Transmission of Secure Biometric Data for Network-based User Authentication

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

26-12-2020 / 30-12-2020

CITATION

Khan, M (2020): Transmission of Secure Biometric Data for Network-based User Authentication. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.13489464.v1>

DOI

[10.36227/techrxiv.13489464.v1](https://doi.org/10.36227/techrxiv.13489464.v1)

Transmission of Secure Biometric Data for Network-based User Authentication

Muhammad Khan

ABSTRACT

The large-scale utilization of biometric authentication systems creates a demand for effective and reliable security and privacy of its data. Biometric data is not secret and if compromised, it can have catastrophic effects on the integrity of the whole verification system. To address these issues, this paper presents a novel encryption and watermarking method by using public key infrastructure for the secure transmission of biometric data over network. Encryption is applied on the biometric template before embedding as a watermark to make it more secure and robust and then, it is hid into the cover image. Experimental results show that the security, performance, and accuracy of the presented method is encouraging comparable with the other methods found in the current literature.

Keywords: Biometrics, Iris template, Watermarking, Network, Authentication, Security

I. INTRODUCTION

Biometric is defined as measurable physiological and/or behavioral characteristic that can be utilized to verify the identity of an individual. It includes fingerprint, hand geometry, palm print, voice, face, and iris recognition etc. Biometric is of interest in any area where it is important to verify and authenticate the true identity of an individual. Biometric technologies are gaining more attraction because of secure authentication methods for user access, e-commerce, remote authentication, and access control. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric has shown itself as an emerging technology and can be integrated other technologies to implement high security [1] [2] [3].

Biometric techniques have inherent advantages over traditional personal identification techniques such as PINs, identification cards, and passwords; but the problem of ensuring the security and integrity of biometric data is critical. The reliability and user acceptance of a biometric system depends on the effectiveness of the system and the security of the system against intruders, unauthorized modification, and misuse. A biometric-based verification system works properly only if the verifier system can guarantee that the templates come from the valid and legitimate user at the time of enrollment [4].

Biometric data is unique, but it does not provide secrecy. Only biometrics is not a panacea for the secrecy of data because it has some risks of being hacked, modified, and reused whenever it is sent over the network, so there is a need to protect biometric data from different attacks. To promote wide spread utilization of biometric techniques, an increased security and secrecy of its data are necessary. Watermarking and encryption can be used to achieve the data security and secrecy [4] [5] [6].

Watermarking can be considered as a special technique of steganography [7], where one message is embedded in another and the two messages are related to each other in some way. The most common example of watermarking is the presence of specific patterns in currency note, which is visible only when the note is held to light, and logos in the background of printed text documents. The watermarking

techniques prevent forgery and unauthorized replication of physical objects [8]. A watermark must exhibit the following quality factors:

- ✧ A watermark must be imperceptible, that is to say the insertion of such a watermark must preserve the perceptual quality of the digital data. The imperceptibility of the watermark also makes it more difficult to pirate it.
- ✧ A watermark must also be indelible and undetectable to resist from intentional attacks for destroying the watermark.
- ✧ A watermark must also be robust against conventional processing applied to digital data, such as compression, resizing, cropping, and filtering etc.
- ✧ Finally, a watermark must be reliable, that is to say must allow a reliable decision with regard to the existence.

Encryption is mostly used way of data security. Before the content is made ready for delivery over a network, it should be encrypted. Once the data has been encrypted, it cannot be used until it is decrypted. In encryption, there are two basic problems 1) Hackers have historically found ways to crack encryption, in effect, obtaining the key without being a legitimate user; and 2) Once a single legitimate copy of some content has been decrypted, a hacker is now free to make another copy of the decrypted data [6].

Nowadays, public key infrastructure is widely utilized because of its assurances against the data misuse and impersonation risk. The PKI is a system of digital certificates, certificate authorities, and other registration authorities that verify the authenticity and validity of each party involved in a transaction [9]. PKI enables a number of other security services including data integrity, confidentiality, non-repudiation, and authenticity under one umbrella. It provides a way by which organizations or private users can implement a level of data transmission security appropriate to their needs.

It is also possible for a user or an organization to send the data directly to receiver without formally going through the certification authority or trusted third party process. However, managing the ongoing situation could become susceptible if a hacker gets the data and then he can copy it to make fake transactions whenever he wants. A trusted certification authority (CA) thus provides a useful management function to implementing a PKI. PKI uses digital certificates as an authentication mechanism and manages these certificates e.g. issuance and revocation, and their associated keys. This digital certificate acts a data package, which identifies an entity, and is issued by a CA only after the verification of that entity. This certificate includes the public key that belongs to that entity. Digital certificates are the vital component in the PKI and they act as digital passports by binding the user's digital signature to their public keys [10]. Industry standard PKI and their certificates are built on the X.509 specifications of the ISO [9].

A. Related Work

First, Yeung-Pankanti [12] investigated the effects of watermarking fingerprint images on the recognition and retrieval accuracy using an invisible fragile watermarking technique for image verification applications on a fingerprint recognition system. They specified that introducing watermarking in the fingerprint images can provide a value-added protection, as well as copyright notification capability, to the fingerprint data collection processes and its usage.

Later, Sonia [11] researched on a local average scheme where an executable compares the block-by-block local average of the transmitted image and the received image. Her method does not provide the detailed results on the watermarked image, and she did not give any signal or image processing effects on her method.

In 2002, Gunsel et al. [5] presented two spatial domain-watermarking methods. Their first method utilizes an image adaptive strength adjustment technique to make low visibility of watermark, while

another method uses feature adaptive watermarking technique, thus applicable before feature extraction. The drawback of their system is that they did not encrypt watermark data, so their method is also vulnerable to attack if an adversary is successful in extracting the biometric template from the transmitted image.

Recently, Jain-Uludag [4] proposed two application scenarios based on amplitude modulation watermarking method for hiding biometric data. First application is based on steganography, while another is embedding the facial information in fingerprint images. Jain-Uludag did not mention the different kinds of noises and attacks on their method, so it is difficult to judge performance of their system under different conditions. Furthermore, their both applications embed watermark without being encrypted so it could also have the risk of biometric data copy attack if an adversary is able to extract it from the transmitted host image.

To improve the security and secrecy of transmission, this paper presents a novel encryption and watermarking method, in the PKI domain, to protect biometric data, for the network-based authentication. For the PKI domain, a trusted third party as the certification authority (CA) is utilized. The CA works for the administration and monitoring of integrity, authentication, non-repudiation, and confidentiality of biometric data. It also creates a trust between biometric client and biometric authentication server as a trusted third party (TTP). The CA can act as a judge in the case of any dispute of transaction originated from the either side, so it safes the system from the security risks. On the other hand, for the watermarking, our method utilizes DWT due to its excellent time-frequency features and well matching to the human visual system (HVS) characteristic, which makes embedded watermark more imperceptible and robust to image distortions than embedded watermark in the spatial domain. Before embedding the watermark, we encrypt the biometric template by a chaotic sequence that is very sensitive to its initial value [13], gives good performance, and easy to implement. Hence, the proposed scheme solves the problems found in the related literature cited at the beginning of this subsection. We also perform rigorous experiments and show the better performance of the proposed scheme.

B. Outline

Rest of the paper is outlined as follows: Section II gives an overview, architecture, and details of the proposed system. Section III presents the proposed transmission scheme. Experiments and results are reported in Section IV. At the end, Section V concludes the findings and gives the consideration of future work.

II. PROPOSED SYSTEM MODEL

In the proposed system, there are three main entities; biometric client, biometric authentication server, and certification authority (CA), as shown in Fig. 1. If client generates connection request to the server, then server issues its digital certificate to the client to ensure the server's authenticity. This digital certificate is signed by the trusted CA, which contains the server's public key together with the confirmation of integrity from the CA in the form of its digital signature. The purpose of using the server's digital certificate is that, it creates the client's trust in the server and ensures that the server is not an adversary or fake party.

After this process, the authentication server sends a message to the client for biometric data transfer. On the client side, biometric data of a user is captured from the sensor and then image processing algorithms are performed to extract the features for watermark generation, as shown in Fig. 2. For the proposed system, as a reference biometric, human iris templates are used to embed as the watermark.

To perform encryption, chaotic logistic map is utilized to scramble the iris template before watermarking. The most attractive features of chaos in encryption and information hiding are its extreme

sensitivity to initial conditions and the outspreading of orbits over the entire space [13]. These special characteristics make chaotic maps excellent candidate for watermarking and encryption, based on the classic Shannon's requirement of

Figure 1. The CA Model

confusion and diffusion [14]. In recent years, chaotic maps have been widely used for digital watermarking, to increase the security [13]. Because of these attractive properties, a chaotic sequence is applied on the iris code for the encryption and to make it more secure.

After encryption, biometric template is inserted into the cover/host image and the end result of this step is a watermarked image, which contains iris template hidden in the encrypted form. For this process, DWT based blind watermarking algorithm is employed, which does not require the original image to extract watermark from the cover that contains watermarked data. The reason for using DWT is due to its superior robustness against various signal processing attacks and high data compression [15].

We also utilized the client digital certificate to ensure the authenticity of the client. This certificate is also signed by the CA with its private key. Before sending the data to the server, the client's secret key is encrypted with the server's public key for the symmetric key encryption and then the watermarked image with the client digital certificate is sent to the server for the verification of the client. For further encryption/decryption process, this secret symmetric key is used, which increases the encryption/decryption performance of the system. After receiving the client certificate with the encrypted secret key, server verifies the authenticity of the client by its digital certificate and decrypts the client's secret key with its private key. This is a temporary key and for every transaction, this key will be different. After decrypting secret key and validating the client's authenticity, server performs watermark extraction from the cover image. The same chaotic sequence with the secret key is applied on the extracted iris code to decrypt it in its actual form, as it was embedded in watermark embedding process. The watermark embedding and extraction process is depicted in Fig. 3(a) and 3(b), which is the detailed delineation of the process shown in Fig. 1. The end result of this step is extracted iris template code ready to perform for identification and verification in the database. Hence, secure transmission of the biometric data is ended after this process.

Figure 2. Proposed system model

III. PROPOSED TRANSMISSION SCHEME FOR BIOMETRIC DATA

Our proposed scheme, for the secure transmission of biometric data, consist of the digital certificate creation, watermark generation and encryption, watermark insertion, watermark extraction, and watermark decryption and matching. In the following subsections, these processes are described in detail.

A. Client Server Session Management

In the presented system, if the client wants to send biometric data to the authentication server, first the client makes an initial connection with the server. In response, the server issues its digital certificate to the client that contains the server's public key and different data fields, as shown in figure 4. This digital certificate is signed with the private key of the CA. After getting the certificate, the client verifies it by the public key of the CA. Digital certificate contains digital signature of the CA, which is signed with its private key and is difficult to be forged. So, it makes a trust that the authentication server is not an intruder or a fake party.

B. Watermark Generation and Encryption

Before the watermark generation and encryption, we capture the iris-biometric of the client by the camera. After capturing the iris image, we extract the iris features by the process and method described by John Daugman [1], the inventor of the iris recognition system. For the encryption, we use a chaotic sequence to encrypt the iris template before embedding as a watermark. We use Logistic chaotic map to generate a sequence of real numbers [7]:

$$y_{n+1} = g(y_n) = \lambda y_n (1 - y_n) \quad (1)$$

Where $3.57 < \lambda \leq 4$, the sequence is non-periodic, non-convergent, and very sensitive to the initial value, which is used as a secret key. Then, we normalize this sequence to a binary image $c_{i,j} \in \{0,1\}$ by

$$c_{i,j} = \begin{cases} 1 & y_n \geq 0.5 \\ 0 & y_n < 0.5 \end{cases} \quad (2)$$

We use Exclusive-OR (XOR) operation to encrypt the watermark sequence $s_{i,j}$, and the encrypted

watermark is obtained by $w_{i,j} = s_{i,j} \oplus c_{i,j}$.

Figure 3. Watermarking process (a). Embedding process
(b). Watermark extraction process

C. Watermark Insertion

In generating the pseudo random numbers, a key is used as a seed value. The generated numbers are used as a watermarking position of LH2, HL2, and HH2 sub-band. To avoid overlapping of watermark allocation and modification of pixel value, we select the watermarking position separated with at least one pixel. The same pixel should not be selected as watermark embedding position in selecting the procedure. If size of the watermark is large, we can also select the pixels in HL3, LH3 and HH3 for embedding e.g. the template size of multimodal biometric template is large, which can contain face, voice or iris together.

After that, we compute neighboring symbol's mean value of selected pixel by using (3). The pixel value of the watermark embedding position is $x_{i,j}$, and the mean value of the neighboring value is $m_{i,j}$, then we compute $m_{i,j}$ using the following formula:

$$m_{i,j} = \text{mean}(x_{i,j-1}, x_{i-1,j}, x_{i+1,j}, x_{i,j+1}) \quad (3)$$

i. Flag generation and watermark insertion

After computing the mean value, we embed the encrypted watermark into the selected pixels and generate flags ($f_{i,j}$) by the following steps:

- 1) If the selected $x_{i,j}$ is bigger than the mean value $m_{i,j}$ and $w_{i,j} = 1$, we change $x_{i,j}$ with $x'_{i,j}$ using (4) and create a flag $f_{i,j}$ that contains value of 0.

$$\begin{aligned} & \text{if}(x_{i,j} > m_{i,j} \text{ and } w_{i,j} = 1) \text{ then} \\ & x'_{i,j} = x_{i,j}(1 - \alpha w_{i,j}) \\ & f_{i,j} = 0 \end{aligned} \quad (4)$$

Where α is the watermark embedding strength.

- 2) If the selected $x_{i,j}$ is bigger than mean value $m_{i,j}$ and $w_{i,j} = 0$, we change $x_{i,j}$ with $x'_{i,j}$ using (5) and create a flag $f_{i,j}$ that contains value of 1.

$$\begin{aligned} & \text{if}(x_{i,j} > m_{i,j} \text{ and } w_{i,j} = 0) \text{ then} \\ & x'_{i,j} = x_{i,j}(1 - \alpha) \\ & f_{i,j} = 1 \end{aligned} \quad (5)$$

- 3) If the selected $x_{i,j}$ is smaller than the mean value $m_{i,j}$ and $w_{i,j} = 1$, we change $x_{i,j}$ with $x'_{i,j}$ using (6) and create a flag $f_{i,j}$ that contains value of 2.

$$\begin{aligned} & \text{if}(x_{i,j} < m_{i,j} \text{ and } w_{i,j} = 1) \text{ then} \\ & x'_{i,j} = x_{i,j}(1 + \alpha w_{i,j}) \\ & f_{i,j} = 2 \end{aligned} \quad (6)$$

- 4) If the selected $x_{i,j}$ is smaller than the mean value $m_{i,j}$ and $w_{i,j} = 0$, we change $x_{i,j}$ with $x'_{i,j}$ using (7) and create a flag $f_{i,j}$ that contains value of 3.

$$\begin{aligned} & \text{if}(x_{i,j} < m_{i,j} \text{ and } w_{i,j} = 0) \text{ then} \\ & x'_{i,j} = x_{i,j}(1 + \alpha) \\ & f_{i,j} = 3 \end{aligned} \quad (7)$$

These equations describe that the modified value $x'_{i,j}$ is proportional to the original value of the image $x_{i,j}$, which makes the watermark more robust. The generated flag $f_{i,j}$ is stored in the database and is used in the watermark extraction procedure. After this process, we take the inverse transform of the host image using inverse discrete wavelet transform (IDWT) to construct the watermarked image.

X.509 Ver. 3 Digital Certificate
Certificate Version
Certificate Serial Number
Signature Algorithm ID
Issuer Name
Validity Period (Start and End)
Subject Name
Subject Public Key (RSA 1024 Bits)
Unique Identifier of CA & Subject
Extensions (Optional)
Digital Signature by CA

Figure 4. X.509 Digital Certificate Fields

D. Client Digital Certification and Secret Key Encryption

After the watermark has been successfully embedded, the client encrypts its secret key Sk_c with the public key Pk_s of the authentication server. The client's secret key was used to encrypt the biometric data in the encryption step. We also use the client's digital certificate, which creates the trust of server in the client and this certificate is issued by the CA. At the end of this stage; client's digital certificate, encrypted secret key, and the watermarked image are sent to the authentication server for the client verification. The mathematical notation of client's secret key encryption process is shown in the following.

$$E_{Sk_c} = Enc(Pk_s, Sk_c)$$

Where, $Enc()$ shows the encryption process and Pk_s is the public key of the authentication server.

E. Client Certificate Verification, Key Decryption and Watermark Extraction

At the server end, the watermarked image with the encrypted secret key and the client's digital certificate is received. First, the authentication server validates this digital certificate and signature using the public key of the CA. After checking the certificate, if it is not forged or tempered, the server decrypts the encrypted secret key of the client by its private key Sk_s and extracts the watermark from the host image. The mathematical form of decryption of the client's secret key is as follows:

$$D_{Sk_c} = Dec(Sk_s, E_{Sk_c})$$

Where, $Dec()$ shows the decryption process and Sk_s is the secret key of the authentication server.

For the data extraction, we transform the watermarked image using second level discrete wavelet decomposition, as it was decomposed in watermark insertion process, to extract the watermark from LH2, HL2 and HH2 sub bands. After transforming the image into wavelet domain, we find the watermark embedded location by using the same key, which was used in watermark insertion procedure. After then, we compute neighbor's mean value $m_{i,j}$ using the same method described in watermark insertion process and generate a flag $f'_{i,j}$, and then generate $w'_{i,j}$ using the opposite procedure described in flag generation and watermark insertion process.

F. Watermark Decryption and Matching

After successfully extraction of the watermarked data from the received watermarked image, we perform decryption by using the secret key of the client. We utilize the formula $s'_{i,j} = w'_{i,j} \oplus c_{i,j}$ to decrypt the extracted data. Then, we compare the extracted watermark $s'_{i,j}$ with the original template, which is stored in the database. Equation (8) is used for this matching process.

$$M_{Match} = \frac{N_z(xor(s_{i,j}, s'_{i,j}))}{N} \quad (8)$$

Where, N_z is total number of zeros by an Exclusive-OR (XOR) operation between an original template $s_{i,j}$ stored in the database, while $s'_{i,j}$ is an extracted and decrypted watermark sequence from the cover image. N is the size of the template. Here, we may define a matching threshold according to the criticality and usage of the system.

IV. Experimental Results and Discussions

In this section, we present experimental results performed during the research of this work. The security of the system by the encryption and digital certificates, and biometric data matching performance is also discussed. To evaluate the performance of the proposed method, portions of the research in this paper use the CASIA iris image database collected by institute of automation, Chinese academy of sciences. CASIA iris image database (ver 1.0) contains 756 iris images from 108 eyes [16].

For the trust between two parties, public key certificates are utilized, which are issued by the CA. We used the client and server certificates to verify both parties for each other and it make a trust between them. The server digital certificate is issued to the client on which client relies and vise versa. Certificates are signed by the CA with its private key and are impossible to forge, because of the CA's digital signature. Usage of this protocol protects the system from man-in-the-middle and replay attacks [17]. This certificate also contains the public key of the server, which we used to encrypt secret chaotic key that was utilized for the encryption of biometric data before embedding as a watermark. The generated chaotic sequences for the encryption process showed good statistical properties and their auto-correlation and cross-correlation curves are depicted in Fig. 5.

(a). Auto-correlation curve of the chaotic sequences (b) Cross-correlation curve of chaotic sequences
Fig. 5. The statistical correlation curves of chaotic sequences

The embedded watermark size is 512 bytes, which is normally the standard size of the iris template used in the industry [1]. We performed experiments on different images as shown in Fig. 6. We used Baboon, Lena, New York, and Sailboat images for the experiments and the extracted biometric data is exactly the same as it was encoded. The watermarked data extraction performance in comparison with others is shown in Table I. If the embedded watermark size is smaller, then the performance to extract the watermark will be higher because each bit of the watermark will be embedded into more locations, and the effects and distortions of noises and other signal processing effects will be lower.

TABLE I
COMPARISON OF THE PROPOSED METHODS (In %)

Image	Method in [18]	Method in [5]	Our method
Lena	99.57	99.78	99.86
Baboon	91.79	100	99.84
Sailboat	73.87	99.78	99.81
New York	98.49	99.78	99.79

TABLE II
PERFORMANCE COMPARISON AFTER 50% CROPPING EFFECTS

Image	Method in [5]	Our method
Lena	93.52	97.29
Baboon	95.03	97.14
Sailboat	84.02	96.85
New York	93.74	94.13

Furthermore, we applied cropping on the watermarked images and evaluated the performance of our method against Günsel et al. [5], as shown in Table II. Jain-Uludag [4] did not mention the effect of

cropping in their method, so it is very difficult to judge the performance of their system against cropping and other noises.

Figure 6. Sample cover images (a-d) and watermarked stego images (e-h)
(New York Image courtesy of Patrick Loo, University of Cambridge, others from USC-SIPI)

There are two kind of attacks on watermarking: one is through signal processing such as filtering, additive noise, and compression; the other is to use geometric transformations, which include cropping, scaling, and rotating, and so on [14]. In most watermarking algorithms, the tolerance to the first type of attack is higher than that to the latter. Our scheme also aims at gaining high robustness against cropping attack, describe earlier, as compare to Günsel et al.'s system [4]. Even, it tolerates against both kind of noises and distortions e.g. Wiener filtering, median filtering, resizing, JPEG compression, Gaussian noise, and cropping etc. The detailed experimental results on each image are shown in Table III. As a reference, in Fig.7, Lena image is depicted under different attacks. These attacks are described in Table III on each individual watermarked image with their decoding performance and PSNR value. The performance of Table III shows that if watermarked image is significantly affected, the watermarked-biometric data is little distorted and is able to perform the verification of a person. PSNR is computed by the following equation [20].

$$PSNR(I, \hat{I}) = 10 \log_{10} \left[\frac{(\max_{\forall(m,n)} I(m,n))^2}{\frac{1}{N_I} \sum_{\forall(m,n)} (\hat{I}(m,n) - I(m,n))^2} \right] \quad (8)$$

Where, I and $\hat{I}$ are original and watermarked images, respectively. N_I is the number of pixels in the image, $(\max_{\forall(m,n)} I(m,n))$ is the maximum gray-value of the original host image.

Furthermore, Günsel et al. [5] and Jain-Uludag [4] didn't apply encryption on the biometric template before or after the watermark embedding, so their method is susceptible if a hacker becomes successful in extracting the watermarked data from the host image. Thus, their scheme is vulnerable to the so-called copy attack [19], where any unauthorized person can copy hacked watermark from the host image and misuse it on purpose [21]. Sonia's [11] method does not provide detailed results on the watermarked image, and she

did not give any signal or image processing effects on her method. Yeung-Pankanti [12] also did not give the detail of attacks on their method, but claimed that their method gives a significant performance. So, it is difficult to judge performance of their method under different kind of attacks and noise.

Figure 7. Lena image under different attacks (a) Median filtering (b) Wiener filtering (c) Gaussian noise (d) Resize (e) Cropping (f) JPEG compression

TABLE III
DETAILED EXPERIMENTAL RESULTS ON EACH IMAGE

(A) BABOON IMAGE		
Attacks	PSNR (dB)	Accuracy (%)
Median Filtering (3x3)	20.42	87.19
Wiener Filtering (6x6)	23.40	88.66
Resize Attack	19.48	87.08
Cropping (50%)	16.44	97.14
Gaussian Noise (0,0.001)	29.10	93.83
JPEG Compression (4:1)	23.73	94.84

(B) LENA IMAGE		
Attacks	PSNR (dB)	Accuracy (%)
Median Filtering (3x3)	30.89	88.68
Wiener Filtering (6x6)	32.90	87.25
Resize Attack	27.95	86.97
Cropping (50%)	17.20	97.29
Gaussian Noise (0,0.001)	29.61	87.27
JPEG Compression (4:1)	34.76	95.85

(C) SAILBOAT IMAGE		
Attacks	PSNR (dB)	Accuracy (%)
Median Filtering (3x3)	26.33	88.14
Wiener Filtering (6x6)	28.91	88.11
Resize Attack	24.12	86.76
Cropping (50%)	14.38	96.85
Gaussian Noise (0,0.001)	29.41	89.25
JPEG Compression (4:1)	30.41	94.84

(D) NEW YORK IMAGE		
Attacks	PSNR (dB)	Accuracy (%)
Median Filtering (3x3)	20.48	92.26

Wiener Filtering (6x6)	23.02	90.47
Resize Attack	18.35	89.59
Cropping (50%)	17.50	94.13
Gaussian Noise (0,0.001)	30.63	89.44
JPEG Compression (4:1)	22.99	88.03

V. Conclusion

In this work, we have presented a novel scheme for the secure transmission of biometric data over network in which X.509 digital certificates, encryption, and watermarking are combined to ensure the authenticity, confidentiality, and integrity of the transmitted templates. Due to the excellent time-frequency features and well matching to the human visual system (HVS) characteristics, we utilized DWT to hide iris templates as watermark. To validate the client and server authenticity, we used X.509 public key digital certificates which safe the system from non-repudiation, man-in-the-middle, and replay attacks, and provide the secure authentication and integrity of the biometric data. We encrypted biometric data by chaotic logistic encryption method before embedding as watermark, which makes our system more secure and protected from the copy attack. Furthermore, we performed a series of experiments to evaluate the proposed system. Moreover, we carried out extensive quantitative comparisons among some existing methods and provided discussions on the overall experimental results. Experimental results have shown that presented system is highly robust against different kind of attacks and gives better performance than others.

The proposed system can also be used for any biometric data e.g. fingerprint, face or palm print etc for network-based biometric authentication. Hence, our system is an open ended system for securing biometric templates. An interesting future research in this area can be to use both, robust and fragile watermark simultaneously for hybrid watermark based identification.

References

- [1] J. Daugman. "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, pp.1148-1161, Nov. 1993.
- [2] Muhammad Khurram Khan, Zhang Jiashu, "Securing Biometric Templates for Reliable Identity Authentication", ICIC, Lecture Notes in Computer Science, part II, no. 3645, pp. 723-732, Springer-Verlag, August 2005.
- [3] S. B Pan et al, "An Ultra-Low Memory Fingerprint Matching Algorithm and Its Implementation on a 32-bit Smart Card", IEEE Transactions on Consumer Electronics, vol. 49, no. 2, pp. 453-459, May 2003.
- [4] Anil K. Jain, Umut Uludag, "Hiding Biometric Data", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, November 2003.
- [5] B. Günsel, U. Uludag, and A.M. Tekalp, "Robust Watermarking of Fingerprint Images," Pattern Recognition, Elsevier Science Ltd., vol. 35, no. 12, pp. 2739-2747, Dec. 2002.
- [6] I.J. Cox et al, "Digital Watermarking", Morgan Kaufmann Publishers, CA, USA, 2002
- [7] ED Dawson, Javier Lopez, J.A. Montenegro, and Eiji Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure", IEEE International Conference on ITRE, pp. 274-278, Aug. 2003.
- [8] N. Memon, and P.W Wong, "A Buyer-Seller Watermarking Protocol", IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643-649, April 2001.
- [9] A. Bourka, D. Polemi, and D. Koutsouris, "Interoperability among Healthcare Organizations Acting as CA", IEEE Transactions on IT and Biomedicine, vol. 7, no. 4, Dec. 2003.
- [10] Ray Hunt, "PKI and Digital Certification Infrastructure", IEEE Conference on Networks, pp. 234-239, Oct. 2001.
- [11] Sonia Jain, "Digital Watermarking Techniques: A Case Study in Fingerprints and Faces", Proc. Indian Conference on Computer Vision, Graphics, and Image Processing, pp.139-144, Dec.2000

- [12] M.M. Yeung and S. Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval," *Journal of Electronic Imaging*, vol. 9, issue no .4, pp. 468-476, Oct. 2000.
- [13] Jiashu Zhang, Lei Tian and Heng-Ming Tai, "A New Watermarking Method Based on Chaotic Maps", *Proc. IEEE ICME'04*, Taiwan, 2004.
- [14] Zhao Dawei, Chen Guanrong, Liu Wenbo, "A Chaos-based Robust Wavelet-domain Watermarking Algorithm", *Chaos, Solitons and Fractals*, Elsevier Science Ltd., vol. 22, pp. 47-54, 2004.
- [15] I. Hong, I. Kim, and S.S Han, "A Blind Watermarking Technique Using Wavelet Transform", *Proc. of IEEE ISIE*, pp. 1946-1950, 2001
- [16] CASIA Iris Database, [online] <http://www.sinobiometrics.com>, October 2005.
- [17] T. Jiang, Y. Hou. and S. Zheng, "Secure Communication between Set-top Box and Smart Card in DTV Broadcasting", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 3, pp.882-886 , Aug. 2004
- [18] U. Uludag, B. Gunsel, A.M. Tekalp, "Robust Watermarking of Busy Images", *Proceedings of SPIE Electronic Imaging 2001 Conference, Security and Watermarking of Multimedia Contents III*, vol. 4314, California, USA, pp. 18-25, 2001.
- [19] F. Deguillaume, S. Voloshynovskiy, T. Pun, "Secure Hybrid Robust Watermarking Resistant Against Tampering and Copy Attack", *Signal Processing*, Elsevier Science Ltd., pp. 2133-2170, 2003
- [20] D. Kundur, D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", *Proceedings of the IEEE*, vol.87, no.7, pp.1167-1180, July 1999.
- [21] M.K Khan, K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'", *Sensors*, vol. 10, Issue 3, pp. 2450-2459, 2010.
- [22] Horng, S.J. Tzeng, S.F. Pan, Y. Fan, P. Wang, X. Li, T. Khan, M.K, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", *IEEE Transactions on Information Forensics Security*, 2013, 8, 1860-1875.
- [23] Z. Liu, X. Huang, Z. Hu, M.K. Khan, H. Seo, L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age", *IEEE Transactions on Dependable and Secure Computing*, pp. 99, 2017, pp. 237-248
- [24] S.F Tzeng, S.J Horng, T. Li, X. Wang, P.H. Huang, M.K Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", *IEEE Transactions on Vehicular Technology*, vol 66, no. 4, pp. 3235-3248, 2017
- [25] A.K Das, M. Wazid, N. Kumar, M.K Khan, K.W.R Choo, Y.H Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment", *IEEE Journal of Biomedical and Health Informatics*, vol. 22, issue 4, pp. 1310-1322, 2017
- [26] F. Wu, L. Xu, S. Kumari, X. Li, A.K. Das, M.K Khan, M. Karupiah, R. Baliyani, "A Novel and Provable Authentication and Key Agreement Scheme with User Anonymity for Global Mobility Networks", *Security and Communication Networks*, 2016
- [27] I. Uddin, M. Guizani, B.S Kim, S. Hassan, M.K Khan, "Trust Management Techniques for the Internet of Things: A Survey", vol. 7, pp. 29763-29787, *IEEE Access*, 2018
- [28] A.S Tolba, M.K Khan, Khaled A, "Systems and Methods for Three Factors Authentication", *US Patent No. 8862888*, 2014
- [29] M.K Khan, "Fingerprint Biometric-based Self and Deniable Authentication Schemes for the Electronic World", *IETE Technical Review*, vol. 26, issue 3, pp. 191-195, May-June, 2009