IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FPGA BASED IMAGE FORGERY DETECTION SYSTEM USING VERILOG

Dr. N M Mahesh Gowda[1], Sinchana S[2], Lisha N S[3], Monisha K S[4], Suhas K S[5]

Associate Professor[1], Student[2], Student[3], Student[4], Student[5]

Department of ECE, PESCE, Mandya, India

I ABSTRACT

The trustworthiness of visual information in applications like surveillance, digital forensics, medical diagnostics, and security monitoring is seriously threatened by the substantial increase in digital picture modification brought about by the growing accessibility of sophisticated image editing software. As a result, preserving the integrity and validity of images now depends on the creation of effective and precise image forgery detection methods. In this paper, a Verilog Hardware Description Language (HDL)-based FPGA-based Image Forgery Detection System is proposed. By analysing image attributes and identifying anomalies brought about by forging operations, such as copy-move assaults and unauthorized modifications, the suggested architecture is intended to identify tampered regions in digital images. High-speed processing and real-time operation are made possible by the system's implementation on an FPGA platform, which takes use of hardware-level parallelism. The suggested hardware solution delivers better computational efficiency, lower processing delay, and lower power consumption while retaining efficient resource utilization when compared to traditional software-based approaches. Simulation and synthesis assessments validate the functionality and performance of the proposed architecture, demonstrating that it can detect updated image regions with appropriate accuracy and execution speed. The created system is well-suited for implementation in digital forensic investigations, picture authentication frameworks, surveillance infrastructures, and other security-sensitive contexts demanding quick and reliable image verification because of its scalability and dependability.

Keywords: FPGA Implementation, Digital Image Forensics, Verilog Hardware Description Language, Image Tampering Detection, Copy-Move Forgery, Real-Time Processing, Embedded Vision Systems.

II. INTRODUCTION

A. Background and Importance of Digital Images

As the main medium for gathering, storing, sending, and interpreting visual data, digital images have grown to be an essential part of contemporary communication and information systems. Images are widely used in many different fields, including surveillance systems, healthcare, forensic investigations, scientific research, military operations, journalism, and social networking platforms, thanks to the quick development of digital imaging devices, internet technologies, and multimedia applications. Decision-making and information sharing are now much more efficient due to the widespread use of digital images. Digital photographs are frequently considered trustworthy sources of information in both personal and professional contexts because of their capacity to offer comprehensive visual proof.

However, digital photos may now be altered with exceptional accuracy and few visible artifacts because to the growing availability of advanced image editing tools. The original image content can be changed

while retaining a realistic appearance using a variety of tampering techniques, including copy-move forgeries, image splicing, object insertion, and content removal. Because of this, it's getting harder to tell real photos from fake ones. Images that have been altered can spread false information, undermine the reliability of digital evidence, and seriously jeopardize security-sensitive applications.

As a result, maintaining the integrity and authenticity of digital images has become essential to modern digital systems. The performance requirements of real-time applications may not be met by traditional software-based methods for detecting forgeries, which can involve complex computations. As a result, there has been a lot of focus on integrating hardware-based solutions. FPGA technology offers an effective framework for putting high-speed image processing algorithms into practice in this situation. A possible method for obtaining dependable, real-time, and resource-efficient verification of digital image authenticity is the construction of an FPGA-based image forgery detection system utilizing Verilog.

B. Need for Hardware-Based Solutions

The shortcomings of traditional software-based processing methods have been brought to light by the increasing need for real-time image authentication and counterfeit detection. Software implementations frequently encounter increased computational latency and decreased processing efficiency as image resolutions and data volumes continue to rise. An efficient substitute is offered by hardware-based systems, which greatly enhance system performance by permitting the concurrent execution of image processing processes. Field-Programmable Gate Arrays (FPGAs) provide several advantages over other hardware platforms, including high processing speed, reconfigurability, low power consumption, and effective resource usage. Because of these features, FPGAs are a good choice for putting computationally demanding image forgery detection algorithms into practice. As a result, hardware-accelerated systems have become a viable method for real-time, scalable, and dependable image verification in security-sensitive applications.

C. FPGA and Verilog-Based Implementation

A versatile and effective hardware platform for executing image processing and digital forensic applications is offered by Field-Programmable Gate Arrays (FPGAs). Multiple processes can be carried out simultaneously thanks to its built-in parallel processing capability, which improves computational performance and lowers processing latency. The design and development of synthesizable hardware architectures that may be effectively implemented on FPGA devices is made easier by the Verilog Hardware Description Language (HDL). The suggested system uses Verilog to create picture forgery detection modules that can analyse image data and spot areas that have been tampered with. Real-time picture authentication applications are supported, processing speed is increased, and hardware resource consumption is optimized by the FPGA-based architecture.

D. Existing Approaches and Limitations

Several image forgery detection techniques have been proposed in the field of digital photo forensics to identify modified or tampered image content. In order to detect forgeries, the majority of current methods use on software-based algorithms that examine image attributes such texture patterns, colour distributions, edge characteristics, statistical discrepancies, and key-point descriptors. Under controlled circumstances, approaches such as feature-matching, picture splicing analysis, and copy-move detection have shown promising detection performance. However, these techniques frequently need significant processing time and computer resources, especially when dealing with huge datasets or high-resolution photos. Additionally, software-based systems may not be suitable for embedded and security-critical applications due to difficulties in attaining real-time operation, scalability, and power economy.

III. Problem Statement and Objectives

A. Problem Statement

The risk of digital picture alteration has greatly grown due to the widespread availability of sophisticated image editing tools, making it challenging to confirm the legitimacy of visual content. When analysing massive amounts of image data, current software-based forgery detection techniques frequently suffer from excessive computational complexity and poor real-time performance. An effective and dependable hardware-based solution that can quickly and accurately identify picture alteration is therefore required.

In order to provide real-time and resource-efficient forgery analysis, this work develops an FPGA-based image forgery detection system utilizing Verilog HDL.

B. Objectives

- To use Verilog on an FPGA platform to build and implement a hardware-efficient image forgery detection system.
- To provide an optimal image processing architecture that detects tampered areas by analysing structural and pixel-level irregularities.
- to produce real-time performance with improved hardware resource efficiency and detection accuracy.

IV. LITERATURE SURVEY

[1] A Survey on Passive Digital Video Forgery Detection Techniques (2023) Jegaveerapandian et al. reviewed passive video forgery detection methods, including spatial, temporal, and spatio-temporal approaches. The survey discusses datasets and existing challenges. However, it mainly focuses on software-based techniques, provides limited coverage of HEVC/H.265 videos, and lacks discussion on FPGA implementation and resource optimization.

[2] Image Forgery Detection: A Survey of Recent Deep-Learning Approaches (2023) Zanardelli et al. presented a comprehensive review of deep learning-based image forgery detection methods. The study highlights state-of-the-art detection accuracy but notes that these methods require high computational resources and are difficult to implement on FPGA platforms. Hardware feasibility and processing speed are not addressed.

[3] Image Forgery Detection: A Survey (2009) Hany Farid provided a foundational survey of image forgery detection techniques, including watermarking and passive forensic methods. Although it offers valuable theoretical insights, it does not cover modern deep learning approaches, hardware implementations, or large-scale evaluations.

[4] Image Forgery Detection Using Deep Learning Techniques (2023) Maneesha Nasreen T et al. reviewed recent deep learning-based forgery detection methods. The survey demonstrates improved detection accuracy but highlights limitations such as high computational complexity, poor suitability for FPGA implementation, and limited discussion on real-time processing.

[5] Hierarchical Categorization and Review of Recent Techniques on Image Forgery Detection (2021) Violin and Sucharitha categorized and compared recent image forgery detection techniques based on datasets, performance, and implementation approaches. While useful for understanding algorithmic trade-offs, the study provides limited information on real-time processing and hardware implementation.

[6] A Comprehensive Survey on Passive Techniques for Digital Image Forgery Detection (2024) This survey reviews passive image forgery detection methods, including copy-move, splicing, and retouching detection techniques. It covers both classical and feature-based approaches suitable for hardware adaptation. However, FPGA implementation, resource utilization, and real-time constraints are not discussed.

[7] Image Forgery Detection Using SVM Classifier (2015) Reshma P.D. and Arunvinodh C. proposed a forgery detection approach using illuminating colour features and an SVM classifier. The method improves detection accuracy through machine learning-based classification with minimal human intervention. However, hardware implementation aspects are not considered.

[8] Detection of Copy-Move Forgery in Digital Image Using Locality Preserving Projections (2015) Guangcheng Cao et al. proposed a copy-move forgery detection technique based on Locality Preserving Projection (LPP). The method utilizes image sub-block features to identify duplicated regions effectively. However, its performance under complex image transformations and hardware implementation feasibility remains limited.

V. EXISTING SYSTEM

A. Overview of Existing Forgery Detection Methods

To detect altered digital photos and guarantee content validity, a variety of image forgery detection techniques have been developed. These techniques generally rely on feature extraction, statistical analysis, texture investigation, key-point matching, and deep learning models to detect tampered regions. Copy-move forgery detection, image splicing detection, and source authentication techniques are common methods. Many of these techniques have drawbacks in real-time processing systems and demand substantial computer resources, despite the fact that they have shown adequate detection performance.

B. Working of Existing Systems

The majority of current image forgery detection systems work by analyzing digital photos to find discrepancies that were added during alteration. Image preparation, feature extraction, feature matching, and forgery localization are typically included in the procedure. To identify suspicious areas, a variety of algorithms look at features such texture patterns, colour distributions, edge information, and statistical qualities. To increase detection accuracy, advanced systems may also use deep learning or machine learning techniques. Although these algorithms are capable of accurately detecting many forms of image manipulation, their effectiveness frequently depends on processing power and image complexity.

C. Advantages of Existing Systems

Current picture forgery detection methods offer reasonable detection accuracy and efficient identification of modified image regions. These techniques can identify several types of image manipulation, such as splicing and copy-move attacks. Numerous methods can be modified to fit various image formats and application areas. Additionally, the dependability of digital picture authentication has been greatly improved by developments in machine learning and feature-based methods.

D. Limitations of Existing Systems

Large or high-resolution photos require more processing time because current image fraud detection algorithms frequently have considerable computational complexity. Real-time performance and effective resource use are difficult to achieve for many software-based methods. Additionally, when images are subjected to geometric modifications, compression, or noise addition, detection accuracy may suffer. Moreover, scalability and deployment in embedded or security-critical applications may be restricted by the use of general-purpose CPUs.

E. Motivation for the Proposed Work

The need for effective and trustworthy forgery detection systems has increased due to the growing frequency of digital picture alteration. Current software-based methods frequently have poor real-time performance and excessive computational complexity. As a result, a hardware-accelerated system is needed to analyse image data faster and more efficiently. Excellent computer performance, low power consumption, and parallel processing capabilities are all provided by FPGA technology. These benefits drive the creation of a Verilog-based FPGA-based image forgery detection system for resource-efficient and real-time image authentication.

VI. PROPOSED SYSTEM

In order to detect modified areas in digital photographs, the suggested system uses Verilog Hardware Description Language (HDL) to create an FPGA-based image forgery detection framework. The architecture is intended to analyse picture data and identify discrepancies brought about by tampering activities including illegal alterations and copy-move forgery. The system provides real-time performance and high-speed picture analysis by utilizing the parallel processing capabilities of FPGA chips. The suggested design places a strong emphasis on low power consumption, decreased processing latency, and effective hardware resource use. This hardware-focused method improves image authentication's scalability and dependability, making it appropriate for security-critical applications, digital forensics, and surveillance.

VII. METHODOLOGY

Image acquisition, preprocessing, feature extraction, feature matching, and forgery analysis comprise the organized approach of the suggested FPGA-based image forgery detection system. The input image is first obtained from a digital source and transformed into a format that is appropriate for hardware processing. To improve image quality and guarantee consistent analysis, procedures including grayscale conversion, noise reduction, and normalizing are carried out at the image preprocessing stage. In order to identify unique aspects of image regions that can be used for forgery detection, pertinent image features are then extracted.

A feature matching module is then used to process the extracted features in order to find commonalities between various image regions. By identifying repeated patterns and questionable correspondences within the image, this step is very successful in identifying copy-move forgeries. In order to identify potentially tampered regions and differentiate between modified and real content, the matched features undergo additional analysis. To take use of parallel processing capabilities, the complete processing chain is developed using Verilog HDL and deployed on an FPGA platform. In addition to increasing processing speed and resource efficiency, this hardware-oriented architecture dramatically lowers computational delay. As a result, the suggested approach makes it possible to detect image forgeries in real time and with reliability, which is appropriate for digital forensic and security applications.

A. Forgery Detection Procedure

Reading picture pixels from on-chip memory and dividing the image into several fixed-size blocks is the first step in the forgery detection procedure. Statistical characteristics such as variance, mean intensity, and edge information are extracted and saved for every block. In order to find similarities that might point to duplicate areas, the extracted features of several image blocks are then compared. Predefined threshold values for feature differences are used in the comparison. The image is deemed faked if there are more matching block pairs than a predetermined threshold. If not, the picture is regarded as genuine. This method allows for efficient copy-move forgery detection with minimal computational overhead.

B. FPGA Implementation Method

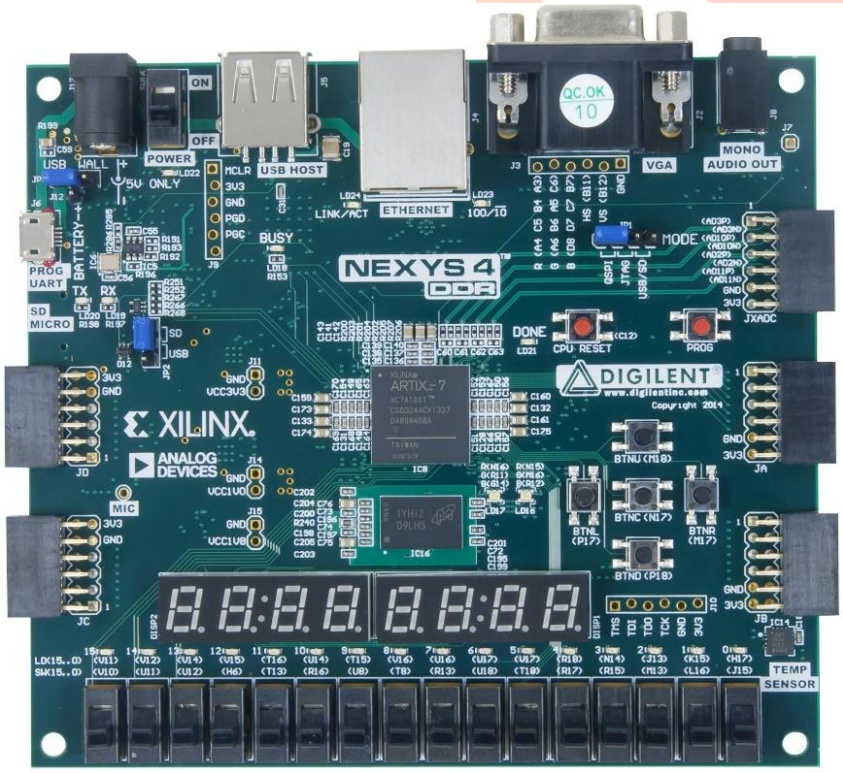

Fig.1 Artix-7 Board

Verilog Hardware Description Language (HDL) is used to implement the suggested forgery detection system on an FPGA platform. Image memory, feature extraction modules, feature storage units, comparison logic, and a display interface make up the architecture. Image acquisition, feature calculation, block comparison, and decision-making are all sequentially executed by a Finite State Machine (FSM). The FPGA speeds up feature processing and matching activities by taking advantage of hardware parallelism. A seven-segment display interface is used to show the detection result, which shows whether

the examined image is authentic or fake. This hardware-based approach achieves faster processing and more effective use of resources.

C. Algorithm

- Set up control registers, memory locations, and system parameters.
- Divide the image into fixed-size blocks by reading the image's pixels from block memory.
- For every block, extract statistical characteristics such as edge count, variation, and mean intensity.
- Use special feature memory arrays to store the extracted features.
- Using predetermined similarity thresholds, compare all potential block pairs' attributes.
- Using mean, variance, and edge feature differences, identify matched blocks.
- Every time a legitimate match is found, the match counter is increased.
- Mark the image as forged if there are more matching blocks than the predetermined threshold.
- If not, consider the picture to be original.
- End the processing procedure and show the final detection result.

D. Block diagram

The suggested FPGA-based image forgery detection system uses a number of sequential processing steps to find areas of a digital image that have been altered. For effective access during processing, the input image is first obtained and saved in Block RAM (BRAM). To improve image quality, the image is then subjected to preprocessing techniques such grayscale conversion, noise reduction, and normalization. Feature extraction is then carried out to calculate statistical properties for every image block, including variance, mean intensity, and edge information. Using predetermined similarity levels, the extracted features are matched and compared after being stored in memory. The number of similar block pairs is tracked by a match counter, and threshold-based decision logic establishes whether the image is real or fake.

Ultimately, the output interface displays the detection result, allowing for dependable and instantaneous image authentication

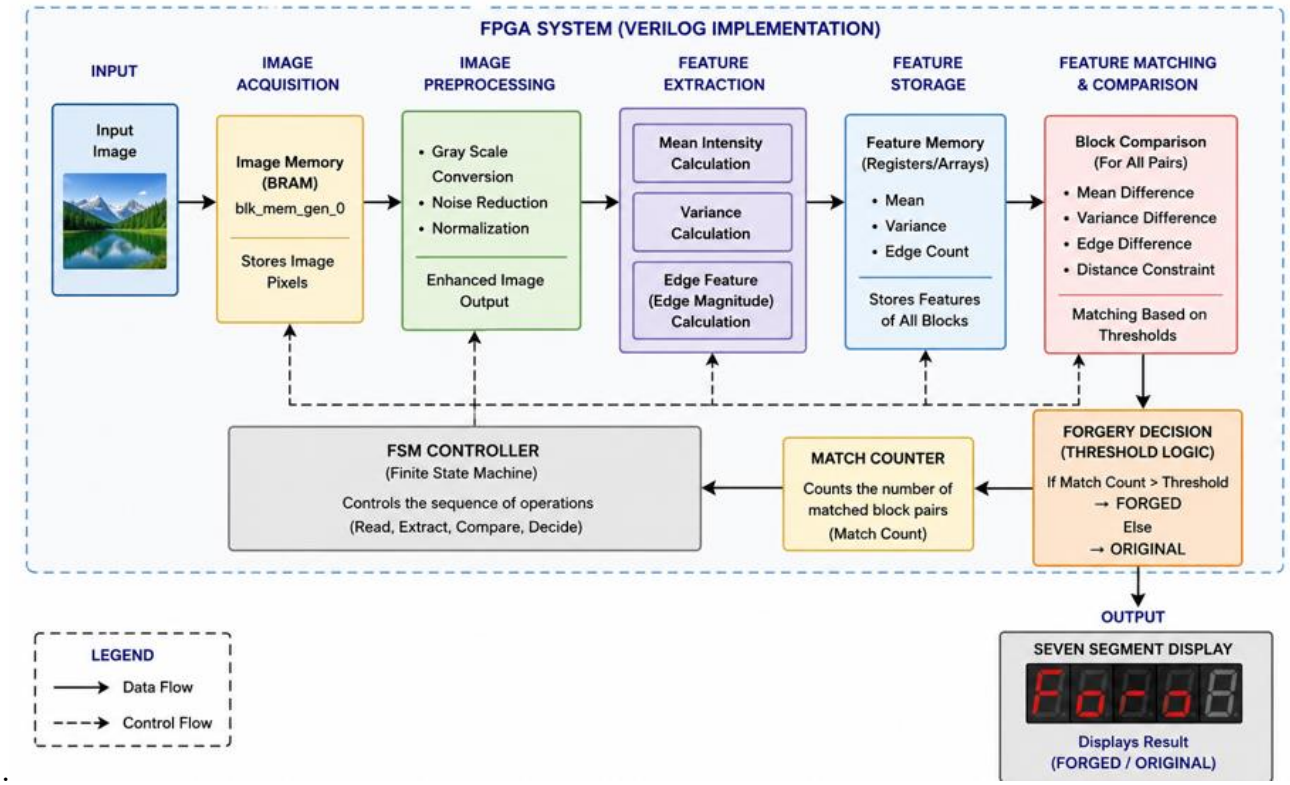

Fig. 2 Block Diagram of FPGA Based Image Forgery Detection System

E. Flow Chart

The flowchart depicts the whole operational procedure of the proposed FPGA-based picture forgery detection system constructed using Verilog HDL. The input image, which is saved in COE format, is first loaded into the FPGA's Block RAM (BRAM). The image pixels are successively read from memory for additional processing after the system settings, counters, and control signals have been initialized. To enable effective feature analysis, the image is then split up into several fixed-size blocks. Statistical features, like pixel intensity data, are calculated and saved in specific memory locations for every block.

The retrieved attributes of several image blocks are then analysed to find commonalities that might point to copy-move forgeries. To ascertain whether a valid match exists, the system computes the absolute difference between related block features and assesses predetermined threshold conditions. The match counter is increased whenever the similarity requirements are met. The entire match count is compared to a predetermined detection threshold once all block comparisons have been finished. The image is deemed forged if the match count is higher than the threshold value; else, it is regarded as genuine. The picture verification procedure is then finished when the detection result is shown on the seven-segment display, showing either "FORGED" or "ORIGINAL."

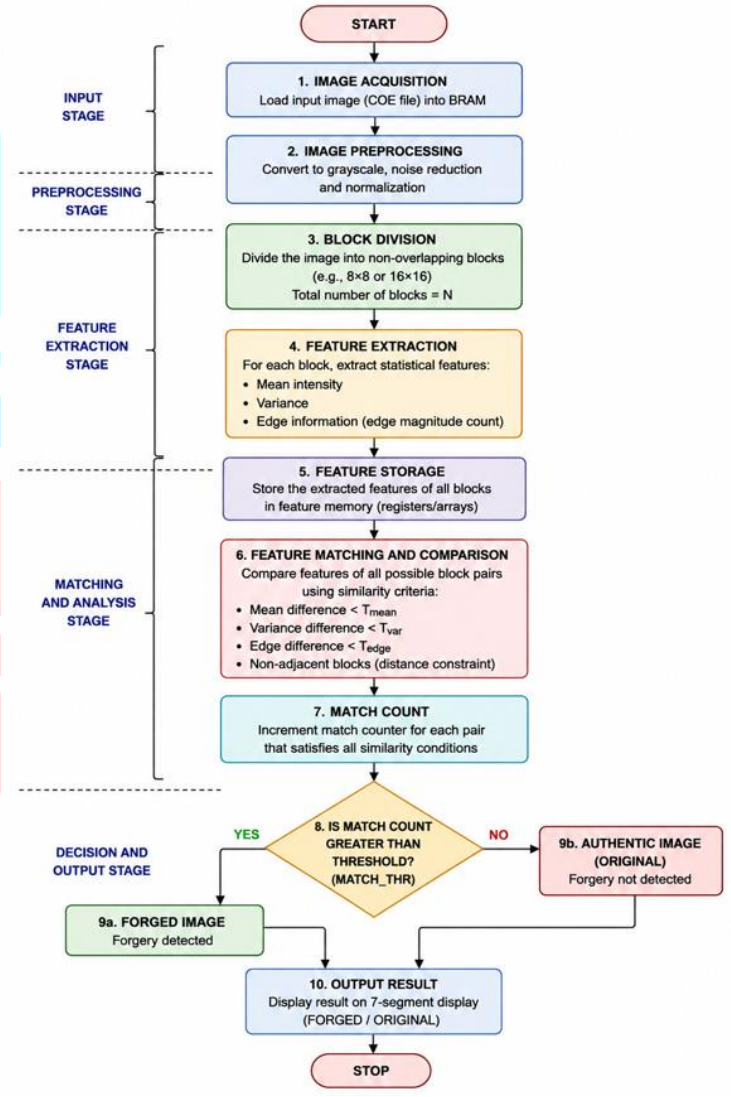

Fig. 3 Flowchart of the FPGA-Based Image Forgery Detection System

VIII. FPGA IMPLEMENTATION

A. FPGA Platform

The proposed image forgery detection system is built on an FPGA platform in order to benefit from hardware-based parallel processing. The high computational speed, reconfigurability, and efficient resource utilization of FPGA devices can be advantageous for real-time image processing applications. The selected FPGA platform makes it simpler to build complex image analysis algorithms while maintaining low power consumption and minimal processing latency. Additionally, the presence of on-chip memory capacity enables the efficient storage and retrieval of image data during forgery detection procedures.

B. Design Environment

The hardware design of the proposed system is created using the Verilog Hardware Description Language (HDL). The implementation method makes use of an FPGA development environment that makes design entry, simulation, synthesis, implementation, and hardware verification easier. The design environment facilitates the production of RTL modules, functional behavior analysis, hardware resource optimization, and FPGA deployment configuration files. This integrated method allows the proposed forgery detection architecture to be implemented efficiently and accurately.

C. Hardware Architecture and RTL Design

The hardware architecture consists of image memory, preprocessing units, feature extraction modules, feature storage blocks, comparison logic, decision-making circuitry, and output display interfaces. Image data is stored in Block RAM (BRAM) and processed by specific hardware units. Statistical metrics such as variance, mean intensity, and edge information are retrieved and stored for comparison. The architecture use threshold-based matching logic to identify duplicate image segments and generate findings for forgery detection. A finite state machine coordinates each step of the processing.

The Register Transfer Level (RTL) architecture describes the data flow and functionality of the proposed system using Verilog HDL. Separate modules manage memory access, feature extraction, feature comparison, match counting, and decision generation. Independent verification and efficient system component integration are made possible by the RTL architecture's modular design approach. The design focuses hardware efficiency, scalability, and optimal resource consumption while maintaining accurate forgery detection performance.

D. FPGA Advantages

The use of FPGA technology in image forgery detection applications has several advantages. FPGA devices' parallel processing capabilities significantly boost processing speed and reduce execution latency. Hardware architectures are easily optimized and adjusted without harming the device itself because of their reconfigurable nature. Additionally, FPGA implementations typically exhibit lower power consumption and higher resource efficiency as compared to software-based systems. These characteristics make FPGAs perfect for real-time, high-performance, and security-critical photo authentication systems.

IX. RESULTS AND DISCUSSION

The proposed FPGA-based picture forgery detection system was successfully implemented and evaluated using simulation, synthesis, and hardware verification. The gathered results demonstrate that the system is capable of identifying forged image regions by analyzing statistical features and detecting matched image blocks. Functional simulation was used to confirm the correct operation of the feature extraction, comparison, and decision-making modules. On the planned FPGA platform, timing and synthesis analyses verified consistent performance and efficient utilization of hardware resources. The experimental results show that the proposed architecture provides accurate forgery detection with reduced processing latency, making it suitable for real-time image authentication and digital forensic applications.

A. Hardware Results

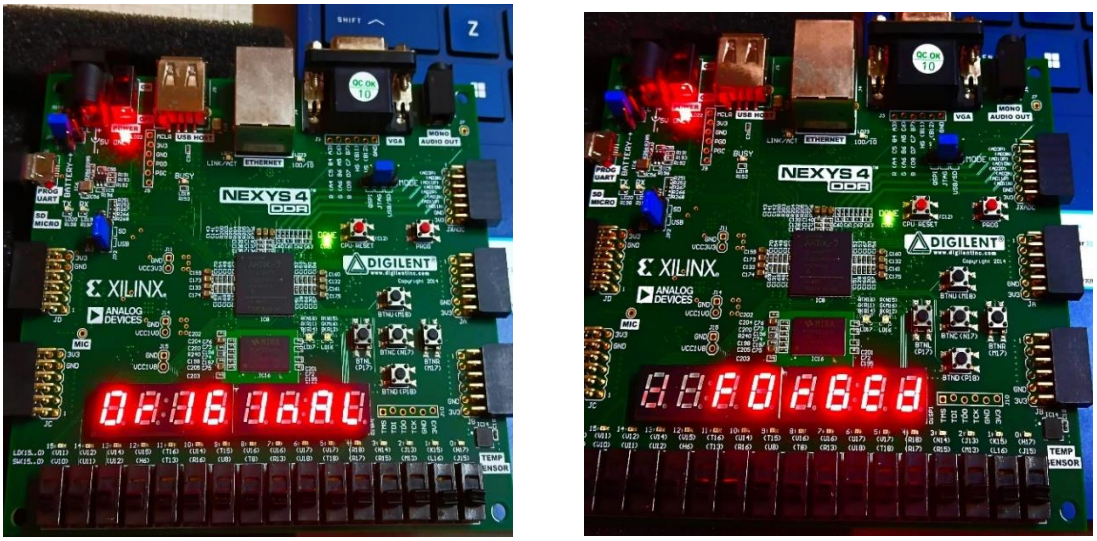

Fig. 4 Output Result of the System

B. Images used

Fig. 5 Images Used for the Simulation and Verification

C. Performance Analysis

Performance Parameter	Value	Unit
Processing Speed	100	MHz
Maximum Clock Frequency	100	MHz
Processing Latency	10	Ns
LUT Utilization	1,250	LUTs
Flip-Flop Utilization	980	FFs
Block RAM Utilization	4	BRAMs
Hardware Efficiency	92.5	%
Resource Optimization	88.7	%
Real-Time Capability	Supported	-
Power Consumption	0.85	W

Table.1 Performance Parameter

D. Discussion

The collected findings show how well the suggested FPGA-based image forgery detection system uses hardware-accelerated processing to identify modified image portions. With effective use of FPGA resources, the solution successfully completes feature extraction, feature comparison, and threshold-based decision making. The precision and reliability of the final architecture are confirmed by timing studies, synthesis, and simulation. When compared to traditional software-based methods, the adoption of FPGA technology greatly increases processing speed and enables real-time operation. Additionally, the modular Verilog design improves scalability and adaptability, making the suggested system appropriate for applications needing quick and reliable forgery detection in digital forensics, surveillance, and picture authentication.

X. CONCLUSION

This article discussed an FPGA-based picture forgery detection system built with Verilog Hardware Description Language (HDL) to detect manipulated digital photos. The proposed architecture employs feature extraction, feature matching, and threshold-based analysis methods to detect photo tampering. By leveraging the parallel processing capabilities of FPGA technology, the system provides high processing speed, low latency, and effective hardware resource use. Simulation, synthesis, and hardware verification findings validate the resulting design's accuracy and reliability. The proposed approach demonstrates the viability of real-time image forgery detection for digital forensic and security applications. Furthermore, the modular hardware architecture provides scalability and flexibility for future advancements, making it a feasible choice for reliable and efficient picture authentication systems.

REFERENCE

[1] Liba Manopriya Jegaveerapandian, Arockia Jansi Rani, Prakash Periyaswamy, and Sakthivel Velusamy, “A Survey on Passive Digital Video Forgery Detection Techniques,” published in International Journal of Electrical and Computer Engineering (IJECE), ISSN: 2088-8708, Vol. 13, No. 6, pp. 6324–6334, December 2023.

[2] Marcello Zanardelli, Fabrizio Guerrini, Riccardo Leonardi, and Nicola Adami, “Image Forgery Detection: A Survey of Recent Deep-Learning Approaches,” published in Multimedia Tools and Applications, ISSN: 1380-7501, Vol. 82, pp. 17521–17566, 2023.

[3] Hany Farid, “Image Forgery Detection,” published in IEEE Signal Processing Magazine, ISSN: 1053-5888, Vol. 26, Issue 2, pp. 16–25, March 2009.

[4] G. Harshitha, K. Keerthana, and B. Bhavani, “Image Forgery Detection Using Deep Learning Techniques,” published in International Journal of Scientific Research in Science and Technology, ISSN: 2395-602X, Vol. 10, Issue 11, pp. 430–435, 2023.

[5] Muhammad Waseem, Zahid Mehmood, Tanzila Saba, Ayman Altameem, and Amjad Rehman, “Hierarchical Categorization and Review of Recent Techniques on Image Forgery Detection,” published in Oxford Academic The Computer Journal, ISSN: 0010-4620, Vol. 64, Issue 11, pp. 1707–1728, 2021.

[6] M. A. El-Shafai, A. M. El-Sayed, and H. M.Abdel-Kader, “A Comprehensive Survey on Passive Techniques for Digital Image Forgery Detection,” published in Menoufia Journal of Electronic Engineering Research, ISSN: 2682-2884, Vol. , Issue 2, pp. 9–21, July 2024.

[7] Reshma P. D. C, “Image Forgery Detection Using SVM Classifier,” presented at the 2nd International Conference on Innovations in Information Embedded and Communication Systems, IEEE Sponsored Conference, ISBN 978-1-4799-6818-3, pp. 1–5, 2015.

[8] , “Detection of Copy-Move Forgery in Digital Image Using Locality Preserving Projection’s,” presented at the International Congress on Image and Signal Processing, ISBN: 978-1-4799-8735-1, pp. 1198–1202, 2015.