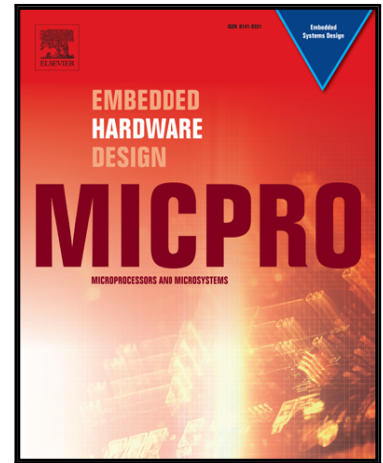


Accepted Manuscript

Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller

Siva Janakiraman , K. Thenmozhi ,
John Bosco Balaguru Rayappan , Rengarajan Amirtharajan

PII: S0141-9331(17)30247-8
DOI: [10.1016/j.micpro.2017.10.013](https://doi.org/10.1016/j.micpro.2017.10.013)
Reference: MICPRO 2631



To appear in: *Microprocessors and Microsystems*

Received date: 17 May 2017
Revised date: 22 October 2017
Accepted date: 27 October 2017

Please cite this article as: Siva Janakiraman , K. Thenmozhi , John Bosco Balaguru Rayappan , Rengarajan Amirtharajan , Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller, *Microprocessors and Microsystems* (2017), doi: [10.1016/j.micpro.2017.10.013](https://doi.org/10.1016/j.micpro.2017.10.013)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller

Siva Janakiraman^{1*}, K Thenmozhi¹, John Bosco Balaguru Rayappan¹, Rengarajan Amirtharajan¹

¹Faculty, School of Electrical & Electronics Engineering, SASTRA University, Thanjavur, Tamilnadu, India

*Corresponding Author: siva@ece.sastra.edu

ABSTRACT

The scintillating technological advancements have redefined the process of communication around the world. Banking, purchases, investments, emails, bill payments, etc. are being managed through online communications and needless to mention the linkage of these internet serves with embedded gadgets. A microcontroller being the low-cost solutions for real-time embedded applications has to handle rigid security algorithms for information security paradigm. The high level of sensitivity in chaos-based systems is highly suitable for the design of encryption schemes due to the randomness offered by them. The minimal memory resource and speed are the factors restricting the use of microcontrollers for implementing chaotic schemes that encrypt image data. This paper presents the design of a chaos-based image encryption algorithm with lightweight properties and its optimised implementation on a 32-bit microcontroller. This work also includes parameters related to the analysis of the security level and performance of the microcontroller that was missed to concentrate by the authors on their similar schemes reported in the literature. The level of safety of the proposed algorithm has been analysed via key sensitivity analysis, encryption quality analysis, randomness analysis, differential analysis, statistical analysis, visual analysis and attack analysis. Additionally, the results of performance analysis regarding smaller memory footprint and better throughput of proposed algorithm guarantee its suitability for real-time embedded applications.

Keywords: Image Encryption; Chaotic; Microcontroller; Hardware security; Lightweight and Embedded system.

1. Introduction

Communicating digitised form of visual information among transmission network has happened to be an essential need of the present world [1]. The presence of intruders in the communication medium necessitates the security solutions to protect the information from unauthorised access. Medical images like X-rays are the grayscale images that demand high security. One solution called cryptography [2] keeps the image visible after hiding its readability feature through a process known as encryption. The other solution called steganography [3], hides the image behind a cover by the process of embedding and leaves the image visible to all in the form of stego cover. The cover used is an image; it has been referred as image steganography. Both techniques are equally useful regarding securing the information being communicated from the perception of unauthorised persons. Many techniques have been found

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات