Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW CARD AUTHENTICATION SCHEMA BASED ON EMBED FINGERPRINT IN IMAGE WATERMARKING AND ENCRYPTION

MARWA KAREEM RASHEED[1], ALI J. DAWOOD[2]
Department of Computer Science, College of Computer Science and Information Technology, University of Anbar
E-mail: [1]mrkr25@gmail.com , [2]dralijd@yahoo.com

ABSTRACT

The wide use of the smart card makes the security issue more and more important. Authentication by using traditional password can't meet user requirements. Many schemes for user's authentication have been proposed, especially, those based on image encryption. However, most of the existing schemes complain of many problems like single authentication mode, weak quality of the restored image and low encryption intensity. The authentication scheme is a cryptographic mechanism, which helps two communication parties in the network environment to authenticate each other. In this paper dual authentication scheme based in image watermarking and encryption was proposed. Watermarking techniques have been used to enhance the fingerprint-based authentication process where the fingerprint feature are extracted and embedded in the user face image which act as watermark, in addition to use the user name as second watermark in order to protect the user's data from the illegal use. To increase the security level of the proposed scheme we encrypt the two watermarks before embedding it by using the Rivest Cipher 4 (RC4) encryption algorithm, in order to integrate the advantages of watermarking and encryption into a single system. The obtained result shows more robust authentication scheme to authorized the user to access the system with a high quality watermarked image, the PSNR value's range between 83.57 dB and 92.05 dB.

Keywords: *Authentication · Smart card · Fingerprint Minutiae · Digital watermarking · RC4 encryption.*

1. INTRODUCTION

For a long time, personal authentication issue has received more attention in people's daily lives, law enforcement, and business. The purpose of personal authentication is to confirm or determine the identity claims by individuals. Besides its applications has been widely used in building access, automatic systems, computers and mobile phones [1]. Personal authentication serves both verification and identification, each has a specific application. the verification mode, based on one-to-one comparison to check whether a person's identity is as requested; whereas, the identification mode, based on one-to-many comparisons in order to distinguish the person's identity. Traditionally, the personal authentication process is based on what you hold (e.g. keys and ID cards) or what you know (e.g. passwords). Approaches like this have several drawbacks. First, the user can lose or forgotten has knowledge and tokens. Second, the perpetrator can plead that the ID card or his password was stolen and deny their wrongdoing. Third, there is 'spoofing' attack risk, so that any person who has the key can access all services. Further, the people are more and more mobile and electronically connected, this led to the detection of new methods used to identify the individuals remotely where the traditional identification methods cannot be trusted [2].

The personal authentication approaches based on Biometric have been proposed to solve these problems [3][4][5]. the description of the Biometrics is the person features that is constant and (ideally) not forgotten, lost, or changeable. which make them a more effective and useful authentication technique than traditional one [6]. Among different biometric types, the fingerprints are the most widely used [7]. A fingerprint is represented by the pattern of ridges and valleys on the fingertip surface. The fingerprint uniqueness is determined by the integration of the ridges, valleys pattern and the minutiae points [8]. The watermarking technique used to embed a name, logo or information of individual copyright into the host digital data who can be text information, digital image, audio, and video [9]. There are some limitations on the use of these types of watermarks such as lower important information and lower related to an individual copyright for authentication.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

whereas these types of watermarks can be found easily, easy to reproduced and tamper. Recently, the researchers have been using individuals biometric features in watermarking technique in order to improve the copyright authentication process and provide protection to the conventional watermarking.

The encryption process precedes the digital watermarking process in order to give an extra layer of security. The biometric features are encrypted by using the RC4 encryption algorithm before embedding as a watermark in the image. This ensures that the biometric features cannot be interpreted or used even if is removed. Though combined encryption with watermarking is uncommon, implementing it in a correct way proves that it is an effective technique.

2. RELATED WORK

In the fingerprint authentication systems, the Minutia is extracted from binary images and used as a feature to verify the legitimacy of the user. (Xinxin Peng1 et.al) [11], they proposed a dual authentication scheme based on using digital watermarking techniques and fingerprint biometric modality. In this scheme, they hide the collected user's fingerprint image in the user's image data. After that, they applied the Discrete Cosine Transform DCT and the compression technology to the image encryption process. The results display that the scheme can resist the simulated attacks, and have low storage cost. However, we can see that the proposed scheme is robust somewhat and the Image quality is not good enough.

(Sani M. Abdullahi et.al) [12], the proposed scheme using 8-layers features enhancement algorithm in order to enhance the fingerprint image before using it. They use a semi-fragile watermarking technique to hide the fingerprint biometric data after enhanced into audio signals. It provides a secure system.

(Wioletta Wojtowicz et.al) [13], proposed a new authentication scheme that protects the ownership of digital images based on use biometric watermarking approach. They try to integrating fingerprint and iris biometric images and create the biometric watermarks to embedding it in the cover image. The proposed algorithm submitting Independent Component Analysis (ICA) to the biometric watermarking field. In this method, the standard ICA approach used in order to make the embedding of two watermarks possible. The proposed method enables authenticating images, the quality of the resulted image can consider good.

(Mita Paunwala et.al) [14], the proposed biometric watermarking algorithm it aims to protection the biometric template. where they use two watermarks, the fingerprint features vector and iris features to embed in the cover image. Which transformed using DCT-based watermarking technique for embed watermarks in low-frequency Alternating Current (AC) coefficients of the selected 8 × 8 DCT blocks. The results show that the proposed algorithm is robust against several signal processing and channel attacks. Hence, the performance of the biometric system does not damage even adopting template protection scheme.

(Malay Kishore Dutta et.al) [15], they propose a possible solution to the digital right management through generating a digital watermark from biometric features. Biometric-based watermarks have been done by using a Discrete Cosine Transform (DCT) based on image watermarking. The pattern of fingerprint biometric is used to generate the digital watermark and embedding it in the image by using DCT transform this technique used the middle-band DCT coefficients to encode a single bit into a DCT block. The results obtained for perceptual transparency and robustness against signal processing are encouraging.

(Mohammed et.al) [16], proposed new fingerprint image watermarking approach using Dual-Tree Complex Wavelet Transform (DTCWT). This method expatiates further on the effect of the watermarking on fingerprint biometric features after the watermarks embedding process. where decompose Both the fingerprint and watermark images into real and imaginary parts. So this might lead to a major drawback on the system with the trade-offs issue between the robustness and security of the system even though the template was retrieved successfully without corrupting the minutiae.

3. PROPOSED METHOD

The general structure of the proposed authentication scheme is shown in Figure 1. We proposed a dual authentication scheme based on image watermarking and encryption. The proposed system has two phases, registration phases and authentication (matching) phase. In the registration phases, the fingerprint features are extracted after enhanced the fingerprint image, the performance of a fingerprint features extraction and matching algorithm depends heavily upon the quality of the input fingerprint image. Several reasons may lie degrade the quality of the fingerprint image.

Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Therefore, enhancement step are used for fingerprint image before extract it features. After extract, the fingerprint features it will encrypted by using the RC4 algorithm, in addition to the user name (second watermark). The two encrypted watermarks embedded in the host user image by using the DWT watermarking technique. Finally, the watermarked image stored in the database.

At authentication phases the fingerprint feature will be extracted from the user image by applying the watermark extraction process and decrypt the extracted watermark before execute the proposed matching algorithm between the extracted watermark (fingerprint feature) and the feature collected from the capture fingerprint of the user who want to ensure of his authorized.

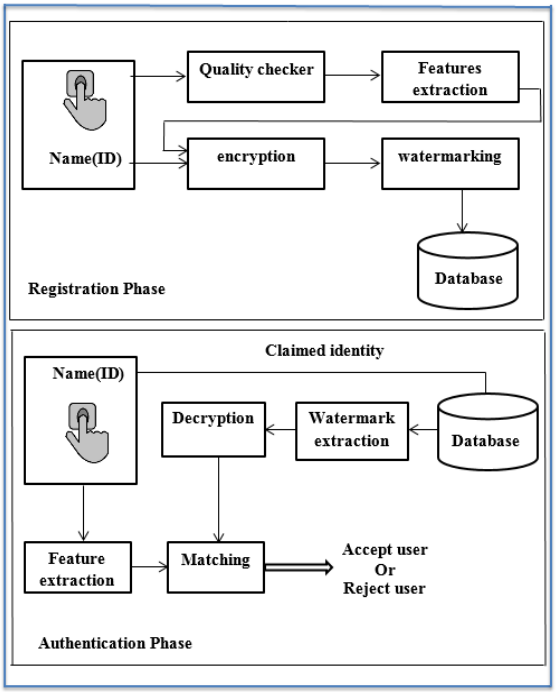

Figure 1. General Structure of the Proposed Authentication Scheme.

3.1. Dataset

The dataset has been used in this study are consist of user face image of 100 person and their fingerprint image, two printing per user. The fingerprint image used is from the FVC 2004 set A.

3.2. Registration Phase

The responsibility of the enrollment module is to registering individuals in the system database (system DB). During the registration phase, the quality of the acquired fingerprint is checked. The checking of fingerprints quality is generally performed in order to ensure that the acquired fingerprint can be reliably processed during the successive stages. Thus facilitating the matching process. Figure 2 shows the steps of the registration phase of the proposed scheme, which is divided into the following steps:

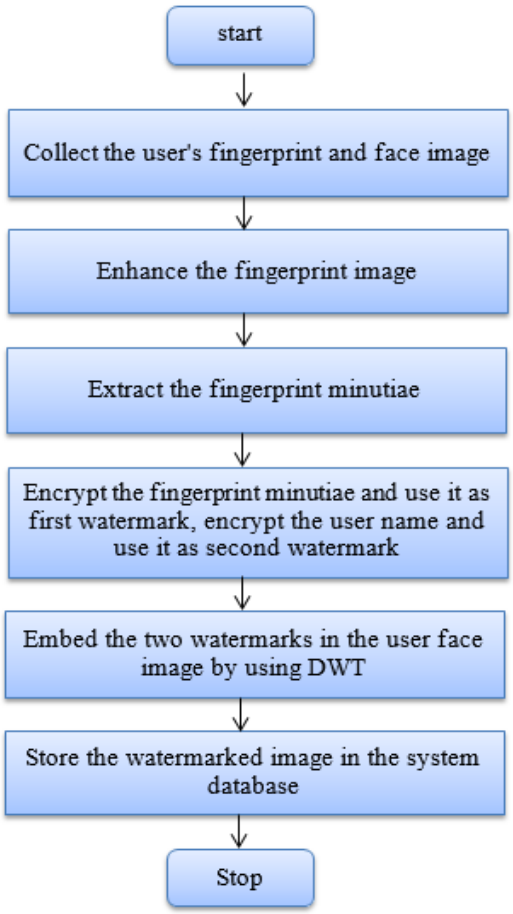

Figure 2. Flowchart of the Registration Phase of the Proposed scheme.

3.2.1 Enhancement of the Fingerprint Image

Enhance the fingerprint image by using Short Time Fourier Transform STFT analysis process similar to that mentioned in [18]. The performance of a fingerprint feature extraction and matching algorithm implementation depends critically on the quality of the input fingerprint images. While the quality measure of a fingerprint image may not be objective, it almost corresponds to the visibility of the ridge structure in the fingerprint image, thus it is necessary to enhance a fingerprint image. Figure 3 show the image before and after the enhancement.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

a)

b)

Figure 3. a) Fingerprint image 2_1 from DB, b) Enhanced version of fingerprint image 2_1.

3.2.2. Binarization

Image binarization is the process of convert a grayscale image into a black and white image. The pixels value In a gray-scale image extends within the range [0,255]. While each pixel in binary images is allocated to be either black or white. The conversion process from gray-scale to binary is performed by applying thresholding the gray image. in applying a threshold to an image, the pixels values compared to a predefined threshold value. Where all pixel value lower than the threshold is set to zero else it set to one. In the end, all pixel's values become either zero or one, and consequently, a binary image is produced. Figure 4 show the image binarization process.

Figure 4. Binarization result of enhanced fingerprint image

3.2.3. Thinning

After binarization, another major pre-processing technique applied on the image is thinning, in the ridge thinning the redundant pixels of ridges is eliminate until the ridges become just one pixel wide. An iterative, parallel thinning algorithm use. In each scan of the fingerprint image, the algorithm will marks down redundant pixels in every small image window (3x3). After several scans, all those marked pixels are removed. Then the thinned ridge map is filtered by using other Morphological operations in order to remove some H breaks, spikes, and isolated points. In this step, any single points in a ridge are eliminated and considered noise processing. Figure 5 shows the result of the thinning process.

Figure 5. Thinning Process Result.

3.2.4 Get Core Point of the Enhanced Fingerprint

The first step in the actually minutiae extraction process is to get a core point of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

fingerprint. The idea of determining the core point is taken from [19] , which is described as follows:

The definition of core point is "the point of the maximum curvature on the convex ridge [20]" which is generally located in the central of the fingerprint area. The reliable detection of the core point location can be accomplished through the maximum curvature detecting using complex filtering methods.

The complex filters are applied to the ridge orientation image which generated from the original fingerprint image. The reliable detection of the core point with the complex filtering methods summarized as below:

Firstly, For each overlapping block in fingerprint image; generate a ridge orientation image with the same method in STFT analysis. Now using the result orientation image and apply the corresponding complex filter equation 1.

$$h = (x + iy)^m \, g(x, y) \quad (1)$$

centered at the pixel orientation in orientation image, where m is the order of the complex filter and g(x, y) is the Gaussian window equation 2;

$$g(x,y) = \exp\left\{-\left(\frac{x^2 + y^2}{2\sigma^2}\right)\right\} \quad (2)$$

when m =1, the filter response can be obtained by a convolution, $h * o(x,y) = g(y) * ((xg(x))^t * o(x,y)) + ig(x)^t * ((yg(y) * o(x,y)))$

Where O (x, y) is the pixel orientation image. Finally, the filtered blocks composed to reconstruct the filtered image.

In the filtered image the maximum response of the complex filter can be considered as the core point. Since there is only one output, this output point is taken as the (core point).

3.2.5. Minutiae Extraction

Once the binary image has been obtained, a simple scan of fingerprint image allows to discover the pixels corresponding to minutiae. The minutiae (ridge endings and bifurcations) are extracted by using a 3x3 window scanning of each ridge pixel in the image. The Crossing Number CN value of a pixel p is then calculated, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood of p:

$$cn(p) = 1/2 \sum_{i=1}^{8} |p_{imod8} - p_{i-1}| \quad (3)$$

where p1, p2, ...p8 are the ordered sequence pixels defining the eight neighborhood pixels of p, and val (p) ∈ {0, 1} is the pixel value. It is simple to note Figure 6 that a pixel p with val (p) = 1:

Using the properties of the CN, the ridge pixel can then be classified as a ridge ending, bifurcation.

- When cn(p) = 1 its mean a ridge ending minutia.
- When cn(p) = 2 is an intermediate ridge point.
- When cn(p) = 3 its mean a bifurcation minutia.
- When cn(p) >= 3 defines a more complex minutia (e.g., crossover).

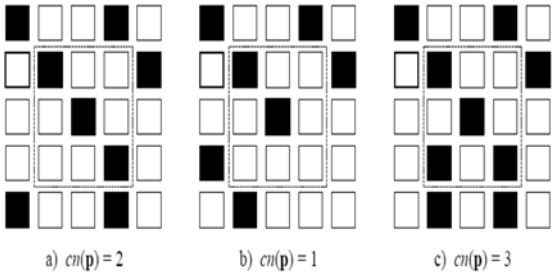

Figure 6. a) Intra-Ridge Pixel; b) Ridge Ending Minutia; c) Bifurcation Minutia.

Hence, for each fingerprint minutia we have three information: x and y coordinates of the minutiae location, and type of the minutia (type1 if it is a ridge end (termination), type2 if it is a bifurcation). The result of this minutiae extraction stage is shown in Figure 7 where the termination minutiae represented by circles, the bifurcation minutiae represent by diamonds, and the core point of the fingerprint by an asterisk.

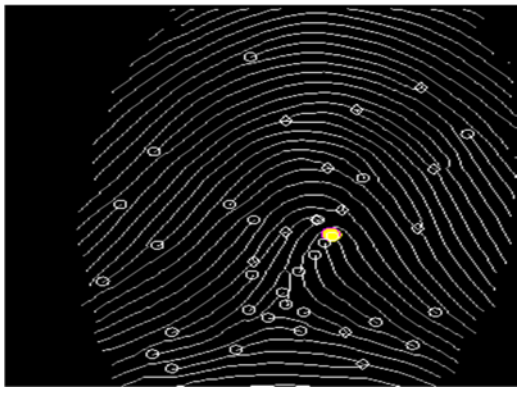

Figure 7. Core Point (Asterisk), Terminations (Circles) and Bifurcations (Diamonds).

3.2.6. Construct The Minutiae Array

The proposed system using array of minutiae contain just the number of minutiae of type1 or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

type2 in each constructed track around the core point of the fingerprint. This method gives better results to the system because using smaller size minutiae as watermark gives better results in terms of storage and non-distortion of the image.
After get all minutiae locations with their types, calculate the distances between all the extracted minutiae and the core point of the fingerprint, By using Euclidean distances: the Euclidean distance between the core and that minutiae as equation 4:

$$\sqrt{(x-x_c)^2+(y-y_c)^2} \quad (4)$$

Where the core point located at (xc, yc) and a minutia located at (x, y). Now, construct tracks with wide of 10*n pixels (where n=1…max_distance /10) until all minutiae are spent, the center of that tracks is the core point, the width of track is chosen to be 10 depending on the average distance (in pixels) between two successive ridges is 10 pixels.

Now, construct the minutiae array, this array contains pairs of an element, the number of pairs equal to the number of constructed track around the core point of the fingerprint. Record the minutiae information of the first track in the first pair of the array, where the number of minutiae of type1 found in the first track represents the first element in the pair and number of minutiae of type2 as the second element. Repeat the recording process for the remaining tracks until all tracks of the fingerprint are processed. An example of minutiae array of fingerprint 2-1 from FVC2004 DB1 is:

Minuarray={{1,0},{1,1},{1,2},{0,0},{1,1},{2,3},{2,1},{1,1},{3,2},{1,1},{2,1},{3,2},{1,0},{1,1},{1,2},{0,1},{0,0},{1,0},{1,0},{0,0},{0,0},{1,0},{1,4},{0,1}}

3.2.7. Encryption with RC4

To encrypt the minutiae data it's converted into a bit stream and encrypted by using RC4 algorithm. The concept of RC4 is to permute the elements by swapping them to achieve the higher randomness. RC4 algorithm enjoys different lengths of key which are between (0-255) bytes to start the 256 bytes in the first state array (State [0] to State [255]) [17]. The steps of encryption by RC4:

1. Get the minutiae data after convert it to stream of bit and secret key to use them for encryption.
2. Create two arrays.
3. Fill the first array with the numbers from 0 to 255.
4. Put the selected key in the other array.
5. The first array is permutation based on the second array (key array).
6. First array is permutation through itself in order to produce the final key.
7. Now, The last key stream is XOR-ed with the stream of bit of minutiae data to get the encrypted first watermark.

The same steps is followed to encrypted the (user name) and get the second encrypted watermark.

3.2.8. Host Color Image Composition Stage

The host color image that contains three-color components is decomposed into its components before using it to embed the watermarks. After separate the three-color components into three isolated color channels (Red, Green, Blue) we will use the blue channel components for watermark embedding and extraction process. Because, "the sensors in the human eye are called as cones which are responsible for color vision. The cones could be separated into three major sensing categories as red, green and blue. Nearly 65% of the cones are sensitive to red color, 33% are sensitive to green color and just 2% are sensitive to blue color [21]".

3.2.9. The Proposed Watermarking Method

The digital watermark technique used to hidden the two encrypted watermarks (fingerprint minutiae and user name) in the user face image to verify identifications and protect the personal data from loss. There are many digital watermarking schemas are developed in this way. In general, due to several advantages of the transform domain, Discrete Wavelet Transform (DWT) has been used to produce watermarked image with the best visual quality. In the scheme we use 4 level Discrete Wavelet Transform to hidden the two watermarks.

The four level DWT synthesis can be illustrated by figure 8. The 2D-DWT two dimensional DWT) of an image yields LL, HL, LH and HH coefficients, these are the first level DWT coefficients. To calculate the second level DWT coefficients, the LL coefficients of the first level is used as the input. The second level DWT coefficients obtained are LL2, HL2, LH2 and HH2. For the third level DWT the LL2 is used as input to obtained the coefficients LL3, HL3, LH3 and HH3.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Finally, the LL3 is used to calculate the fourth level coefficients LL4, HL4, LH4 and HH4.

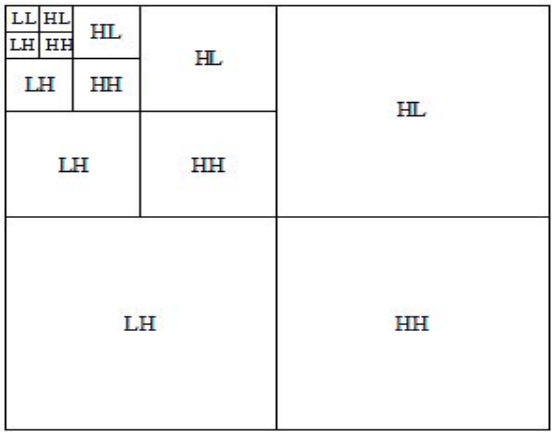

Figure 8. : Four Level DWT Decomposition.

The host image in the proposed method will be the face of the user, while the two watermark will be the minutiae array of the fingerprint and the user name. The 4– level DWT watermarking process consists of two stages, embedding and extraction as described below.

3.2.9.1 Watermarking Embedding

First The original color digital image (user face image) is decomposed into three color components of O(Red), O(Green) and O(Blue) respectively, resulting in three color components we use the blue components to embed the watermark, Due to lower sensitivity of human eyes to blue light, it is recommended to embed watermark in blue component.

Determine the host image pixels to start embedding the watermark by using the key (K), To avoid embedding in the white background of personal user's image, we selected the key by testing all the personal user images in the dataset and found that the selected positions are occupied by the person's body at all time with result of 100%.

Now, the watermark bit of the first watermark (fingerprint minutiae) is multiplied by a factor (α) and then multiplied it by the level - 4 host image approximate coefficients (LL4) to form the new level - 4 coefficients (LL4) of the host image. The process is as in equation (5).

$$LL4new = LL4 * (1 + 0.001 * W1) \quad (5)$$

After finishing the first watermark, embedding the second watermark (user name) by using the same process of embed the first watermark in equation (5).

The watermarked host image is reconstructed using the same Haar wavelet filters and inverse DWT (IDWT) of the new level - 4 coefficients (LL4) and level - 3 LL coefficients (LL3), level - 2 LL coefficients (LL2), and level - 1 LL coefficients (LL) as follows:

- The new LL3 coefficients are calculated by IDWT of new level - 4 coefficients and HL4, LH4, HH4 as in equation (6).

  L3new = IDWT (LL4new, HL4, LH4, HH4) (6)

- The new LL2 coefficients are calculated by IDWT of new level - 3 coefficients calculated in the previous step and HL3, LH3, HH3 as in equation (7).

  LL2new = IDWT (LL3new, HL3, LH3, HH3) (7)

- The new LL coefficients are calculated by IDWT of new level - 2 coefficients calculated in the previous step and HL2, LH2, HH2 as in equation (8).

  LLnew = IDWT (LL2new, HL2, LH2, HH2) (8)

- The watermarked shared image is reconstructed by IDWT of new level - 1 LL coefficients calculated in the previous step and HL, LH, HH as in equation (9).

  Watermarked image = IDWT (LLnew, HL, LH, HH) (9)

Finally, reconstruct the colored image by integrate the component of the colored host image and construct the watermarked image.

3.3. Authentication Phase

For authenticate the user, verification phase should be applied on the user's fingerprint. Figure 9 shows the steps of the verification phase of the proposed matching algorithm, which is divided into the following steps:

1. Capture the fingerprint of the user to be verified.
2. Apply the steps of enhancement and feature extraction on the fingerprint under test to obtain its minutiae array.
3. Extract the watermarks to get the corresponding minutiae array.
4. Apply the matching algorithm between that extracted minutiae and the minutiae of the

corresponding claimed fingerprint, and then accept user or reject him.

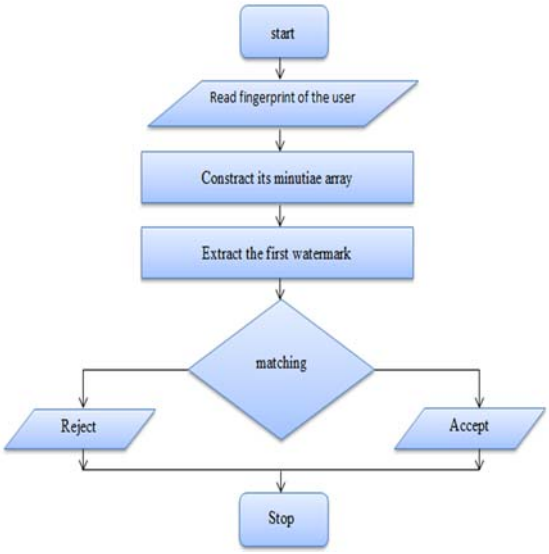

Figure 9. The Steps of the Authentication Phase.

3.3.1. Watermarks Extraction

Now, get the corresponding minutiae array by extract the watermark from the user face image. First, The watermarked color image is decomposed into three color components of O(Red), O(Green) and O(Blue) respectively, resulting in three color components we select the blue components that has been imbedded the watermarks inside and transformed it to four level 2D-DWT and LL4 is chosen.

determine the watermark location by using the same key (K) used in the imbedding stage, and start extracting the first watermark by using the equation (10).

W1 =(LL4-LL4new)/(0.001 * LL4new) (10)

After finishing the extract of the first watermark (encrypted minutiae), extract the second watermark (encrypted user name) by using the same process of extracting the first watermark in equation (10).

3.3.2 Decryption using RC4

The result of the watermark extraction is encrypted watermark (minutiae data). To decrypt the minutiae data, the same secret key as during the encryption phase is used. Then XOR keystream with the extracted encrypted first watermark to generate the original first watermark (minutiae array). In addition, XOR keystream with the extracted encrypted second watermark to generate the original second watermark (user name).

Logic is simple (A xor B) xor B = A

3.3.3. The proposed matching algorithm

After extract and decrypt the watermarks we obtained the minutiae array from the first watermark. Appling the proposed matching algorithm between the extracted minutiae array and another one that calculated from the claimed fingerprint, the first step in the matching algorithm is to calculate the absolute differences between that extracted minutiae array and its noise version on the assumption that the minutiae may have been get some noise, and between that extracted minutiae array and the minutia array of the corresponding claimed fingerprint now we have two absolute differences.

Because the sizes of minutiae array (number of pairs) are not equal, so the minimum size of the tracks (number of pairs) must be determined in order to able to perform the absolute differences on the same size for different array. The minimum number of tracks found by experiment is 14. So, just the first 14 pairs (tracks) in each minutiae array will be considered in the calculation of the absolute differences, and then calculate the summation of the absolute differences of each type for the two absolute difference array.

The second step is to get the geometric mean (g1) of the summation of the type1 and the geometric mean (g2) of the summations of the type2.

The geometric mean, in mathematics, is an average or type of mean, which specifies the typical value or central tendency of a set of numbers. It is similar to the arithmetic mean, except that the numbers will be multiplied and then the nth root (where n is the count of numbers in the set) of the resulting output is taken.

$$g1 = \sqrt[2]{S11 * S12} \quad (11)$$

$$g2 = \sqrt[2]{S21 * S22} \quad (12)$$

Where S11 is the absolute difference summation of the type1 in the first absolute difference array, and S12 is the absolute difference summation of the type1 in the second absolute difference array. The S21, S22 is the absolute difference summation of the type2 in the first absolute difference array, and the absolute difference summation of the type2 in the second absolute difference array respectively.

Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then check the values of g1 and g2 with the threshold value:

If g1 <= threshold1 and g2 <= threshold2 then the user is authentic and accept him

Else The user is fraud and reject him

The threshold values obtained through experiments on the database used and which give desired results are the threshold1=16, and threshold2=12.

4. RESULTS

The results of the proposed system is calculated for two parts: the performance of a watermarking method and the performance of the biometric authentication system. The evaluation metrics are different for each part. The implemented results of the two parts are presented in terms of running time and errors.

Some evaluating metrics are required to compute in order to determine the quality of the proposed digital watermarking techniques, which compares the watermarked face image with the original one. such as Mean-Squared Error (MSE) equation 13, the Peak Signal-to-Noise Ratio (PSNR) equation 14, the Structural Similarity Index Measure (SSIM) equation 15, and the Normalized Correlation (NC) equation 16 are presented to determine the quality of the watermarking method.

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I^{*}(i,j)]^2 \quad (13)$$

where M and N are the size of the image. I (i, j) is the value of the pixel located at (i ,j) position in the original image and I*(i ,j) is the corresponding pixel in the watermarked image

$$PSNR = 10 * \log 10 \left[\frac{MAX^2}{\text{MSE}}\right] \quad (14)$$

Where MAX is the maximum pixel value of the image, MSE is the Mean Square Error between the original image and the watermarked image.

The PSNR values are measured in decibel scale (dB). the human eye cannot able to distinguish images with PSNR values above 40 dB from the original image. $SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}$ (15)

where μ, σ^2, σ_{xy} are mean, variance, and covariance of the images and c1, c2 are the stabilizing constants . SSIM is a better comparison measure than PSNR of an image because it tells us how a human eye sense changes in an image.

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,j) * I1(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)]^2} \quad (16)$$

where M, N are the size of the image, I and I1 denote the original image and watermarked image, respectively.

Table 1 show the result of this evaluating metrics which calculated to the host image (face images) of 5 persons before adding watermark and after adding watermark. The PSNR value's calculated between the watermarked image and the original image is range between 83.57 dB and 92.05 dB. High PSNR values indicate that the quality of the host image is not perceivably distorted and difficult to distinguish the difference between the original image and the watermarked image by the human eye. Also, the MSE, NC and SSIM values between the original and watermarked image are display. This result indicate that the distortion caused by the embedding of watermarks in image is invisible in all tested images. Moreover, the similarity between the original watermark and the extracted watermark for the two watermarks is equal to 100% for all tested image.

Table 1. The Results of Applying Watermarking

Image	PSNR	MSE	SSIM between original and watermarked image	NC of the original and watermarked image
Image 1	83.5732	4.1476e-09	1	1
Image 2	92.0563	3.1302e-10	1	1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Image 3	89.5327	1.0961e-09	1	1
Image 4	83.7252	4.2411e-09	1	1
Image 5	85.1106	2.0747e-09	1	1

The different of the two types of error (mean square error (MSE) and Peak Signal to Noise Ratio (PSNR)) have been computed between the three color channel. Figure 10 shows the different of the PSNR for the red green blue channels where the blue channel have the higher PSNR value than the other two channel. Figure 11 show the different of the MSE values between this three channel where the blue channel have the best MSE value.

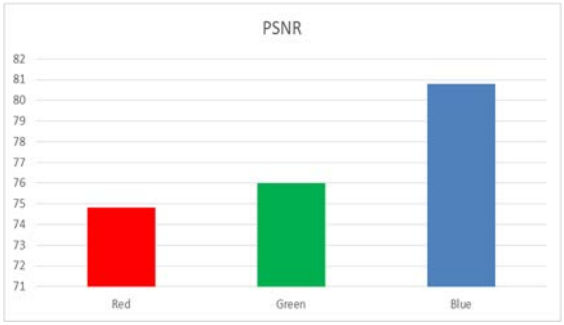

Figure 10. The PSNG Values of the Three Color Channel.

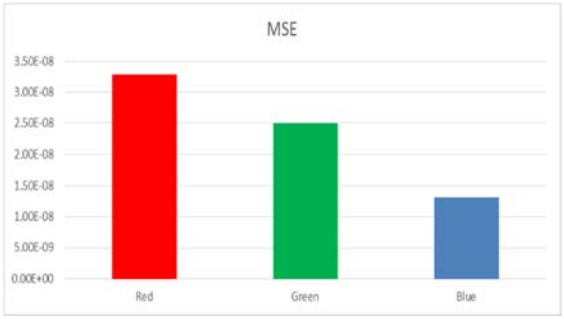

Figure 11. The MSE Values of the Three Color Channel.

The times of watermarking and De-watermarking implementation stage are display in table 2 which calculated for 5 persons. As we show the time of the embedding the two watermark is calculated along with the time it takes to encrypt this watermarks. likewise, the time taken to extract the two watermarks is calculated with the time needed to decrypt the watermarks. The result show that the our scheme consider fast.

Table 2. Watermarking and De-Watermarking Times.

Image	Watermarking & Encryption time	De_ watermarking & Decryption time
Image1	2.66e+00 sec	02 sec
Image2	2.84e+00 sec	2.25e+00 sec
Image3	2.83e+00 sec	2.08e+00 sec
Image4	2.69e+00 sec	2.20e+00 sec
Image5	2.78e+00 sec	2.11e+00 sec

The verification accuracy performance of the watermarked images obtained by watermarking algorithm was evaluated. The original and the watermarked images were compared and similarity scores obtained. Now the genuine and imposter test is performed. The performance evaluation of the biometric authentication system is done by using (FRR) and (FAR).

$$FRR = \frac{\text{False Non-matches.}}{\text{genuine-Attempts}} \quad (17)$$

$$FAR = \frac{\text{False-matches.}}{\text{Imposter-Attempts}} \quad (18)$$

The authentication result of matching the entered fingerprint with the same embedding fingerprint after extract and decrypt it the result show matching 100% for all samples in the dataset.

The matching results which are obtained based on 19800 matching processes between images from different classes (FAR) and 200 matching between images in the same class (FRR). The FAR result is 0.02 and the FRR result is 0.3.

The time factor is important in similar applications, so we will calculate the Central Processing Unit CPU time taken by a single

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

registration processes as average registration time and the time taken by the CPU for single authentication process as average authentication time. The registration time includes the encryption and watermark time, where the authentication process includes the de-watermark and matching process. The table 3 below show the full time required for implementation the two process for different fingerprint. The result indicated that the authentication time range between 1.2 to 1.4 which is consider fast and convenient to use in verifying the user.

Table 3. Time Required for Registration and Authentication Process.

Image	Registration time	Authentication time
Image1	3.23e+00 sec	1.42e+00 sec
Image2	2.98e+00 sec	1.42e+00 sec
Image3	03 sec	1.39e+00 sec
Image4	2.91e+00 sec	1.27e+00 sec
Image5	2.98e+00 sec	1.44e+00 sec

5. CONCLUSIONS

In this paper, a user authentication scheme has been proposed and implemented based on the smart card. The presented authentication scheme proved that it is feasible to confirm the data accessed only by the authorized user. The combination of the two authentication methods "biometric authentication" and "watermarking technique," gave us more robust authentication scheme. Furthermore, the using of two biometric for each person: the fingerprint and face image give high accuracy to the scheme which make it achieve the authentication, recognition and give security to a person biometric data. The using of encryption before watermarking process gives the scheme a dual layer of security which ensure that the watermark is safe, even if the watermark is detected it will be incomprehensible, so that makes this scheme more secure. The results demonstrated the validity and efficiency of the scheme compared to previous schemes.

REFERENCES

[1] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*, vol. 479. Springer Science & Business Media, 2006.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[3] D. D. Zhang, *Automated biometrics: Technologies and systems*, vol. 7. Springer Science & Business Media, 2013.

[4] K. W. Bowyer, K. P. Hollingsworth, and P. J. Flynn, "A survey of iris biometrics research: 2008–2010," in *Handbook of iris recognition*, Springer, 2013, pp. 15–54.

[5] J. Ashbourn, *Biometrics in the new world: The cloud, mobile technology and pervasive identity*. Springer Science & Business Media, 2014.

[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Commun. ACM*, vol. 43, no. 2, pp. 90–98, 2000.

[7] G. Költzsch, "Biometrics-market segments and applications," *J. Bus. Econ. Manag.*, vol. 8, no. 2, pp. 119–122, 2007.

[8] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Trans. Image Process.*, vol. 9, no. 5, pp. 846–859, 2000.

[9] A. K. Jain, U. Uludag, and R.-L. Hsu, "Hiding a face in a fingerprint image," in *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, 2002, vol. 3, pp. 756–759.

[10] V. S. Inamdar and P. P. Rege, "Dual watermarking technique with multiple biometric watermarks," *Sadhana*, vol. 39, no. 1, pp. 3–26, 2014.

[11] X. Peng, J. Lu, L. Li, C.-C. Chang, and Q. Zhou, "A New Card Authentication Scheme Based on Image Watermarking and Encryption," in *International Workshop on Digital Watermarking*, 2016, pp. 358–369.

[12] J. G. Ko and K. Y. Moon, "Biometrics Security Scheme for Privacy Protection," in *Advanced Software Engineering and Its Applications, 2008. ASEA 2008*, 2008, pp. 230–232.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] W. Wojtowicz and M. R. Ogiela, "Digital images authentication scheme based on bimodal biometric watermarking in an independent domain," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 1–10, 2016.

[14] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Mach. Vis. Appl.*, vol. 25, no. 1, pp. 263–275, 2014.

[15] M. K. Dutta, A. Singh, K. M. Soni, R. Burget, and K. Riha, "Watermark generation from fingerprint features for digital right management control," in *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*, 2013, pp. 717–721.

[16] M. Alkhathami, F. Han, and R. Van Schyndel, "Fingerprint image watermarking approach using DTCWT without corrupting minutiae," in *Image and Signal Processing (CISP), 2013 6th International Congress on*, 2013, vol. 3, pp. 1717–1723.

[17] M. A. Orumiehchiha, J. Pieprzyk, E. Shakour, and R. Steinfeld, "Cryptanalysis of RC4 (n, m) Stream Cipher," in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 165–172.

[18] CHIKKERUR, Sharat; GOVINDARAJU, Venu; CARTWRIGHT, Alexander N. "Fingerprint image enhancement using STFT analysis. In: International Conference on Pattern Recognition and Image Analysis". Springer, Berlin, Heidelberg, 2005. p. 20-29.

[19] J. C. Yang and D. S. Park, "Fingerprint Verification Based on Invariant Moment Features and Nonlinear BPNN," International Journal of Control, Automation, and Systems, vol. 6, no. 6, pp. 800-808, Dec. 2008.

[20] M. Liu, X. D. Jiang, and A. Kot, "Fingerprint reference-point detection," EURASIP Journal on Applied Signal Processing, vol. 4, pp. 498-509, 2005.

[21] VAISHNAVI, D.; SUBASHINI, T. S. "Robust and invisible image watermarking in RGB color space using SVD". procedia computer science, 2015, 46: 1770-1777.