Optik xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Digital camera with image encryption

Jun Li*, Ting Zhong, Meixia Jiang, Bo Dai, Renfei He, Rong Li

Laboratory of Quantum Engineering and Quantum Materials, School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 5 February 2015
Accepted 29 October 2015
Available online xxx

Keywords:
Camera system
Image encryption
Image compression
Chaos system
DM6446

ABSTRACT

In this paper a camera system with image encryption is proposed, which integrates image acquisition, image encryption and image compression into the camera system. In contrast to conventional camera just acquiring image and compressing it, this camera system gathers original image data coming from outside scene with CCD, then compresses and encrypts it by three-dimensional Lorenz chaos sequence XOR original image data in DSP chipset. Finally the secured image data are stored in the camera or transmitted via network on the system. We designed the prototype camera based on the DM6446. Our preliminary experiment shows that the new camera system can make up for the deficiency of current camera and effectively protect the secret image or privacy image preventing from stealing and peeking by unauthorized users.

1. Introduction

With the rapid development of computer network technology, data become more important to businesses and the security on communication becomes more and more important [1,2]. For digital image, there are two major protection methods [3]. One is information hiding which includes watermarking, anonymity, steganography and cover channel [4–7]. The other is encryption which includes conventional encryption and chaotic encryption [8,9]. We show by comparing and assessing the survey that the conventional cryptographic algorithms such as DES, AES, VEA, which generally aim at encryption text data, however, are not well suited for image encryption [10]. Compared with the text data encryption, image encryption is characterized by a number of peculiarities, such as bulk data capacity and high correlation among pixels, which are generally difficult to handle by conventional methods. The desirable cryptographic properties of Lorenz chaotic such as initial conditions and random-like behavior can be used to develop new encryption algorithms. The chaos based cryptographic algorithms have suggested new ways to develop efficient image encryption schemes. The random-like nature of chaos is effectively spread into encrypted images. The proposed method transforms the statistical characteristic of original image information. So, it increases the difficulty of an unauthorized individual to break the encryption [11]. The proposed symmetric image encryption algorithm provides an effective way for real-time applications and transmission in our camera system.

In the existing schemes of image encryption, we get an image, process and compress it in the camera, then save the image or send the image data to the network without encryption. Traditional data encryption schemes can be used to prevent eavesdropping, but this method is dangerous. For example, they cannot prevent the misuse of closed circuit television (CCTV) video by authorized personnel, as in the cases of voyeurism and criminal purposes [12]. For another example, if you lost your camera, the image which is stored in it without encryption will be stolen by others. To solve these problems, we designed a system that integrates the image encrypting and processing in the same camera system. We can transmit an encrypted image on the encrypted channel. So, this method can protect the image information better.

We organize the structure of this paper as follows. Section 2 briefly introduces the system overview of the whole system. Section 3 explains the theory of Lorenz chaotic encryption and how it is used in our system. Section 4 explains experimental results and analysis. Finally, Section 5 concludes the paper.

2. System overview

DM6446 are the peripheral parts of the system, and CCD sensor, memory (SD card or mass storage), Synchronous Dynamic Random Access Memory (SDRAM), network controller and so on are the peripheral parts of a camera system with image encryption. The system hardware configuration is shows in Fig. 1.

* Corresponding author. Tel.: +86 13710872106.
E-mail address: lijunc@126.com (J. Li).

http://dx.doi.org/10.1016/j.ijleo.2015.10.211
0030-4026/

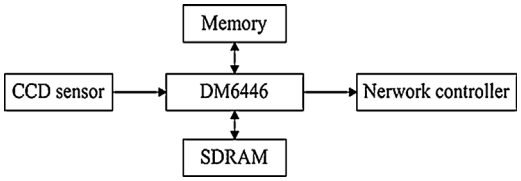

Fig. 1. The hardware configuration of this system.

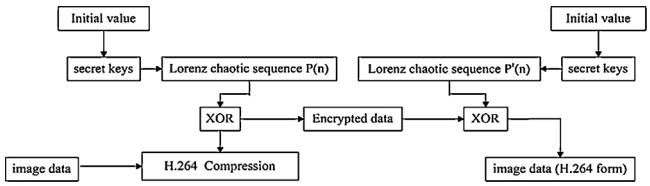

Fig. 2. The software model of the camera system with image encryption.

The principle of a camera system with image encryption as follows: first, DSP sends image acquisition command to get an image data from CCD sensor. Second, it writes the data to SDRAM to store the image. Finally, DSP reads the data from SDRAM and processes the data to image encryption and compresses in the camera, and saves the encrypted data in memory or sends the data to network.

3. Image encryption and compression in the camera system

Lorenz system is a classical three-dimensional chaotic system, which is complicated nonlinear dynamical system. The Lorenz chaotic sequence is generated by Lorenz system. It is an inherent random behavior expressed by defined system and quasi-random movement that seemingly is irregular. Due to the fact that chaotic system can generate very large period and excellent stochastic sequence, it can produce high security key flow, and chaos system can provide many secret keys by its sensitive dependence on initial values and parameters to resist various attacks. It makes the chaotic system suitable for application towards image encryption [13].

In our experiment, we use Lorenz chaotic sequences to encrypt an image. Lorenz equation describes atmosphere movement mode using following equation group; solution of the equation group is not stable and discrete as well, but it is attracted around a region and enters a chaos state [14]. The system of Lorenz is a well-known example of chaotic system and is represented by the following nonlinear system, i.e. Eq. (1):

$$\begin{cases} \dfrac{dx}{dt} = -u(x-y) \\ \dfrac{dy}{dt} = -xz + rx - y \\ \dfrac{dz}{dt} = xy - bz \end{cases}, \quad (1)$$

where the standard parameter values and initial conditions for the system are $u = 10$, $r = 28$, $b = 8/3$. Under the conditions of invariable for u and b, and when r is more than 24.74, the system is in a state of chaotic [15].

Combined with Euler method, we can change the above equation into a different equation (Eq. (2)):

$$\begin{cases} x(i+1) = x(i) + h * u * (y(i) - x(i)) \\ y(i+1) = y(i) + h * (-x(i) * z(i) + r * x(i) - y(i)) \\ z(i+1) = z(i) + h * (x(i) * y(i) - b * z(i)) \end{cases}, \quad (2)$$

In this paper, the experiment is to encrypt an image in the camera system. We use Eq. (2) to set our initial values. Three-dimensional Lorenz chaos system parameters are $u = 10$, $r = 28$, $b = 8/3$, $h = 0.001$, $x(0) = 0.6$, $y(0) = 0.4$, $z(0) = 0.6$. Then we will get three Lorenz chaotic sequences $x(i)$, $y(i)$, $z(i)$. Combining with three sequences ($x(i)$, $y(i)$, $z(i)$), intersecting and mixing each other, a new chaos sequence ($P(n)$) is generated ($P(n) = \{x(1), y(1), z(1), x(1), y(1), z(1), \ldots\}$).

For another, compression is used in the most digital image for transmitting and saving. H.264/AVC is one of the latest image coding standards which can save up to 45% of a stream's bit-rate compared with the previous standards [16]. The coding efficiency is mainly the result of two new features: variable block-size MC and quarter-pel (q-pel) interpolation accuracy. Lorenz chaotic encryption will destroy the correlation of the image that image compression ratio will be very low for the H.264 compression. So, we adopt the method compressing the image firstly and encrypting it. In our experiment, we apply exclusive XOR between $P(n)$ and the original data of the image, and then the encrypted data are compressed into H.264. Fig. 2 shows the software mode of the camera system with image encryption.

The procedure to decrypt the image data is just the inverse way. In Fig. 2, arrow from box XOR and box H.264 compression is reversed. Lorenz chaotic sequence $P'(n)$ is generated under the same secret keys as referred above. That is $P'(n)$ is the same with $P(n)$. The encrypted data exclusive XOR the elements in $P'(n)$, then the image data will be reconstructed.

4. Experiment results and analysis

A good encryption system should resist all kinds of known attacks. In order to demonstrate that the camera system with image encryption is secured against most common attacks, detailed security analyses about the proposed image encryption scheme are carried out such as key space analysis, statistic analysis, and sensitivity analysis with respect to the key and original image.

4.1. Key space analysis

Key space is one way of measuring encryption algorithm safety. Due to the sensitivity of x, y and z to control parameters and initial conditions of the system, even though the secret-key has tiny change, it shall result in very different of scrambling index matrix [17,18]. Under actual conditions, the accuracy of the DM6446 chipset is limited. In our experiment, if the initial parameters fluctuate to 0.0000001, the Lorenz sequence will change a lot. So, our key space is $(10^7)^3 = 10^{21}$ possible keys. Comparing with other approaches to encrypt the image, chaotic image encryption has more safety. For another, there are four system parameters in the Lorenz chaotic encryption system. If we take the four system parameters in the Lorenz chaotic encryption system into account, there will be more keys. So our algorithm has a good anti-attack capability.

4.2. Experiment result

In order to give the visual effect of Lorenz chaotic encryption, the following two pictures show the direct effect of encryption. We got an image, and then encrypted and stored the image as "encrypted image". Finally, the encrypted image was decrypted with right and wrong keys separately. All of these steps are finished in the prototype camera based on DM6446. Fig. 3 shows the original data image. The encrypted image is shown in Fig. 4 which is original data image under $u = 10$, $r = 28$, $b = 8/3$, $h = 0.001$, $x(0) = 0.6$, $y(0) = 0.4$, $z(0) = 0.6$. As demonstrations show, wrong and correct decryption results are shown in Figs. 5 and 6. In this case, Fig. 6 shows an example of correct decryption to the image, and Fig. 5 shows an example of wrong decryption under the frame image $u = 10$, $r = 28$, $b = 8/3$, $h = 0.001$, $x(0) = 0.6000001$, $y(0) = 0.4$, $z(0) = 0.6$ as secret keys. The

Please cite this article in press as: J. Li, et al., Digital camera with image encryption, Optik - Int. J. Light Electron Opt. (2015), http://dx.doi.org/10.1016/j.ijleo.2015.10.211