RBWCI: Robust and Blind Watermarking Framework for Cultural Images

Publisher: IEEE

Samrah Mehraj ; Subreena Mushtaq ; Shabir A. Parah ; Kaiser J. Giri ; Javaid A. Sheikh ; Amir H. Gandomi ; Mohamma… **All Authors**

Abstract: Heritage multimedia, which comprises images, audio, and videos, are precious artifacts of a region. In addition to enabling a better understanding of earlier generations,... **View more**

Metadata

Abstract:

Heritage multimedia, which comprises images, audio, and videos, are precious artifacts of a region. In addition to enabling a better understanding of earlier generations, heritage media provides information about their creative approach, style of living, and diversity of historical and archaeological ideologies. Heritage is an important resource that boosts the local economy, generates sustainable communities, and improves tourism and business sectors. Once heritage images are dissipated to consumers, they may be transmitted through wire/wireless systems, where the data may be accessed by both authorized and unauthorized consumers. With the rapid advancement of technology and 5G networks, establishing an approach that protects cultural heritage media from unauthorized consumers is necessary. This study presents a robust and blind watermarking-framework for cultural images (RBWCI) utilizing the discrete cosine transform domain for ownership verification and copyright protection. The embedding scenario of our technique relies on the difference between coefficients obtained from the two channels of the YCbCr color model. The watermark bit is embedded by taking the difference between two preselected mid-frequency coefficients (Cb-Cr). Moreover, chaotic and deoxyribonucleic acid encryption are employed to ensure double-layer watermark security. The proposed algorithm demonstrates a peak signal-to-noise ratio between 42-43 dB and structural similarity index metric value of approximately 1 for different test images when not under attack. The robustness of the RBWCI was revealed by comparing it with various state-of-the-art schemes, making it suitable for different consumer applications.

Published in: IEEE Transactions on Consumer Electronics (Volume: 69 , Issue: 2, May 2023)

Page(s): 128 - 139

Date of Publication: 28 October 2022

INSPEC Accession Number: 22999430

DOI: 10.1109/TCE.2022.3217974

Publisher: IEEE

ISSN Information:

Print ISSN: 0098-3063
Electronic ISSN: 1558-4127

Funding Agency:

No metrics found for this document.

Contents

Cultural heritage (CH), as defined by UNESCO, includes multiple performances, practices, systems of skills and knowledge, forms of expressions, as well as related objects, tools, cultural places, and crafts that are considered CH by many groups [1]. CH is also perceived to create employment prospects, boost the identity of community cultures, and reinforce social wealth. The digitization of CH permits the formation of a warehouse of cultural and historical-tangible heritage, provides global access to the various cultures of the world's heritage, protects its treasured resources against degradation, and thereby ensures its instant preservation for future generations. Moreover, a smart camera network consists of homogenously distributed intelligent camera devices that can process and transmit digital pictures. The data in these devices, when shared with a cluster of available digital devices, such as mobile phones, laptops, and TVs, face the risk of copyright violation against unauthorized consumers. In addition, owing to the rapid development of technology, the growth of 5G networks is expected to satisfy greater performance demands and extreme capacity. While this has enabled the widespread dissemination of cultural images, it has increased the risk of data breaches. Many informative, educational, and social websites have been affected by illegal accesses worldwide. MyHeritage, a genealogical service website providing information about ethnic backgrounds, was affected by a data breach that affected 92 million consumers. Developing technologies, such as software-defined networks, Internet of Things (IoT), 5G platforms, network function virtualization, and pervasive edge computing (PEC), are expected to become leading pillars of technology. To satisfy the requirements of mobility support, location awareness, and low latency, PEC brings cloud-related resources and facilities closer to consumers [2], [3]. PEC is a notion wherein storage, networking, and computing resources are integrated into a base station. However, concerning security, PEC is difficult in a disseminated environment because the data handling capacity of many devices is less secure than that of centralized systems [3]. This necessitates the formulation of the latest security alternatives for privacy protection and data safety [4]. Optical sensors have recently emerged in IoT systems because of their potential to produce versatile and huge amounts of information [5]. Steganography, digital signatures, encryption, and digital watermarking are employed to safely transfer information with high network insecurity in these environments [6]. For solving problems such as copyright protection, data authentication, and digital fingerprinting; digital watermarking has proven to be the best option [7], [8]. This is explained in Figure 1 by considering a general scenario of sending a precious CH image by the heritage site owner. Two possibilities may arise: In case (1), the CH images are transmitted without the addition of a watermark, and in case (2), the pictures are sent with the addition of a watermark. In both cases, the data is available to both authorized and unauthorized consumers. In case (1), the owner has no IP protection, resulting in revenue loss for the owner/authorized consumer and gain of illegal money for the unauthorized consumer. Conversely, in (2), the owner has IP protection, resulting in revenue gain for the owner/authorized consumer and enables the owner to claim ownership if any illegal access occurs. Typically, studies on watermarking heritage images are based on grayscale images. However, in current scenarios, the implementation of camera sensors can provide colored data that must be protected. The RGB color space is used to represent most real-world color images owing to the correlated red, green, and blue channels [9]. Based on the visual data, the YCbCr color model divides an image into three components: one of luminance (Y) and two of chrominance (Cb and Cr). Fig. 1.