Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/69

Implementation of Digital Image Watermarking That Is Both Safe and Effective in Terms of Space on a Reconfigurable Platform

Surendra Shukla[1], Durgaprasad Gangodkar[2], Devesh Pratap Singh[3], Rajesh Upadhyay[4]

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[3]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[4]School of Management,Graphic Era Hill University, Dehradun, Uttarakhand India, 248002

ABSTRACT

Now a day digital data is straightforward to handle yet it lets unauthorised users to obtain this information. In order to prevent unwanted access, typical methods include encryption and watermarking. In this research, we propose a Discrete Wavelet Transform (DWT)-based, cryptographically-integrated, invisible picture watermarking method for rapidly deploying new configurations of hardware. In DWT implementation, simpler equations are created for creation of approximation and detailed coefficients owing to which this operation requires only 306 slice registers and its maximum operating frequency is 556.174 MHz

Keywords: Cryptography, Deadweight tonnage , Advanced Encryption Standard, Field Programmable Gate Arrays, Very-large-scale integration, Watermarking

INTRODUCTION

Rapid advancements in IT and widespread availability of digital consumer devices occurred in the prior decade. However, this makes the system vulnerable to hacking and creates duplicates of the original data. Digital Rights Management (DRM), which includes cryptography and watermarking, may be used to prevent illegal access to this digital data. The goal of cryptography is to ensure that only authorised parties have access to sent data by encrypting it before transmission. There are two distinct categories of cryptography, distinguished by the kind of the key they use. Bits, not alphabets, are used to represent data in digital systems. Block cyphers and stream cyphers are the two main categories of symmetric key cryptography based on the different ways in which these binary values are handled. The plaintext of a block cypher is broken down into groups of bits and processed one block at a time. where plaintext is handled byte-by-byte in a stream cypher. Digital watermarking is the technique of embedding hidden information about digital media (video, audio,

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/69

etc.) inside the media itself. Digital watermarking may be broken down into two distinct categories—those that are visible to the naked eye and those that are not. When using visible watermarking, the watermark is plainly discernible, but when using invisible watermarking, it is not. A more secure method is invisible watermarking, which is resistant to assaults from signal processors.

Rather than altering pixel values, as is done in traditional watermark removal methods, transform domain techniques instead alter transform coefficients, from which the inverse transform is then employed to retrieve the watermark.

DCT and DWT are two popular methods in the transform area. With the spatial domain method, the watermark data is incorporated into the image's pixels itself. Since the coefficients of the watermark are dispersed over the cover picture, transform domain approaches are able to provide more resilience against compression and filtering attacks.

REVIEW OF THE LITERATURE

For both lossy and lossless image compression, [1] suggested an efficient FPGA implementation of DWT. Using a frequency of 43.63 MHz, it makes use of 144 slice registers. Strong, undetectable picture watermarking was advocated by [2] using MATLAB. As seen by the test results, the proposed design holds up well in the face of a wide variety of pictures. Real-time image processing benefits from the DRM approaches outlined by [3], which were implemented on an FPGA using 2117 slices and a maximum operating frequency of 228.064 MHz. Systematic VHDL-based design, modelling, and simulation was proposed by [4]. This technique was implemented on a Virtex-5 processor, which allowed for the use of 249 slices at a maximum speed of 400 MHz. In [5], proposed robust invisible picture watermarking using MATLAB and discrete wavelet transforms. The proposed layout has been tried with both colour and monochrome photos, and the results confirm its durability. Khose want to implement the AES algorithm in hardware in a way that reduces resource use without sacrificing throughput. The suggested system uses BRAM in place of standard S-box logic to provide results in real time [6].

Using steganography, [7] proposed a way to conceal numerous colour pictures inside a single colour image using DWT. An effective DES implementation on less dense FPGA was advocated by [8]. In order to verify the authenticity of the original data, [9] presented a System Generator-based hardware solution. This design employs 4708 slices at a frequency of 344 MHz, as shown by the synthesis results. According to the work of Borkar AM et al. [10], an FPGA-based AES algorithm was proposed, and it was then simulated and improved in software. Here, hardware requirements are minimised by using an iterative design process. The ASIC implementation of a crypto algorithm was reported Blowfish cryptography has been prototyped on 130 nm bespoke IC. Presented a partially pipelined sequential structure based on System Generator to boost performance and efficiency. At a junction temperature of 280 degrees Celsius and a power consumption of 117 milliwatts, its operating frequency is 231 megahertz. In order to safeguard property rights,suggested a specific method. Before the watermark is inserted in the HL and LH blocks of the original picture, the suggested approach runs it via Discrete Wavelet Transformations. The problems and solutions for developing a robust picture watermarking method were described byA novel approach to

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/69

embedding biometric data into a picture was described by. With respect to the safeguarding of official documents, offered an alternative approach. Invisible robust and fragile picture watermarking were both given, who detailed the design of a VLSI framework for a high performance spatial domain watermarking device. The resilient invisible combined DWT-DCT digital picture watermarking method was described. An efficient FPGA version of the AES algorithm was proposed which makes use of pipelining methods as part of architectural optimization. With a maximum clock speed of 19.954 MHz and a total of 6279 Slices and 5 BRAMs, Virtex-2 is used to execute an efficient programme.

When compared to the outcomes of the suggested design, it is obvious from the literature research that just one design has been executed up to this point. In addition, several researchers have developed and published FPGA-based AES algorithm implementations and/or FPGA-based digital picture watermarking. FPGA-based DWT-oriented digital picture watermarking is achieved with efficient results using [3]. Maximum frequency of 228.064 MHz was utilised with 2117 slices in this application. Multiple authors have attempted to perform picture watermarking on a reconfigurable platform, however the resulting implementations are inefficient because of the need to convert MATLAB code to HDL. As a result of this mode of operation, the system's speed is diminished, and more space is required in the design. However, if HDL or a system generator is used throughout the design phase, optimal performance and minimal overhead may be attained. Watermarking alone isn't a foolproof technique, but when paired with encryption, it becomes much more so. In this research, we propose using a reconfigurable platform and the AES method for digital picture watermarking based on discrete wavelet transforms.

Proposed Design

The first step of watermark embedding is to run the original picture and the watermark through DWT. To get the watermarked version of the picture, the embedded output is fed through an inverse discrete wavelet transform. In addition, the picture with the watermark is encrypted using AES to create an encrypted watermarked image. When doing watermark extraction, an encrypted watermarked picture is used as input for AES decryption, yielding the original watermarked image as output. The next step is wavelet decomposition of the watermarked picture. The inverse DWT is then used to remove the watermark.

Watermark embedding and watermark extraction rely heavily on DWT-IDWT and AES Encryption/Decryption.

Applying Discrete- and Discrete-Irreversible Transforms:

Discrete wavelet transform (DWT) is a transform implementation that uses discrete samples of wavelets. This makes use of sub-band coding in a practical sense. Sub-band coding works by breaking down the input spectrum into a series of band-limited components. By piecing together these sub-bands, we can accurately reproduce the original spectrum. Wavelet analysis often use the framework. where Coefficients of approximation, or Cx Coefficients of granularity, denoted by Dx

In order to get sub-bands with greater frequency for coarser temporal resolution and lower frequency sub-bands for finer frequency resolution, DWT decomposes a signal into multiple sub-bands at various frequencies. We see examples of single-level, two-level, and three-level

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/69

decompositions of a picture. The suggested work substitutes the right shift and left shift operations for multipliers and divisions to yield approximation and detail coefficients. This results in less needed storage space (slices/LUTs). Additionally, this version has an optimised operating frequency.

Utilizing the Advanced Encryption Standard Algorithm
The fact that the same key may be used for both encryption and decryption classifies AES as a symmetric key block cypher. The AES algorithm was developed using linear transformation as its foundation.

All of the rounds' keys in the proposed work are created in MATLAB and then utilised in the corresponding VHDL code. This reduces the total amount of slices needed for the key generation procedure.This technique takes an encrypted plaintext block of 128 bits and a decrypted key block of 128 bits as input. AES algorithm being put into practise by means of a system generator.

Unencrypted Original Image
Image Decrypted
the first edition's cover and watermark
The Use of Watermarking with Encryption (c)
d. Picture With A Watermark
The Watermark Was Efficiently Removed
MATLAB 2013 is used to create the overall implementation's Simulink model..
Five, a comparison of our system to other FPGA-based implementations is necessary to determine the effectiveness or efficiency of the proposed system. Seeing as how this is a whole new take on FPGA-based systems, we compared our findings to those of other, very comparable implementations. Watermarking by itself has been successfully implemented in a number of FPGA-based systems, with varying degrees of success in terms of area use and operation frequency.

CONCLUSION

In this work, we provide a safe and efficient FPGA implementation of digital picture watermarking. According to the reviewed literature, it is evident that up till now, the most effective performance of FPGA based picture watermarking alone has been achieved which employs 2117 slices at maximum working frequency of 228.064 MHz. The optimal layout incorporates encryption and DWT-based watermarking. The proposed layout has a slice count of 2961 and a frequency of 148.895 MHz. Because of the increased throughput and decreased footprint, the suggested implementation is more suited to image processing applications, and the addition of the cryptographic technique makes it more safe.

REFERENCES

1. Savakar, D. G., & Ghuli, A. (2019). Robust invisible digital image watermarking using hybrid scheme. *Arabian Journal for Science and Engineering*, *44*(4), 3995-4008.
2. Zheng, Z., Saxena, N., Mishra, K. K., & Sangaiah, A. K. (2018). Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications. *Future Generation Computer Systems*, *88*, 92-106.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/69

3. Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, *97*, 95-105.
4. Loan, N. A., Hurrah, N. N., Parah, S. A., Lee, J. W., Sheikh, J. A., & Bhat, G. M. (2018). Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*, *6*, 19876-19897.
5. Ambadekar, S. P., Jain, J., & Khanapuri, J. (2019). Digital image watermarking through encryption and DWT for copyright protection. In *Recent trends in signal and image processing* (pp. 187-195). Springer, Singapore.
6. Savakar, D. G., & Pujar, S. (2018). Digital image watermarking using DWT and FWHT. *International Journal of Image, Graphics and Signal Processing*, *10*(6), 50.
7. Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2018). Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. *Multimedia Tools and Applications*, *77*(20), 26845-26879.
8. Kumar, C., Singh, A. K., & Kumar, P. (2018). A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications*, *77*(3), 3597-3622
9. Kaur, K. N., Gupta, I., & Singh, A. K. (2019). Digital image watermarking using (2, 2) visual cryptography with DWT-SVD based watermarking. In *Computational intelligence in data mining* (pp. 77-86). Springer, Singapore.
10. Shinde, G., & Mulani, A. (2019). A robust digital image watermarking using DWT-PCA. *International Journal of Innovations in Engineering Research and Technology*, *6*(4), 1-7.