, et-al, 2016]**The cloud method proposed by is useful for the users who outsource their data. The security framework is very critical if data is to be transmitted through a cloud server. The author proposed to protect the contents of the original data using a pseudo-random permutation process. For other encryption techniques, they are not so cost-effective and too costly. **[Gaurav Bansod, et-al , 2016]** proposed ultra-weight encoding design is The Author has suggested a Feistel cypher, "ANU," which has the highest data complexity and leads to the highest number of S-boxes in some rounds. ANU cypher requiring a 128 bit key length of 934 GE and a very smaller power consumption of 22 mW is substantially less than any other device. ANU cypher also avoids advanced attacks, and prevents simple attacks. **[ZahidMahmood, et-al , 2016]** proposed The Authentication Method was proposed based on the two-level IOT session. A stable and lightweight encryption is provided by the proposed mechanism between end users. This is an efficient approach to reduce energy and power usage. TSK also achieves a 50 % to 100% reduction in electricity. In order to achieve this, we need a highly protected technique for low cost and low power consumption, which has been suggested by the author, which gave almost desirable results. **[D.Jamuna Rani, et al, 2016]** has reviewed various published papers and compared the encryption systems to provide an overview of it. Today's Internet and internet age is becoming more and more popular day by day. It functions as a human-internet interface, which has largely given us the reliance on the Internet. Consequently, the protection and integrity of the network have become very critical. The author analyzed the latest IOT-based computer cryptography schemes. **[SudhirSatpathy, et-al , 2016]** has suggested a very low energy protection system for IOT-based applications. The protection of content and user privacy for IOT-based areas or battery restriction devices is important in lightweight energy efficient safety systems. The energy efficiency is 289 Gbit / W, 190 fJ / bit and 3pJ / bit for AES-128 PUF and µRNG with ultra-low violation circuit techniques, Arithmetic optimization and Micro-architecture Enhancement. **[SainandanBayyaVenkata, et-al, 2016]** the idea for the light-weight transport method of safe data transmission for the internet of things. the author's objective is to evaluate the already existing lightweight cryptographic algorithms and to demonstrate how the data are treated in different IOT layers, and the author describes a protected IOT Lightweight Transport Method. There is talk of the use of the proposed algorithm for parameter such as utilization of the CPU, data fragmentation and latency. **[Amber Sultan, et-al , 2018]** proposed that A physical layer data encryption scheme has been needs to enhance data protection when transmitting the data. In this paper author, digital chaos has been used that provides a huge key space for data protection. The use of radial constellation rotations is based on a new physical layer encryption method and is being experimented with multiplexing orthogonal division frequency. A digital chaotic sequence with less complexity is created for data encryption. **[Xuelin Yang, et-al, 2018]** suggested a multifold encoding method and tested the multiplexing of passive optical network (OFDM-PON) orthogonal frequency splitting method. The suggested scheme screws up and distributes the QAM symbols on the complex plane independently. In order to increase the security level of the proposed system the author generates the constellation shifting parameters, which are carried out by 3-dimensional hyper chaos (digital) and also provides a main space of approx. 10 ^ 162. The author demonstrated the scheme with 9,4Gb / s, 16QAM optical OFDM signal encrypted data transmission, and the testing of standard 20 km signal mode fiber was demonstrated.

3. PROBLEM DEFINITION AND PROPOSED WORK

3.1 Description of Problem

A variety of digital strategies have been proposed as regards the growth of Internet applications, to ensure that multimedia information cannot be accessed or modified by unauthorized users. The technique of watermarking, however, is most widely used. The method of spatial domain and the method of frequency domain are the two wider categorizations of several different watermarking techniques. For the incorporation of watermarks via the spatial domain technique, the lower order bits of the image are enhanced. The main advantages gained by this approach are to reduce the complexity and provide minimal computational values. The robustness of this strategy is therefore very strong in the face of real security attacks. The techniques using such invertible transformations, such as the Discrete Cosine Transformation (DCT) are also known as the transformation techniques of the frequency domain. The picture is housed using DFT and DWT techniques. Discrete Fourier transformations. These transforms can easily adjust the coefficient value according to the watermark to integrate the watermark in the picture. In addition, the opposite transform is used on the original image. These methods are very complex. The computer power needed is high here, too. These approaches offer further reverses for security attacks. Another method used in this step is the GLCM (Gray Level Co Incidence Matrix) technique. The methodology also involves the implementation of watermarking based on spatial analysis like local binary pattern.

3.2 Research Goals

In this study, the main goals are as follows:

- The properties of current watermarking algorithms are analyzed, i.e. DWT
- To suggest improved watermarking technology for the generation of a blind watermark.
- Comparative analysis will be based on the GLCM algorithm and proposed methodology involving improved local binary pattern based watermarking system.
- Implementing and contrasting the proposed technique with current technique, i.e. DWT as regards PSNR, BER and MSE.
- Proposed work is targeted for image enhancement of aerial images based on improved wavelet transform.

3.3 Research Methodology

An effective technology known as watermarking is applied to provide protection to the image data. The two wider classifications of the different watermarking techniques proposed over time are blind and semi-blind watermarking techniques. The OS-ELM approach is used to incorporate semi-blind watermarked images into the base paper and is essentially a master learning approach. The DWT 4-level technique is applied to extract features from the original and watermark images. The training image that is analyzed by DWT is presented as input to incorporate the semi-blind watermarks in order to create the final training sets. DWT algorithm analyses the textual characteristics of images. It replaces DWT with a less complex GLCM algorithm and can easily generate blind watermarks by simply generating the training sets.

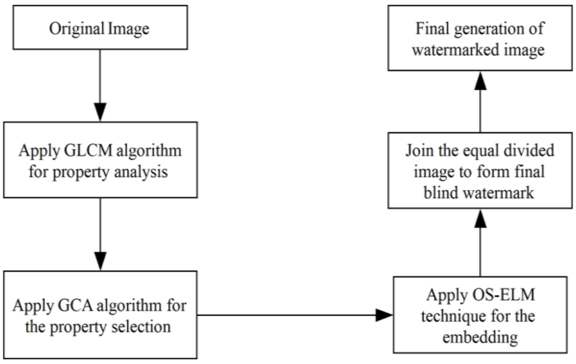

Figure 3.1: Proposed Flowchart of Embedding

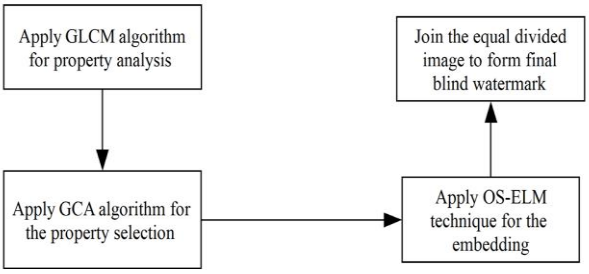

Figure 3.2: Draft Extraction Flowchart

3.3.1 Algorithm of GLCM

The GLCM algorithm takes the next steps:

- An input will be presented as an image and the image will be processed as pixels. The matrix counts the total pixel count of an image.
- To store the counted pixels, a second matrix such as matrix P is used.
- Applied histogram technique monitors the similarity between pixels that are stored in the input matrix.
- To measure the matrix comparison, the following formula is used[21]

$$g = \exp\left[\frac{mean(I) - \min(I)}{\max(I) - mean(I)}\right] \quad (3.1)$$

- The standardization matrix is generated from matrix g as:

$$g = \begin{bmatrix} 0.8\ if\ g < 0.8 \\ 1.2 if g > 1.2 \\ g\ otherwise \end{bmatrix} \quad (3.2)$$

3.3.2 Implementing Principle Component Analysis Algorithm

The PCA algorithm is picked from the pixels extracted. The PCA algorithm as input and similitude takes the picture and discrepancies are studied between different pixels. By measuring the similarity between pixels, PCA algorithms reduce the dimensions of the input data. The transmission distance is used to evaluate similitudes between different pixels. In order to equate pixels with each other, statistic methods and mathematical formulas are used. PCA is commonly used in the fields of recognition and image compression. By the use of the principal component analysis (PCA) method, data is converted from high to low dimensions. For the measurement of low dimensions, the Eigen vector formula is used.

Some steps are accompanied by the PCA mechanism:

- The mean value is determined for the matrix known as A.
- Matrix values deduct the average value and produce a new matrix B.
- To calculate the matrix covariance given as C = AAT the self-formula is used.
- To measure the Eigen value of C, the Eigen formula shall be added.
- For generating covariance matrix from input values the following equation is used:

$$V_N S - \bar{S} = b_1 u_1 + b_2 u_2 + \cdots .. + b_n u_n \tag{3.3}$$

- The highest Eigen values are contained inside the low dimensions:

$$\mathrm{S} - \bar{S} = \sum_{l=0}^{1} b_1 u_1 \,;\, 1 < N \tag{3.4}$$

3.4 Image Watermarking Using Local Binary Pattern

In texture analysis, local contrast [22, 23] is used for identifying the local binary pattern (LBP) operator. Graphics and pictures were analysed successfully [24, 25]. In a local circular district, the definition of the LBP operator uses the centre pixel as the threshold. In a certain radius R, the circularly symmetrical P neighbours are labelled as 1 independently if the value is greater than the centre or 0 if the significance of the middle contrast is smaller. (P= $(2R+1)^2-1$) The middle-pixel LBP code should be observed by weight of the pixels and the result summary. This is derived from a threshold multiplication value, i.e. 1 or 0. The value of the 3×3 LBP window is the mid-pixel R = 1 and P = 8). The binomial weight and neighbouring thresholds. This is a summary of the LBP number. The LBP produces between 0 and 255 numbers. A texture Image range of 256 grey levels is the maximum sum of LBP, which is also used for extracting, classifying and recognising images. Parameters P and R, respectively, that govern resolution quantification, LBP numbers; the contrast in the neighbourhood is marked by LBP.

$$LBP_P = \sum_{p=0}^{P-1} S\left(g_p - g_c\right) \times 2^p \tag{3.5}$$

Where gc refers to the centre pixel grey level c, gp indicates the neighbouring pixel grey level p, and S(x) refers to the symbols feature as specified:

$$S(x) = \begin{cases} 1, \text{ if } x \geq 0 \\ 0, \text{ otherwise} \end{cases} \tag{3.6}$$

The LBP operators can be found at information and application at [25]. Zhang and Jin [27] improved the LBP operator by considering variations in grey level. Concentrate on the most important bits of the visual texture Photos and any details. You did it. Two-phase gas/liquid flow patterns analyze and understand effectively. Guoet al. implemented a new modelling of the local binary construct.[28] Operator for texture classification with two complementary components: The size and the signals. Two-phase gas/liquid flux patterns analyse and recognize effectively. Guoet al. implemented a further modelling of the local binary model. [28] Operator for texture classification with two complementary components:
The magnitudes and the signals.

$$\begin{aligned} g_p &= \{g_i \mid i = 0, \cdots, c, \cdots, P-1\} \\ m_p &= \{m_i | m_i = | g_i - g_c |, i = 0, \cdots, P-1\} \\ s_p &= \{s_i \mid s_i = \text{sign}\ (g_i - g_c), i = 0, \cdots, P-1\}. \end{aligned} \tag{3.7}$$

Please notice that Eq.3.5 uses the equivalent sign function (3.7). Thus, the area is divided into three parts[28]: The gp is an R-radius pixel P vector, mp is a magnitude vector formed from the difference of the pixels to the centre pixel gc, and Sp the difference of the symbol. The figure illustrates the three sections in a local area (P = 8, R = 1). We describe Boolean functions f(sp) which are to be used on the binary sign vector section sp. To integrate watermarks. To illustrate the following two types of Boolean functions are selected.

We insert the watermarks by changing the f(sp) in a regional location. The value of f(sp) is modified by changing the bits sp. These changes are reflected in changes of pixels in the local space region. The different algorithms complement different Boolean functions. For example (P, R) We choose a minimum size pixel in the neighbourhood while using the boolean function f(sp). The most influenced picture block is adjusting the quality of the original for the watermark embedding. That is, we maintain the value(sp) consistent with the corresponding Watermark bit.

$$\begin{aligned} f_{\oplus}(s_p) &= s_0 \oplus S_1 \oplus \cdots \oplus_{P-1} \\ f(s_p) &= \text{Bool}\ (1(s_p) - 0(s_p) > N) \end{aligned} \tag{3.9}$$

We insert the watermarks by changing the f(sp) in a regional location. The value of f(sp) is modified by changing the bits sp. These changes are reflected in changes of pixels in the local space region. The different algorithms complement different Boolean functions. For example (P, R) We choose a minimum size pixel in the neighbourhood while using the boolean function f(sp). The most influenced picture block is adjusting the quality of the original for the watermark embedding. That is, we maintain the value(sp) consistent with the corresponding Watermark bit.

$$\textbf{If}\ (w = 1 \text{ and } f_{\oplus}(s_p) = 0) \text{ or } (w = 0 \text{ and } f_{\oplus}(s_p) = 1) \tag{3.10}$$

$$\begin{aligned} &\text{select } m_i = min(m_p) \\ \text{Then }\ &\text{if } s_i = 1 \text{ then } g_i = (g_i - m_i) \times (1 - \beta); \\ &\text{else } g_i = (g_i + m_i) \times (1 + \beta)\} \end{aligned}$$

It should be pointed out that the min() function is the most simple. If multiple minimum values are available, we select one to choose the pixel to adjust.

$$\text{if } f_{\oplus}(s_p) = 1 \text{ then } w = 1 \text{ else } w = 0 \tag{3.11}$$

The block is changed if all pixels of a block are "0" or "1." The centre pixel was previously based on the respective watermarking bit. Incorporation of the code into the block. The watermark extraction technique of the proposed process. The condition is obvious. In extracting w from a watermarked image, the value of f(sp) is evaluated.

3.5 Automatic Wavelet Based Nonlinear Image Enhancement Technique for Aerial Imagery

Three stages consist of the proposed enhancement algorithm: first and third phases are used for space and second for a discrete wavelet. Our inspiration for a histogram adaptation to minimise the lighting effect is based on certain assumptions about the creation of images and human perception. As the product [8],[26] can be approximated the incident of a sensor S(x,y) on an imaging device.

$$S(x,y) = L(x,y)R(x,y), \tag{3.12}$$

When the reflection is R(x, y), and L(x, y) at any point, the light is (x, y). Equation 3.12 can be broken down in light algorithms if the sensors or filters used in artificial visual systems are of the same nonlinear property, i.e., log-reactions to the physical intensities of their photoreceptor as a sum of two components by using the transformation

$$I(x,y) = \log(S(x,y)) \tag{3.13}$$

$$I(x,y) = \log(L(x,y)) + \log(R(x,y)), (2) \tag{3.14}$$

where I(x,y) is the intensity of the image at pixel location (x,y).Intrinsically, in various spectral bands this change is not the same. The greyscale presumption that the average surface reflection of each scene in every wavelength band is identical; another statement of lightness is the gray colour presumption [8].

This hypothesis suggests from an image processing position that pixels with almost identical average grey levels in each spectra band should be presented in images of natural scenes. Combining equation with the assumption of the grey universe, we change histogram accordingly:

- From the beginning of the lower tail of the histogram, the sum of shifts corresponding to the illumination is calculated to cut the preset number of pixels (usually 0.5 percent) of the pixels.
- Each pixel value of the change is removed
- For each colour channel, this step is repeated separately The WDRC luminance channel is equipped with dynamic range compression and the local contrast improvement. The strength of imagery I(x,y) with the following equation is available for colour images

$$I(x, y) = \max[Ii\ (x, y)],\ i\hat{I}\ \{R,G,B\}. \tag{3.15}$$

The improvement of the local comparison, using a centre-surface method, is followed. A filtering of normalised approximation coefficients with a Gaussian kernel obtains the surrounding intensity information for any coefficient input. The coefficients of detail are updated by the ratio of improved coefficients to the initial approximations. In our previous work, a linear colour restore is used for the final colour image. A non-linear approach is used for WDRC with colour restoration. This element has a canonical value and increases colour saturation to make the colour rendition more attractive. Since the coefficients are normalised during the enhancement, the reverse transformation of improved coefficients, along with the enhanced colour image provided by the span, is achieved almost only in the lower half of the entire histogram range. The domain output is extended to reflect the entire dynamic range for the final show. Cutting a histogram from the top of each channel histograms results the best way to translate the output to a domain.

4. IMAGE COMPRESSION USING TRICONOMETRIC TRANSFORMS

The conversion results to relate there is a reduction in the importance of a certain pixel picture block to use the information to minimize the amount of transforming coefficients to a minimum. For a given application, it mainly depends on two aspects to choose a transformation factor.

- One variable source of computing
- The degree to which the end user may absorb the reconstructed error

As a general rule, transform as "T (u) and reverse is mathematically interpreted for a NxN image f(x , y), the forward discrete transform

$$T(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)g(x,y,u,v) \tag{4.1}$$

$$F(u,v) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} T(x,y)h(x,y,u,v) \tag{4.2}$$

Where g(x, y, u, v) is the kernel of the forward transformation and h(x, y, u , v).

DCT is considered as "almost-optimal transformation" in the late 1990's as the default transformation of the image in the visual system.[16]

Four excellent highlights in an application for image processing are:

- **De-correlation-** As the adjustment is modified, the excess in the picture is de-correlated to establish non-important transformational variables, resulting in an expulsion of spatial redundancy between the pixels.
- **Energy Compact:** sample information is changed to multiple coefficients; the capacity to adjust the compacted set of vitality is conceivable. The coefficients that have a maximum amount of data have wide amplitude. Superfluous / redundant information that is of a low abundance.
- **Divisible property:** the 2-D DCT's meaning is a detachable property, which allows for 2-D transformation into two 1-D transformations backwards.
- **The symmetry property:** the row operations can be seen as the same as the column operations in the 2-D DCT. Consequently, the symmetric characteristics of the DCT.The transformation can be expressed as its separable and symmetrical properties

$$T = A\ f\ (A) \tag{4.3}$$

Where A is a NxN symmetrical matrix with elements Specification:

$$a(i,j) = a(j)\sum_{j=0}^{N-1}\cos\left[\frac{\pi(2j+1)i}{2N}\right] \tag{4.4}$$

And f is a picture of NxN.

Orthogonality Property: The reverse transformation can be seen as an extension of the equation:

$$f = A^{-1}\ TA^{-1} \tag{4.5}$$

The trait of orthogonality means that the inversely transformed Matrix A is equal to its transposition and thus reduces the multifaceted essence of pre calculation.

4.1 Aerial Image Enhancement

Aerial imaging can show soil and crop conditions a great deal. The view of an aerial picture from the "Bird's Eye" helps farmers to observe problems with yield combined with field awareness. Our imaging technology improves proactively and identifies a problem region, thus minimising loss of yield and restricting exposures in other field areas. Hemisphere GPS Imagery uses infrasound technology to help you see a large scale of these daily problems. Digital sensors are highly sensitive to subtle plant health variations and growth rates. Anything, such as curling, wilting and defoliation that changes its aspect has an effect on the image. Software enhancement emphasises these differences in the canopy and suggests problems with disease, water, weed or fertility.

The measured aerial image removes printing and etching processing effects on the wafer. Aerial image emulation for CDU calculation has been successfully used In order to assess the imperfection and repair success, historically; aerial image metrology systems are used.

Figure 4.4: Areal Image of the Test the Building

Digital aerial photography, however, should remain in the public domain and be archived for science, legal and historical purposes in future.

4.2 Uses of Aerial Imagery

An aerial photograph is used in the areas of geography, land use planning, archaeology, film production, the environmental studies, surveillance, trade advertising, communications and artistic projects (especially in photogrammetric surveys often based on the topographical maps). Aerial images are used for property analysis in many phase I environmental screenings in the USA. GIS programme also processes aerial images Advances in radio-controlled models made aerial photography possible for models. This supports real-estate ads, which includes photographic industrial and residential properties. Low-flying aircraft over inhabited areas are prohibited in full-size, manned aircraft. [3] Small-scale models have expanded access to photographs to those areas previously limited. The full-size aircraft cannot replace mini-vehicles, as they are capable of longer flights, higher altitudes and greater loads of equipment. However, they are useful when a full-scale aircraft is unsafe to fly. E.g. inspection of transformers at the top of power transmission lines and slow flight over agricultural fields, which can all be performed by a large radio controlled helicopter. A large model helicopter with a 26 cc gasoline engine can carry a payload of approximately seven kilogram's, and is ideal for use on such a design.

4.3 Implementation and Result Analysis

The results of the proposed and actual methods are shown in Table 4.1. These findings are calculated based on the coefficient values PSNR, MSE, BER and BER.

Table 4.1 Comparison of Results (Sample Image)

Type of Attack/Image	Value of Parameters	Existing Performance Values	**Proposed Results**
Watermarking Image	Peak Signal to Noise Ratio	14.1018	18.10
	Mean Square Error	0.04	0.020
	Correlation Coefficient	0.01	0.01
	Entropy	7.97	7.99
Contrast Attack	Peak Signal to Noise Ratio	21.02	27.01
	Mean Square Error	0.022	0.015
	Correlation Coefficient	0.011	0.01
	Entropy	7.90	7.98
Sharpened Attack	Peak Signal to Noise Ratio	14.1018	18.10
	Mean Square Error	0.02	0.018
	Correlation Coefficient	0.01	0.01
	Entropy	7.93	7.98
Noise Attack	Peak Signal to Noise Ratio	14.1018	18.10
	Mean Square Error	0.027	0.025
	Correlation Coefficient	0.01	0.01
	Entropy	7.91	7.99
Decryption and Encryption	PSNR	13.1018	17.10
	Mean Square Error	0.023	0.023
	Correlation Coefficient	0.01	0.01
	Entropy	7.92	7.96
Execution Time		0.014 Seconds	0.011 Seconds

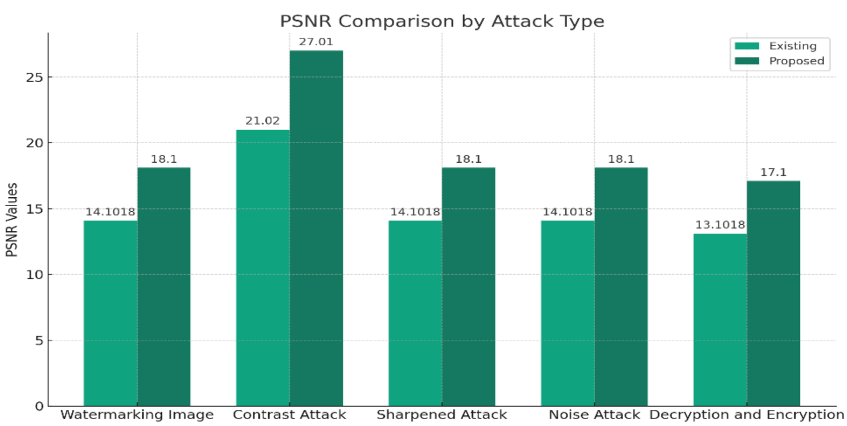

Figure 4.1: PSNR Analysis Based on Type of Attack

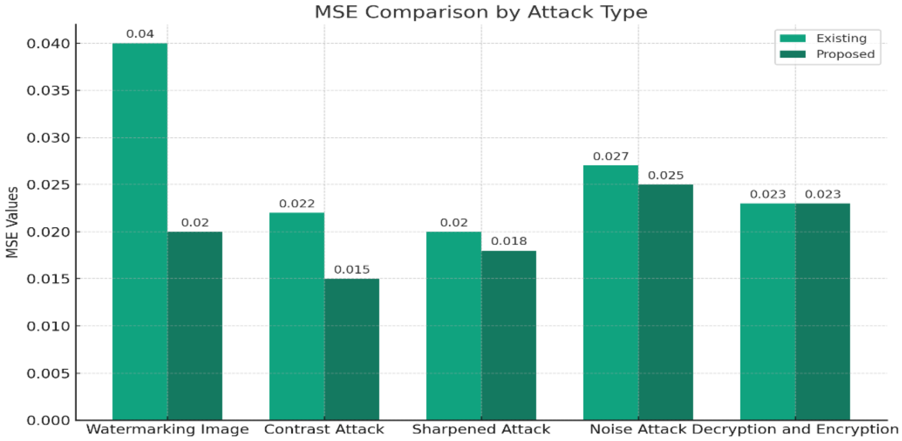

Figure 4.2: MSE Analysis Based on Type of Attack

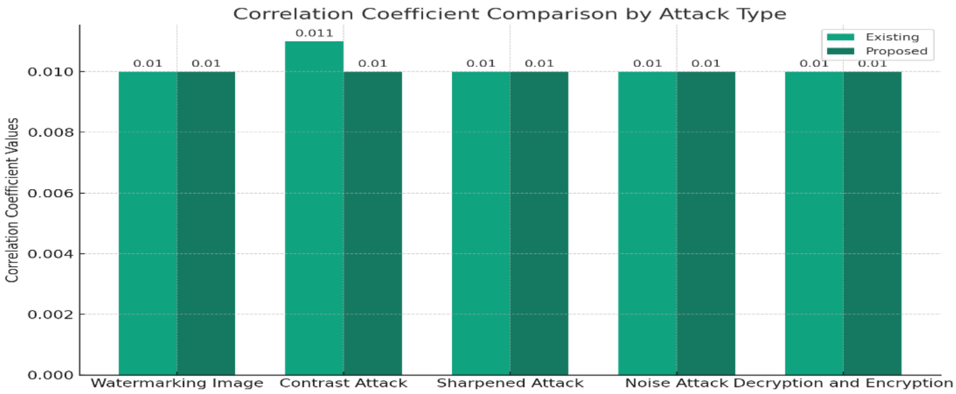

Figure 4.3: Correlation Analysis Based on Type of Attack

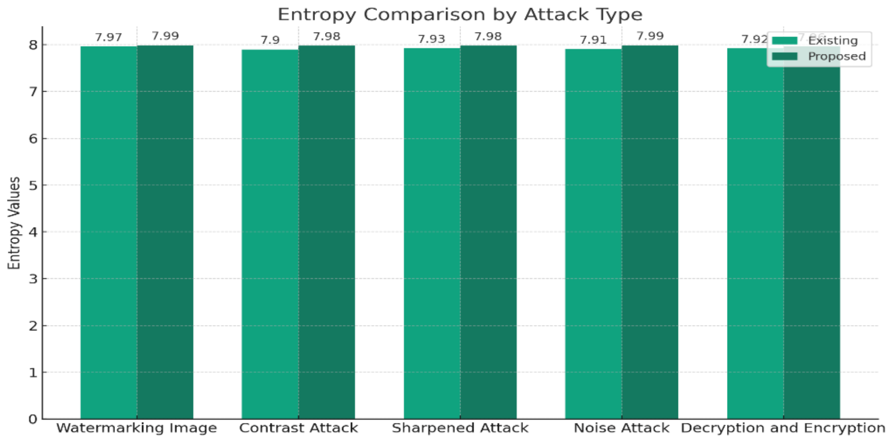

Figure 4.4: Entropy Analysis Based on Type of Attack

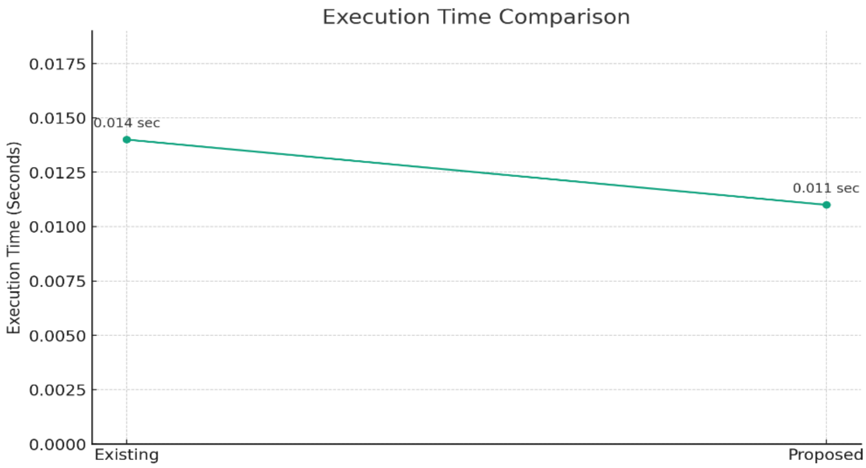

Figure 4.5: Comparative Analysis of Execution Time

The bar chart above visually compares the Peak Signal to Noise Ratio (PSNR) values between the existing system and the proposed system across various attack types. Each pair of bars represents a different type of attack, clearly showing the contrast in PSNR values. The bar chart also illustrates the comparison of Mean Square Error (MSE) values between the existing system and the proposed system for each type of attack. As with the previous chart, each pair of bars represents a different attack type, highlighting the differences in MSE values. Figure 4.16 compares the Correlation Coefficient values between the existing and proposed systems across different types of attacks. Each pair of bars corresponds to a specific attack type, showing the comparison in Correlation Coefficient values. The line graph above compares the execution time between the existing and proposed systems. The points on the graph represent the execution time in seconds for each system, providing a clear visual representation of the performance improvement in terms of speed. These charts collectively illustrate the improvements the proposed system offers over the existing system in various parameters and under different types of attacks

4.4 Image Enhancement for Aerial Images

We proposed a compression algorithm based on wavelets to enhance the visual quality of digital images captured in highly dynamic, uniformly lighting scenes. A very good candidate for aerial imaging applications as image interpreting in security and defense tasks is the fast image improvement algorithm, which provides dynamic range compression that preserves the local contrast and tonal rendition. This algorithm can also be used for aviation safety video streaming. The latest version of the proposed algorithm is presented in this project which enhances aerial images to better provide enhanced images than direct human observation. The results achieved by the application of the algorithm to many aerial images are highly stable and highly image quality.

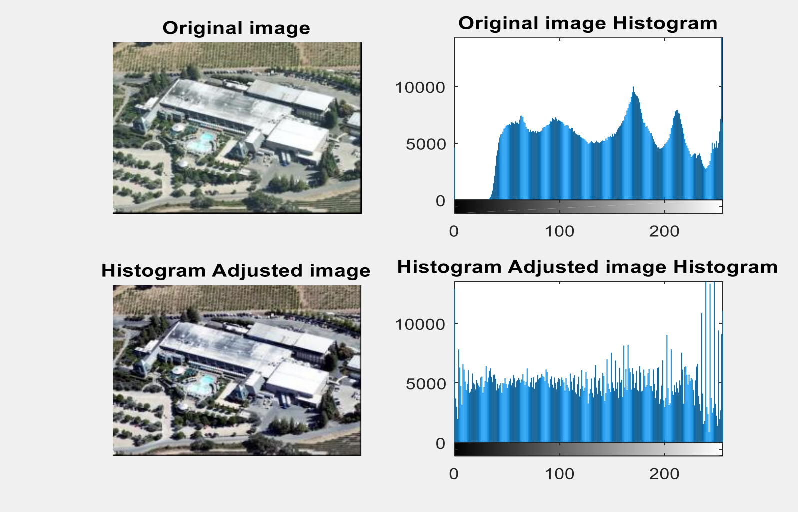

Figure 4.6: Histogram Adjusted Images

Figure 4.7: Image after WDRC Approximation Process

Figure 4.8: Reconstructed Spatial Domain Images

Figure 4.9: Output of Enhanced Image Case-1

The "Original image" is an aerial photo of an architectural complex with a distinctive building, perhaps of historical or institutional significance, given the style and the prominence of a dome-like structure. The lighting is natural, with contrasts coming from sunlight and shadows which gives the photo a range of bright and dark areas.

The "Histogram Adjusted image" is a version of the original where the histogram has likely been manipulated to alter the image's brightness and contrast. This is usually done to enhance the visual appeal or detail of the image. The adjusted image looks brighter and more vibrant, suggesting that the histogram has been stretched to utilize the full range of possible pixel values, from pure black to pure white. This process can increase the overall dynamic range of the image, making it look more lively and detailed.

The histograms to the right of each image graphically represent the distribution of pixel values within the images. In the context of images, a histogram plots the number of pixels for each tonal value.

1. **Original image Histogram**: This histogram is skewed towards the left, suggesting that the image has a lot of dark pixels. The high peak in the lower tonal values indicates that the shadows and darker areas dominate the image. There is a lack of pixels in the higher tonal values, indicating fewer bright or white areas.
2. **Histogram Adjusted image Histogram**: This histogram is more spread out across the tonal range, indicating that the adjustment has expanded the distribution of pixel values. The presence of higher peaks throughout the histogram suggests that there are more pixels in both the dark and bright ranges, which correlates with the visual appearance of the adjusted image being more detailed and having greater contrast. The spread of the histogram from the left edge to the right edge indicates the use of the full tonal range, which can contribute to an image that more closely resembles how the human eye perceives a scene.

5. CONCLUSION AND FUTURE WORK

The research developed a wavelet-based dynamic range compression system aimed at enhancing the visual quality of digital photographs captured in high dynamic range scenarios, particularly in settings with non-uniform lighting. This technique, especially suitable for aerial photography applications in defense and security, is characterized by its ability to preserve local contrast and tonal rendition while effectively managing dynamic range. The method shows great promise for video streaming in the aviation industry.

Key advancements introduced in this study include the latest iteration of the proposed algorithm, which significantly enhances the quality of aerial photographs. The enhanced images achieved through this algorithm surpass direct human observation in terms of image quality and robustness, demonstrating its effectiveness across various aerial images.

Aerial Image Enhancement encompasses several promising directions. These advancements are not limited to agriculture but extend to various fields including environmental monitoring, urban planning, disaster management, and defense. The integration of emerging technologies and methodologies will further revolutionize aerial imaging and its applications.

In conclusion, the future scope of aerial image enhancement is vast and multidimensional. It offers exciting possibilities for advancements in technology and its applications across various sectors, driving innovation and contributing significantly to addressing some of the major challenges faced by society today.

REFERENCES

[1] Wen Zhang, Jie Men, Conglong Ma, “Research progress of applying digital watermarking technology for printing,” 2018, IEEE
[2] David-Octavio Muñoz-Ramirez , VolodymyrPonomaryo , Rogelio Reyes-Reyes , VolodymyrKyrychenko , OleksandrPechenin, Alexander Totsky , “A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images,” 2018, IEEE
[3] AnirbanPatra*, ArijitSaha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, “A New Approach to Invisible Water Marking of Color Images using Alpha Blending,” 2018, IEEE
[4] Irshad Ahmad Ansari, Chang WookAhn and Millie Pant, “On the Security of “Block-based SVD image watermarking in spatial and transform domains”, 2018, IEEE
[5] Alexander S. Komarov, “Adaptive Probability Thresholding in Automated Ice and Open Water Detection From RADARSAT-2 Images,” 2018, IEEE
[6] Thien Huynh-The, Sungyoung Lee, “Color Image Watermarking Using Selective MSB-LSB Embedding And 2D Otsu Thresholding,” 2017, IEEE
[7] Shan Liu ,Keming Yue ,Hua Yang ,Lu Liu ,Xiaorong Duan ,Ting Gu, “Digital Watermarking Technology and Its Application in Information Security,” 2017, IEEE
[8] Oleg Evsutin, Roman Meshcheryakov,Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, “An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata,” 2017, IEEE
[9] Ritu Gill and Rishi Soni, “Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images,” 2017, IEEE.
[10] Mohammad ShahabGoli and AlirezaNaghsh, “Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku,” 2017, IEEE
[11] Anshul Kanchan Khanna, Nihar Ranjan Roy and Dr. Bhupendra Verma, “Digital Image Watermarking and its optimization using Genetic Algorithm,” 2016, IEEE
[12]Maria Almulhim, Noor Zaman, “Proposing secure and the lightweight authentication scheme for IOT based E health applications” *International* conference on advance communication technology; 2018.
[13] Muhammad NaveedAman, KeeChaing Chua, “A light weight mutual authentication protocol for IOT system, 2017.
[14] Mehdi Baahrami, Dong Li, MukeshSinghal, “Efficient parallel implementation of light weight data privacy method for cloud users; seventh international workshop on data intensive computing in clouds, 2016.

[15] Gaurav Bansod, AbhijitPatil, “An Ultra light weight design for security in pervasive computing” IEEE second international conference on big data security cloud, 2016.
[16] ZahidMahmood, HuanshengNing, “Light weight two level session key management for end user authentication in internet of things” IEEE international conference on IOT, 2016.
[17] Ayaz Hassan moon, Ummer Iqbal, “Light weight authentication framework for WSN” International conference on Electrical, Electronics and Optimization techniques, 2016
[18] D Jamuna Rani, “Light weight cryptographic algorithm for medical internet of things”, Online international conference on Green Engineering and Technology, 2016.
[19] SudhirSatpathy, Sanu Mathew, “Ultra low energy security circuits for IOT applications”, IEEE 34th international conference on computer design, 2016.
[20] SainandanBayyaVankata, PrabhkarYellai, “ A new light weight transport method for secured transmission of data for IOT”, international journal of electrical, electronic engineering, 2016.
[21] Amber Sultan, Xuelin Yang, “Physical layer data encryption using chaotic constellation rotation in OFDM-PON” Proceedings of 15th international Bhurban conference on applied science and technology Islamabad Pakistan, 2018.
[22] Xuelin Yang, ZanweiShen, “Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen plaintext attacks”, in ICTON 2016.
[22] Xuelin Yang, ZanweiShen, “Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen plaintext attacks”, in ICTON 2016.
[23] Han Chen, Xuelin Yang, “Physical layer OFDM data encryption using chaotic ZCMT precoding matrix”, IEEE, ICTON 2017.
[24] GaoBaojian, LuoYongling, HouAiqin, “New physical layer encryption algorithm based on DFT-S-OFDM system” International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China, 2013.
[25]Meihua Bi, Xiaosong Fu, “A key space enhanced Chaotic encryption scheme for physical layer security in OFDM-PON”, IEEE photonics Journel”, 2017.
[26] Dana Halabi, Salam Hamdan, “Enhance the security in smart home applications based on IOT-CoAP protocol.
[27] Jongsoek Choi, Yongtae Shin, “study on information security sharing system among the industrial IOT service and product provider, IEEE ICOIN, 2018.
[28] Jin HyeongJeon, Ki-Hyung Kim, “Block chain based data security enhanced IOT server platform, IEEE ICOIN, 2018.
[29] MuhammetZekeriyaGunduz, Resul Das, “A comparision of cyber security oriented test beds for IOT based smart grids, IEEE 2016.
[30] Himanshu Gupta, GarimaVarshney, “A security Framework for IOT devices against wireless threats, second international conference on telecommunication and networks, 2017.
[31] Thomas Maurin, Lurent, George Caraiman, “IOT security assessment through the interfaces P-SCAN test bench platform, 2018 EDAA.
[32] Sanjay Kumar, Ambar Dutta, “A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks,” 2016, IEEE
[33] N. SenthilKumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique,” 2016, IEEE
[34] Junqing Zhang, et al "The encryption scheme is being at the orthogonal frequency-division multiplexing networks (OFDM)physical level", Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2016
[35]] Mukesh Chandra Negi, et-al , "a fast amplification of the Internet, which gave rise to a vision of various sectors going forward in those areas of logical competence to the customers, control, instrumentation, and other systems"IEEE,2017

[36] C. Lin, D. He, X. Huang, K.-K. Raymond Choo, and A. V. Vasilakos, “BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2018.

[37] J. Srinivas, A. K. Das, and A. V. Vasilakos, “Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment,” IEEE Transactions on Industrial Informatics, vol. 16, pp. 7081–7093, 2019. Advances in Multimedia 11

[38] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, “Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems,” Future Generation Computer Systems, vol. 108, pp. 1267–1286, 2020.

[39] M. Wazid, A. K. Das, K. Vivekananda Bhat, and A. V. Vasilakos, “LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment,” Journal of Network and Computer Applications, vol. 150, Article ID 102496, 2020.

[40] Mahbuba Begum, Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Advances in Multimedia, vol. 2020, Article ID 7912690, 12 pages, 2020. https://doi.org/10.1155/2020/7912690

[41] S. K.A. "A.. Raj, V. Sharma, and V. Kumar.“Simulation and Analysis of Hand Gesture Recognition for Indian Sign Language Using CNN”." *International Journal on Recent and Innovation Trends in Computing and Communication* 10, no. 4 (2022): 10-14.

[42] S.K.A. and Abha Jadaun. “Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT”, Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.

[43] Pratiksha Mishra S.K.A.. “Design & Performance Assessment of Energy Efficient Routing Protocol Using Improved LEACH”, International Journal of Wireless Network Security, 2021, Vol-7, Issue-1, PP: 17-33.

[44] S.K.A., Prakash Dangi and Pratiksha Mishra. Design and Comparison of LEACH and Improved Centralized LEACH in Wireless Sensor Network. *IJRITCC* 2021, *9*, 34-39.