

# A Hybrid Concept of Cryptography and Dual Watermarking (LSB\_DCT) for Data Security

Ranjeet Kumar Singh, National Institute of Technology, Department of Computer Applications, Jamshedpur, India

Dilip Kumar Shaw, National Institute of Technology, Department of Computer Applications, Jamshedpur, India

## ABSTRACT

Now a days, in communication technology safety of digital data in the form of text, image, and video, audio is a biggest problem. With the rapid development of the network multimedia systems, security is the biggest issue. Digital watermarking is one of the solutions to these problems. It hides some secret data into the original image and this information is use for image authentication and security. This paper Focus an application using Hybrid approach of Cryptography technique and dual watermarking for the purpose of Providing highly security and authentication of digital data. This paper use cryptography and QR Code in combined approach of LSB and DCT Digital image water marking technique. The Experimental results are given in the form of table and graph. This algorithm provides more security and data authentication compare to other image data security approach.

## KEYWORDS

Cryptography, PSNR, QR Code, SNR, Watermarking

## INTRODUCTION

Now a days, digital media is extremely used through the internet, and the requirement for copyright protection of hypermedia products has emerged. Research has been concentrated to solve a problem of copyright protection and authentication of digital data. In digital data, there is no major difference between the origin data and its copy, so it is very difficult task to identify the original data. Hence, the security of the intellectual property is necessary and important for the society (Sridhar et al., 2010). There are many techniques available for copy right protection. Watermarking is one of the popular techniques for protection of text, image video, audio data. Watermarking is a technique which hides information into original data (Karimi et al., 2013)

## Watermarking

The latest growth of fast communication network and explosion of a huge network of multimedia systems has discouraged the multimedia & hypertext content providers. The authors and producers hesitate to share their article on the network environment because they have no control to protect from copy. The intelligent property with authentication is becoming very important issue today (Karimi et al., 2013). Instead multiple efforts and resources are working to make authorize intellectual property. The total cost of producing such intellectual property and creations of typically constitute significant formation. However, the creator of multimedia is always need some awards with motivation for

DOI: 10.4018/IJISP.2018010101

the development. The researchers today, are involving to the research in image processing with the specialization in watermarking. The basic property of the image allows multiple control and fact to judge the purity and classify accordingly.

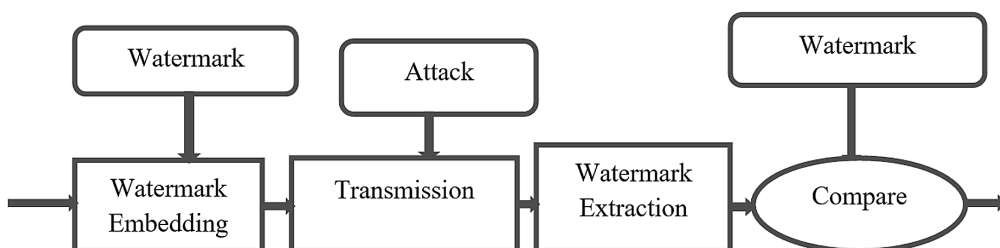
All the watermarking process has basic approach with the component in algorithm, the Figure 1 presents the block diagram of steps with component used in watermarking. Basically, digital watermarks are used as identity information to identify the owner by verifying authenticity and integrity of the image. It is specially used for finding copyright infringements and for banknote authentication. In the past decade, as the information digitalization and internet were developed, digital media increasingly rapidly over traditional analog media. However, as one of the concomitant side-effects of digital media, that it is also becoming easier and providing an easy approach for some individual or group to copy and transmit digital products without the permission of the owner. And to solve this problem watermarking technique were introduced. There are many subject covered by watermarks such as signal processing, encryption and communication theory. The research in the field of digital watermark aimed to provide to prevent and trace prohibited copying and transmission and security of copyright to digital products.

Watermarking techniques are rarely used in spatial domain but widely used in transform domain because spatial domain based watermarking can easily be affected by basic image operation. The spatial domain techniques are not complex to implement, so they cannot withstand low pass filtering. The frequency domain of watermarking are achieved by i.e. DCT, DFT and DWT etc. The comparison of developed techniques reflects that the frequency-domain watermarking is most effective with realizing the imperceptibility and robustness. (Rekha et al. 2014, Mitali et al., 2013). The DWT is most widely researched Frequency-Domain based transforms. The Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) are also used with their own important characteristics and applications. DWT exist fine spatial localization with multi-resolution characteristics, those are matches to theoretical models of human visual system. Further, performance improvement of DWT based Watermarking algorithms changes with the level of DWT (Naghsh et al., 2008).

An effective and interactive watermarking technique should be considering the several properties (Naghsh et al., 2008).

- **Transparency:** The embedded watermark in the image should be perceptually and visually imperceptible. This requirement holds the most challenges for the images having noticeable pixel similarities in different parts of the image. The fixed watermark in the images should must be perceptually invisible because this holds the most challenges
- **Robustness:** The watermarked image should be robust i.e. watermark should not be easy to remove or destroy from image and before missing of the watermark, watermarked image should be degraded. It should also be robust against certain occasional or intentional attacks

Figure 1. Watermark embedding and extraction process



10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/a-hybrid-concept-of-cryptography-and-dual-watermarking-lsbdct-for-data-security/190852](http://www.igi-global.com/article/a-hybrid-concept-of-cryptography-and-dual-watermarking-lsbdct-for-data-security/190852)

## Related Content

---

### Managing the Commonplace: Small Water Emergencies in Libraries

Gerald Chaudron (2016). *International Journal of Risk and Contingency Management* (pp. 42-61).

[www.irma-international.org/article/managing-the-commonplace/148213](http://www.irma-international.org/article/managing-the-commonplace/148213)

### Improving Power Analysis Peak Distribution Using Canberra Distance to Address Ghost Peak Problem

Hridoy Jyoti Mahantaand Ajoy Kumar Khan (2018). *International Journal of Information Security and Privacy* (pp. 27-41).

[www.irma-international.org/article/improving-power-analysis-peak-distribution-using-canberra-distance-to-address-ghost-peak-problem/208125](http://www.irma-international.org/article/improving-power-analysis-peak-distribution-using-canberra-distance-to-address-ghost-peak-problem/208125)

### ICMetric-Based Secure Communication

Shahzaib Tahirand Imran Rashid (2016). *Innovative Solutions for Access Control Management* (pp. 263-293).

[www.irma-international.org/chapter/icmetric-based-secure-communication/152966](http://www.irma-international.org/chapter/icmetric-based-secure-communication/152966)

### Will Comparative Effectiveness Research Lead to Healthcare Rationing?

Mary Brown (2011). *Ethical Issues and Security Monitoring Trends in Global Healthcare: Technological Advancements* (pp. 1-21).

[www.irma-international.org/chapter/will-comparative-effectiveness-research-lead/52356](http://www.irma-international.org/chapter/will-comparative-effectiveness-research-lead/52356)

### Designing Secure Data Warehouses

Rodolfo Villarroel, Eduardo Fernandez-Medina, Juan Trujilloand Mario Piattini (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 1048-1061).

[www.irma-international.org/chapter/designing-secure-data-warehouses/23142](http://www.irma-international.org/chapter/designing-secure-data-warehouses/23142)