Optik 125 (2014) 6530–6534

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

An analysis of chaos-based security solution for fingerprint data

Moting Su [a,*], Wenying Wen [b]

[a] School of Economics & Business Administration, Chongqing University, Chongqing 400044, PR China
[b] School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330013, PR China

ARTICLE INFO

Article history:
Received 15 November 2013
Accepted 19 June 2014

Keywords:
Validity
Reversible hidden transform (RHT)
Reversibility

ABSTRACT

Recently, an engineering report on chaos-based security solution has been proposed for fingerprint data during communication and transmission (IEEE Trans. Instrum. Meas. 61 (April (4)) (2012) 876–887). It has been claimed that experimental results and security analysis demonstrate the efficiency of the security solution in this report. However, from a scientific perspective, we give a validity analysis. Firstly, we demonstrate that the reversibility of integer reversible hidden transform (RHT) cannot be guaranteed under the current constraint condition in the original paper and then counterexamples are given to verify demonstration. In addition, in its experiment and performance analysis parts, there also exist several problems. Finally, we put forward some suggestive remarks on the designing of security solution for fingerprint data.

1. Introduction

Optical transform and chaotic map have become two vital roles in protecting digital images in recent years, since the transmission of images over various communication networks has developed greatly. Optical transform possesses the strengths of high speed, parallel processing and large storage memories while chaotic map has the properties of ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters. Both are used to design numerous image encryption schemes like [1–7] and [8–15], respectively. Obviously, it is possible for the combination of optical transform and chaotic map to integrate their advantages and make up for their respective defects for constructing new-style image encryption schemes [16–21], which is superior to single encryption schemes.

Biometrics has been attracting increasing interest in contemporary society due to the identifiers and permanent characteristics of the individuals, which has applications in physical and logical access controls, attendance recording, payment systems, crime and fraud prevention/detection, border security controls and online signature [22–25]. Some techniques of the biometrics used for authentication are fingerprint, iris, palm print etc. Among all the biometric techniques, fingerprints are the oldest and most widely used biometric features for personal identification because of their high acceptability, immutability and individuality [26,27]. Fingerprint itself can be used to design the biometric cryptosystems [28,29]. Recently, there have been some works that attempted to protect fingerprint image by utilization of chaos maps [30–33] and combinations of optical transform and chaotic map [34–36]. Han et al. [30] proposed a fingerprint image encryption approach based on a two-dimensional (2D) chaotic sequence yielded by multi-scroll chaotic attractors, where the private key is provided by the initial values of the chaotic attractors generated from the pixel distribution of the binary images of the captured fingerprints. Zhao et al. [31] combined shuttle operation and nonlinear dynamic chaos system to construct a secure and efficient fingerprint image encryption scheme. Khan et al. [32] stated challenge/response-based chaotic biometrics image encryption scheme that rectifies the liveness and retransmission issues of biometrics image transmission over the insecure communication channel. Liu [33] designed a classic cryptographic structure of scrambling and confusion for fingerprint image encryption. Cui [34] incorporated chaotic systems into fractional Fourier transform to achieve fingerprint protection. Bhatnagar et al. [35] described a novel fingerprint encryption technique via nonlinear chaos and principal component analysis in fractional dual-tree complex wavelet domain. Bhatnagar et al. [36] further presented a security solution for fingerprint data during communication and transmission based on reversible hidden transform (RHT), piece-wise linear chaotic map (PWLCM), singular value decomposition (SVD) and fractional wavelet packet transform (FrWPT). The core idea of this solution is to modify the gray values in the spatial domain using RHT followed by the deformation of FrWPT coefficients by SVD and PWLCM. The authors have made a good contribution with theoretical and experimental

* Corresponding author.
E-mail address: motingsu@sina.com (M. Su).

http://dx.doi.org/10.1016/j.ijleo.2014.08.026
0030-4026/

study of fingerprint protection. It has been claimed that experimental results and security analysis demonstrate the efficiency of the security solution in [36]. However, we give a verification and validation analysis from a scientific perspective and find that there are some neglects regarding RHT, experiment and performance analysis. Contributions of our paper include:

(1) Non-invertibility of integer RHT is demonstrated and then counterexamples are given.
(2) Several problems about the experiment and performance analysis are discovered.
(3) Some suggestions are indicated in terms of the designing of security solution for fingerprint data.

This paper is organized as follows. The original solution is briefly introduced in Section 2. Validity analysis of the solution is illustrated in Section 3. Finally, some suggestive remarks are given in Section 4.

2. Overview of the original solution

The security solution for fingerprint image primarily leverages four techniques including FrWPT, SVD, PWLCM and RHT, which were introduced in the original solution in detail, respectively. In this section, to better understand the encryption process, we briefly re-describe it as follows:

(1) RHT. Perform (α, β)-RHT on the original fingerprint image F.
(2) PWLCM-based FrWPT. Iterate PWLCM with initial values *key*1 and *key*2 to generate two final values K_1 and K_2, after τ_1 and τ_2 times, respectively. Then, perform n-level (K_1, K_2) order FrWPT on F, denoted by f_n^θ, where $\theta \in \{A, H, V, D\}$.
(3) PWLCM-based SVD. Iterate PWLCM with initial value *key*3 to generate a chaotic sequence K_3 of length $\tau_3 = m \times n$, where m and n are the dimensions of f_n^θ. Map K_3 into an integer sequence $\tilde{K}_3$ such that every element lies in [0, 255] and then arrange it into a matrix denoted by P of size $m \times n$. Finally, perform SVD on P, i.e., $P = U_P S_P V_P^T$, and deform all coefficients of each subband using orthonormal matrices U_P and V_P, i.e., if $m \le n$, $f_n^{\theta,def} = U_P f_n^\theta V_P^T$, otherwise, $f_n^{\theta,def} = V_P f_n^\theta U_P^T$.
(4) PWLCM-based FrWPT. Perform inverse n-level (K_1, K_2) order FrWPT to get the encrypted fingerprint image $\tilde{F}$.

With respect to the detailed encryption process and decryption process, please refer to Ref. [36].

3. Validity analysis

The security solution for fingerprint image under study has a serious problem about decryption. It should be noted that a cryptosystem is well defined only if the encryption function is completely invertible, which means that a legal receiver can determine the plaintext if he or she only possesses the ciphertext and the decryption key. In this section, the non-invertibility of integer RHT is demonstrated and then counterexamples are given to verify the irreversibility. Finally, several problems about the experiment and performance analysis are illustrated.

3.1. Irreversibility of integer RHT

In [36], RHT is defined as:
Forward transform:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha x_1 + \beta x_2 \\ \beta x_1 + \alpha x_2 \end{pmatrix}. \tag{1}$$

Inverse transform:

$$\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} \dfrac{\alpha y_1 - \beta y_2}{\alpha^2 - \beta^2} \\ \dfrac{\beta y_1 + \alpha y_2}{\beta^2 - \alpha^2} \end{pmatrix}. \tag{2}$$

where $\alpha + \beta = 1, 0 \le \alpha, \beta \le 1$. (y_1, y_2) is the transformed pair of pixels and $(\tilde{x}_1, \tilde{x}_2)$ is the reconstructed pair of pixels. If it is possible for the pair of pixels to be reconstructed, we deduce that the second part of Eq. (2) is wrong and the corresponding corrective form is described as

$$\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} \dfrac{\alpha y_1 - \beta y_2}{\alpha^2 - \beta^2} \\ \dfrac{\beta y_1 - \alpha y_2}{\beta^2 - \alpha^2} \end{pmatrix}. \tag{3}$$

Due to $\alpha^2 - \beta^2 = (\alpha + \beta)(\alpha - \beta) = \alpha - \beta$, Eq. (3) can be re-written as

$$\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} \dfrac{\alpha y_1 - \beta y_2}{\alpha - \beta} \\ \dfrac{\beta y_1 - \alpha y_2}{\beta - \alpha} \end{pmatrix}. \tag{4}$$

In order to avoid a fractional part of the transformed pair of pixels in some cases, the authors employed floor function and ceiling function, which are taken on the forward transformed value and the inverse transformed value, respectively. Therefore, the final form of RHT is given by:
Forward transform:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \alpha x_1 + \beta x_2 \\ \beta x_1 + \alpha x_2 \end{bmatrix}. \tag{5}$$

Inverse transform:

$$\begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} \dfrac{\alpha y_1 - \beta y_2}{\alpha - \beta} \\ \dfrac{\beta y_1 - \alpha y_2}{\beta - \alpha} \end{bmatrix}. \tag{6}$$

However, the above form of integer RHT is irreversible. Here is the proof.

Proof. Assume that the fractional part of the first equation in (5) is $\delta (0 \le \delta < 1)$; then the fractional part associated with the second equation in (5) is $1 - \delta$ because

$\alpha x_1 + \beta x_2 + \beta x_1 + \alpha x_2 = (\alpha + \beta)x_1 + (\alpha + \beta)x_2 = x_1 + x_2$ and $x_1 + x_2$ is an integer.

Accordingly,

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{pmatrix} \alpha x_1 + \beta x_2 - \delta \\ \beta x_1 + \alpha x_2 - (1 - \delta) \end{pmatrix}. \tag{7}$$

Substitute (7) into (6) and obtain

$$\begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} = \begin{bmatrix} x_1 + \dfrac{\beta - \delta}{\alpha - \beta} \\ x_2 + \dfrac{\alpha - \delta}{\beta - \alpha} \end{bmatrix}. \tag{8}$$

Since the conditions including $-1 < (\beta - \delta)/(\alpha - \beta) \le 0$ and $-1 < (\alpha - \delta)/(\beta - \alpha) \le 0$ are not always true, the reversibility of the integer RHT cannot be guaranteed. In other words, only when $-1 < (\beta - \delta)/(\alpha - \beta) \le 0$ and $-1 < (\alpha - \delta)/(\beta - \alpha) \le 0$, i.e., $\min(\alpha, \beta) \le \delta \le \max(\alpha, \beta)$, does the reversibility hold. It should be noticed that Eq. (6) in the case of $\alpha = \beta = 1/2$ is meaningless. □