Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2011, Article ID 174945, 12 pages
doi:10.1155/2011/174945

Research Article

Video-Object Oriented Biometrics Hiding for User Authentication under Error-Prone Transmissions

Klimis Ntalianis,[1] Nicolas Tsapatsoulis,[1] and Athanasios Drigas[2]

[1] *Department of Communication and Internet Studies, Cyprus University of Technology, 3603 Limassol, Cyprus*
[2] *Net Media Laboratory, NCSR Demokritos, 15310 Athens, Greece*

Correspondence should be addressed to Klimis Ntalianis, klimis.ntalianis@cut.ac.cy

Received 12 April 2010; Revised 9 November 2010; Accepted 3 January 2011

Academic Editor: Claus Vielhauer

An automatic video-object oriented steganographic system is proposed for biometrics authentication over error-prone networks. Initially, the host video object is automatically extracted through analysis of videoconference sequences. Next, the biometric pattern corresponding to the segmented video object is encrypted by a chaotic cipher module. Afterwards, the encrypted biometric signal is inserted to the most significant wavelet coefficients of the video object, using its qualified significant wavelet trees (QSWTs). QSWTs provide both invisibility and significant resistance against lossy transmission and compression, conditions that are typical in error prone networks. Finally, the inverse discrete wavelet transform (IDWT) is applied to provide the stego-object. Experimental results under various losses and JPEG compression ratios indicate the security, robustness, and efficiency of the proposed biometrics hiding system.

1. Introduction

Person authentication is one of the most important issues in contemporary societies. It ensures that a system's resources are not obtained fraudulently by illegal users. Real-life physical transactions are generally accomplished using paper ID while electronic transactions are based on password authentication, the most simple and convenient authentication mechanism over insecure networks. In [1], a remote password authentication scheme was proposed by employing a one-way hash function, which was later used for designing the famous S/KEY one-time password system [2]. However, in such schemes, a verification table should be maintained on the remote server in order to validate the legitimacy of the requesting users; if intruders break into the server, they can modify the verification table. Therefore, many password authentication schemes [3–7] have recognized this problem, and different solutions have been proposed to avoid verification tables.

One very popular solution is based on cryptographic keys, which are long and random (e.g., 128 bits for the Advanced Encryption Standard [8]), thus it is difficult to memorize. As a result, these keys are stored somewhere (e.g., on a server or smart card) and they are released based on some alternative authentication mechanism (e.g., password). However, several passwords are simple and they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks [9]. In this case, user protection is only as secure as the password (weakest link) used to release the correct decrypting key for establishing user authenticity. Simple passwords are easy to guess; complex passwords are difficult to remember, and some users tend to "store" complex passwords at easily accessible locations. Furthermore, most people use the same password across different applications; if a malicious user determines a single password, they can access multiple applications.

Many of these password-based authentication problems can be confronted by the incorporation of biometrics [10, 11]. Biometrics authentication refers to establishing identity based on the physical and/or behavioral characteristics of a person such as face, fingerprint, hand geometry, iris, voice, way of walking, and so forth. Biometric systems offer several advantages over traditional password-based schemes. They are inherently more reliable, since biometric traits

cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute, and they require the person being authenticated to be present at the time and point of authentication. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional systems, and it can be easily combined with password techniques to enhance the offered security.

In order to further promote the wide spread utilization of biometric techniques to applications over error prone networks, increased security and especially robustness of the biometric data is necessary. Towards this direction, proper combination of encryption and steganography can achieve this goal. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood. In a real-world scenario, encryption can be applied to the biometric signals for increasing security; the templates that can reside in either a central database or a token (e.g., smart card, or a biometric-enabled device such as a cellular phone with a fingerprint sensor), can be encrypted after enrollment. During authentication, these encrypted templates can be decrypted and used for generating the matching result with the biometric data obtained online. As a result, the encrypted templates are secured since they cannot be utilized or modified without decrypting them with the correct key, which is typically secret. On the other hand, steganographic methods can hide encrypted biometric signals so that they cannot be seen, hence, reducing the chances of illegal modifications. Generally, steganography utilizes typical digital media such as text, images, audio, or video files as a carrier (called a host or cover signal) for hiding private information in such a way that unauthorized parties cannot detect or even notice its presence [12].

Several steganographic algorithms have been proposed in the literature, most of which are performed in pixel domain, where more capacity [13] is provided. Many of the existing approaches are based on least significant bit (LSB) insertion, where the LSBs of the cover file are directly changed with message bits. Examples of LSB schemes can be found in [14, 15]. However, LSB methods are vulnerable to extraction [16, 17], and they are very sensitive to image manipulations. For example, converting an image from BMP to JPEG and then back would destroy the hidden information [16]. Furthermore, if an enciphered message is LSB-embedded and transmitted over a mobile network, then it may not be possible to decipher it, even in case of little losses.

On the other hand, a limited number of methods to confront these problems have been proposed. In [18], spread spectrum image steganography (SSIS) was introduced. The SSIS incorporated the use of error control codes to correct the large number of bit errors. In [19], the message is hidden in the sign/bit values of insignificant children of the detail subbands, in nonsmooth regions of the image. Using this technique, steganographic messages can be sent in lossy environments, with some robustness against detection or attack. However, low losses are considered, and the problem of compression remains. A very interesting approach is proposed in [20]. The message is comprised of two components: a soft-authenticator watermark for authentication and tamper assessment of the given image, and a chrominance watermark employed to improve the efficiency of compression. The approach is implemented as a DCT-DWT dual domain, but, unfortunately, the authenticator watermark is not encrypted, making it possible to extract it.

There are also some schemes focusing on steganography of biometric signals. In [21], an amplitude modulation-based steganographic scheme is proposed, which, however, is not tested under compression or lossy transmission. In [22], a wavelet-based steganographic method for minutiae embedding is proposed. Nevertheless, if opponents know the embedding algorithm, they can easily extract the hidden information. In [23], fingerprints are hidden in the region of interest of images. Both DFT and DWT domains are examined. However, again, no encryption is incorporated, thus it is easy to extract the hidden fingerprints. Another interesting, but not resistant to compression, method is proposed in [24], where a remote multimodal biometrics authentication framework that works on the basis of fragile watermarking is designed. Finally, in [25], a DCT-SVD-based watermarking scheme is proposed for ownership protection using biometrics. The scheme is not tested under compression or lossy transmission.

In order to confront the problem of user authentication, in this paper, we propose an efficient wavelet-based steganographic method for biometric signals hiding in video objects, which focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. Interesting techniques for object-oriented data hiding have been presented in the literature, for example [26, 27], however, most of them do not particularly consider the case of biometric data. Thus the main contributions and novelties of the proposed system are as follows. (a) It is one of the first to use video objects to hide their respective biometrics. By this way "dual" authentication is accomplished, the first by visual perception of the figured person, and the second by extraction and matching of the hidden pattern. (b) Biometric signals are encrypted before hiding, using a fast chaotic method. The statistical properties of this novel combination are analyzed and presented. (c) A DWT-based algorithm is adapted for biometrics hiding. In contrast to most steganographic algorithms that are capacity-efficient, the proposed algorithm is very robust to several types of signal distortions. Even though it has been incorporated in a limited number of watermarking schemes, its steganographic potential has not been examined. (d) Resistance of steganographic biometrics systems to signal distortions has not been sufficiently investigated in the literature, a topic that is extensively considered in this paper. By this way, the proposed scheme contributes to illustrate the perspective of encrypted biometrics authentication systems over error prone networks.

In particular, in the proposed system, the biometric signal is initially enciphered using a chaotic pseudorandom bit generator and a chaos-driven cipher, based on mixed feedback and time-variant S-boxes. The use of a chaos-based cryptographic module is justified by the following facts. (a) Chaos presents many desired cryptographic qualities, such as sensitivity to initial conditions, a feature that is

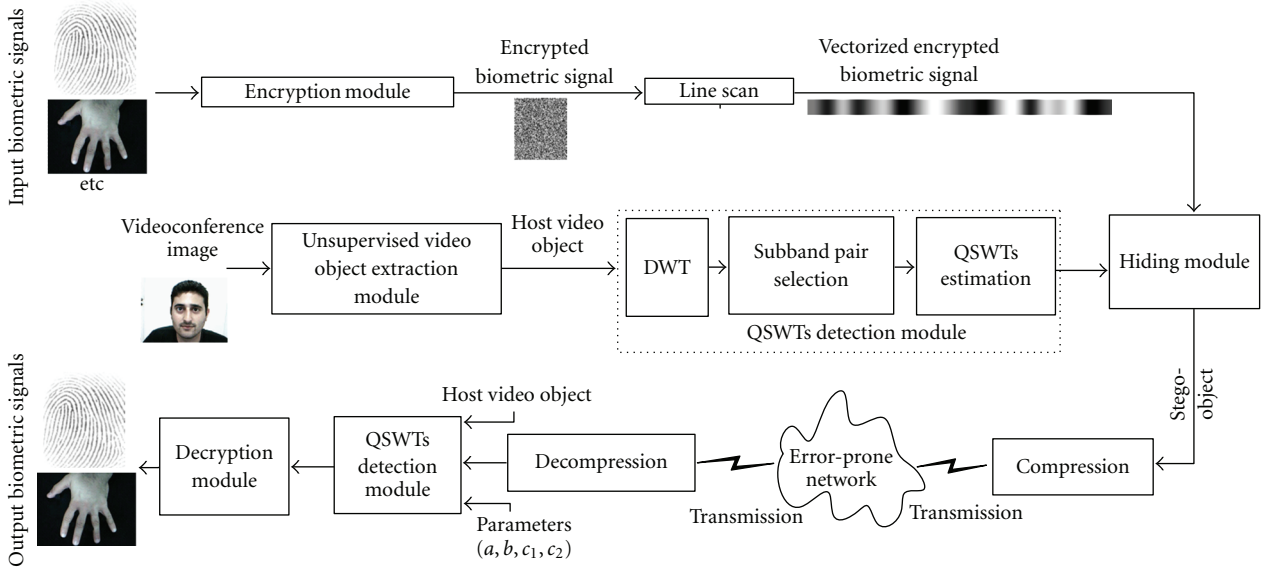


Figure 1: An overview of the proposed system.

very important to an encryption scheme, (b) a chaotic pseudo-random bit generator works very well as a one-time pad generator [28, 29], and one-time pads have been proven to be information-theoretically secure, (c) implementations of popular public key encryption methods, such as RSA or El Gamal cannot provide suitable encryption rates, while security of these algorithms relies on the difficulty of quickly factorizing large numbers or solving the discrete logarithm problem, topics that are seriously challenged by recent advances in number theory and distributed computing and (d) private-key bulk encryption algorithms such as Triple DES or Blowfish, similarly to chaotic algorithms, are more suitable for transmission of large amounts of data. However, due to the complexity of their internal structure, they are not particularly fast in terms of execution speed and cannot be concisely and clearly explained, so as to enable detection of cryptanalytic vulnerabilities.

After encryption, a videoconference image, containing the owner of the biometric signal, is analyzed, and the host video object (VO) is automatically extracted based on the method proposed in [30]. Next, a DWT-based algorithm is proposed for hiding the encrypted biometric signal to the host video object. The proposed algorithm hides the encrypted information into the largest-value qualified significant wavelet trees (QSWTs) of energy-efficient pairs of subbands. Compared to other related schemes, the incorporated approach has the following advantages [31]. (a) It is one of the most efficient algorithms of the literature that better support robust hiding of visually recognizable patterns, (b) it is hierarchical and has multiresolution characteristics, (c) the embedded information is hard to detect by the human visual system (HVS), and (d) it is among the best known techniques with regards to survival of hidden information after image compression.

More specifically, initially the extracted host object is decomposed into two levels by the separable 2-D wavelet transform, providing three pairs of subbands (HL_2, HL_1), (LH_2, LH_1), and (HH_2, HH_1). Afterwards, the pair of subbands with the highest energy content is detected, and a QSWTs approach is incorporated [32] in order to select the coefficients where the encrypted biometric signal should be casted. Finally, the signal is redundantly embedded to both subbands of the selected pair, using a nonlinear energy-adaptable insertion procedure. Differences between the original and the stego-object are imperceptible to the HVS while biometric signals can be retrieved even under compression and transmission losses. Experimental results exhibit the efficiency and robustness of the proposed scheme, an overview of which is provided in Figure 1.

The rest of this paper is organized as follows. In Section 2, a short description of QSWTs together with the essential definitions is provided. In Section 3, the chaotic encryption scheme is analyzed while Section 4 discusses the proposed biometrics hiding method. Experimental results are given in Sections 5 and 6 concludes this paper.

2. Qualified Significant Wavelet Trees (QSWTs)

By applying the DWT once to an image, four parts of high, middle, and low frequencies (i.e., LL_1, HL_1, LH_1, HH_1) are produced, where subbands HL_1, LH_1, and HH_1 contain the finest scale wavelet coefficients. The next coarser scale wavelet coefficients can be obtained by decomposing and critically subsampling subband LL_1. This process can be repeated several times, based on the specific application. Furthermore, the original image can be reconstructed using the IDWT. In the proposed biometrics hiding scheme, coefficients with local information in the subbands are chosen as the target coefficients for inserting a fingerprint image. The coefficients' selection is based on the QSWT derived from EZW [33], and the basic definitions follow.

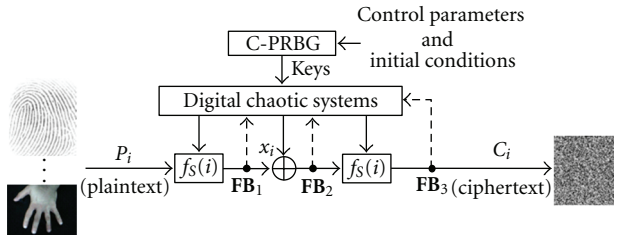


Figure 2: The encryption module.

Firstly, a parent-child relationship is defined between wavelet coefficients at different scales, corresponding to the same location. Excluding the highest frequency subbands (i.e., HL_1, LH_1, and HH_1), every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients corresponding to the same spatial location at the next finer scale of similar orientation are called children. For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants.

Definition 1. A wavelet coefficient $x_n(i, j) \in D$ is a parent of $x_{n-1}(p, q)$, where D is a subband labeled HL_n, LH_n, HH_n, $p = i * 2 - 1 \mid i * 2$, $q = j * 2 - 1 \mid j * 2$, $n > 1$, $i > 1$ and $j > 1$.

Definition 2. If a wavelet coefficient $x_n(i, j)$ at the coarsest scale and its descendants $x_{n-k}(p, q)$ satisfy $|x_n(i, j)| < T$, $|x_{n-k}(p, q)| < T$, for a given threshold T, then they are called wavelet zerotrees, where $1 < k < n$.

Definition 3. If a wavelet coefficient $x_n(i, j)$ at the coarsest scale satisfy $|x_n(i, j)| > T$, for a given threshold T, then $x_n(i, j)$ is called a significant coefficient.

Definition 4. If a wavelet coefficient $x_n(i, j) \in D$ at the coarsest scale is a parent of $x_{n-1}(p, q)$, where D is a subband labeled HL_n, LH_n, HH_n, satisfy $|x_n(i, j)| > T_1$, $|x_{n-1}(p, q)| > T_2$ for given thresholds T_1 and T_2, then $x_n(i, j)$ and its children are called a *QSWT*.

3. The Chaotic Encryption Scheme

Since the process of hiding secret content within host files does not provide maximum security, in this paper each biometric signal is initially encrypted before hiding. Encryption is achieved by the proposed chaotic cryptographic module, an overview of which is given in Figure 2. The subsystem consists of a chaotic pseudo-random bit generator and a chaos-based cipher module. Details are provided in the following subsections.

3.1. Keys Generation Based on C-PRBG. In most secure cryptographic schemes, the security of the encrypted content mainly depends on the size of the key. In our system, for each biometric signal a different key is used, which has a size of 256 bits, leading to a symmetric cipher. Each key is generated by a chaotic pseudo-random bit generator (C-PRBG). C-PRBGs based on a single chaotic system can be insecure, since the produced pseudorandom sequence may expose some information about the employed chaotic system [34]. For this reason, in this paper, we propose a PRBG based on a triplet of chaotic systems, which can provide higher security than other C-PRBGs [35], as three chaotic systems are employed. The basic idea of the C-PRBG is to generate pseudo-random bits by mixing three different and asymptotically independent chaotic orbits.

Towards this direction, let $F_1(x_1, p_1)$, $F_2(x_2, p_2)$ and $F_3(x_3, p_3)$, be three different 1-D chaotic maps:

$$\begin{aligned} x_1(i + 1) &= F_1(x_1(i), p_1), \\ x_2(i + 1) &= F_2(x_2(i), p_2), \\ x_3(i + 1) &= F_3(x_3(i), p_3), \end{aligned} \tag{1}$$

where p_1, p_2, and p_3 are control parameters, $x_1(0)$, $x_2(0)$, and $x_3(0)$ are initial conditions and $\{x_1(i)\}$, $\{x_2(i)\}$, $\{x_3(i)\}$ denote the three chaotic orbits. Then a pseudo-random bit sequence can be defined as

$$k(i) = \begin{cases} 1, & F_3(x_1(i), p_3) > F_3(x_2(i), p_3) \\ k(i-1), & F_3(x_1(i), p_3) = F_3(x_2(i), p_3) \\ 0, & F_3(x_1(i), p_3) < F_3(x_2(i), p_3). \end{cases} \tag{2}$$

According to this scheme, the generation of each bit of a key is controlled by the orbit of the third chaotic system, having as initial conditions the outputs of the other two chaotic systems.

3.2. The Encryption Module. After generating a pseudo-random key for each biometric signal, the cipher module is activated. Before encryption, the samples of each biometric signal are properly ordered. In case of 1-D signals (e.g., voice), the order is the same as the sequence of samples while in 2-D signals (e.g., fingerprint image) pixels are scanned from top-left to bottom-right, providing plaintext pixels P_i. Next, we take into consideration the fact that multiple iterations of chaotic functions lead to slow ciphers while a small number of iterations may raise security problems, so that the encryption algorithm is both fast and secure [35]. In order to make possible a single iteration of the chaotic systems while maintaining high security standards, the proposed scheme combines a simple chaotic stream cipher and two simple chaotic block ciphers (with time variant S-boxes) to implement a complex product cipher.

Considering Figure 2, the operation of the cipher module can be described as follows: assume that P_i and C_i represent the ith plaintext and ith ciphertext samples, respectively, (both in n-bit formats). Then the encryption procedure is defined by

$$C_i = f_S(\{f_S(P_i, i) \oplus x_i\}, i), \tag{3}$$

```
t = 0
QSWT[t] = ∅
For i = 1 to N_P2
  For j = 1 to M_P2 /*M_P2 × N_P2 is the size of subband LH_2*/
   If x_2(i, j) ≥ T_1
          If {x_1(2 ∗ i − 1, 2 ∗ j − 1) ≥ T_2 and x_1(2 ∗ i − 1, 2 ∗ j) ≥ T_2
          And x_1(2 ∗ i, 2 ∗ j − 1) ≥ T_2 and x_1(2 ∗ i, 2 ∗ j) ≥ T_2}
           or {[x_1(2 ∗ i − 1, 2 ∗ j − 1) + x_1(2 ∗ i − 1, 2 ∗ j) + x_1(2 ∗ i, 2 ∗ j − 1) + x_1(2 ∗ i, 2 ∗ j)]/4 ≥ T_2}
          QSWT[t] = {x_2(i, j), x_1(2 ∗ i − 1, 2 ∗ j − 1), x_1(2 ∗ i − 1, 2 ∗ j), x_1(2 ∗ i, 2 ∗ j − 1), x_1(2 ∗ i, 2 ∗ j)}
       t = t + 1
      End If
    End If
  End For j
End For i
```

Algorithm 1: Algorithm for QSWTs detection.

where symbol $\oplus$ represents the XOR function, $f_S(\cdot, i)$ are time-variant $n \times n$ S-boxes (bijections defined on $\{0, 1, \ldots, 2^n - 1\}$) and x_i is produced from the states of three chaotic functions. Here, the f_S are also pseudorandomly controlled by the chaotic functions. The secret key provides the initial conditions and control parameters of the employed chaotic systems. The increased complexity of the proposed cipher against possible attacks is due to the mixed feedback (internal and external): $f_S(P_i, i)$ at $\mathbf{FB}_1$, $f_S(P_i, i) \oplus x_i$ at $\mathbf{FB}_2$ and ciphertext feedback C_i at $\mathbf{FB}_3$, which lead the cipher to acyclic behavior.

The procedure is terminated after all ordered signal samples are enciphered, providing the final encrypted biometric signal. This encrypted signal is then used by the hiding module.

3.3. The Decryption Module. The decryption module receives at its input a vector of enciphered signal samples, the initial control parameters and initial conditions for the triplet of chaotic maps (C-PRBG module), and the initial cipher value C_0 (used at the first feedback).

Afterwards, the digital chaotic systems produce the same specific values used during encryption, but now for decryption purposes. The procedure is terminated after the final sample is decrypted and all decrypted samples are reordered (in case of 2D signals), to provide the initial biometrics signal.

4. The Proposed Biometrics Hiding Method

In the proposed biometrics hiding method, one of the initial steps includes detection of the QSWTs for a pair of subbands of the host video object. Towards this direction, let us assume that the host video object is decomposed into two levels using the DWT to provide three pairs of subbands: $P_1 : (HL_2, HL_1)$, $P_2 : (LH_2, LH_1)$, and $P_3 : (HH_2, HH_1)$. In this paper, and after extensive experimentation, just two levels are used, where 1 to 4 levels' decomposition has been examined. According to our findings, the best tradeoff between complexity and robustness was provided for 2 levels.

Next, in the proposed scheme, the selected pair contains the highest energy content compared to the other two pairs, that is: select $P_i : E_{Pi} = \max(E_{P1}, E_{P2}, E_{P3})$, where

$$E_{Pk} = \sum_{i=1}^{M_{Pk}} \sum_{j=1}^{N_{Pk}} [x_2(i, j)]^2 + \sum_{p=1}^{2M_{Pk}} \sum_{q=1}^{2N_{Pk}} [x_1(i, j)]^2, \quad k = 1, 2, 3 \tag{4}$$

with $x_2(i, j) \in R$, $R = \{HL_2\ LH_2, HH_2\}$, $x_1(p, q) \in S$, $S = \{HL_1, LH_1, HH_1\}$, and $M_{Pk} \times N_{Pk}$ is the size of one of the subbands at level 2.

4.1. The Hiding Strategy. After selecting the pair of subbands containing the highest energy content, QSWTs are found for this pair, and the encrypted biometric signal is embedded by modifying the values of the detected QSWTs. Let us assume, without loss of generality, that pair $P_2 : (LH_2, LH_1)$ is selected. Initially, the threshold values of each subband are estimated as

$$T_1 = \frac{1}{N_{P2} * M_{P2}} * \sum_{i=1}^{M_{P2}} \sum_{j=1}^{N_{P2}} (x_2(i, j)), \quad x2(i, j) \in LH_2$$

$$T2 = \frac{1}{2N_{P2} * 2M_{P2}} * \sum_{p=1}^{2M_{P2}} \sum_{q=1}^{2N_{P2}} (x_1(i, j)), \quad x1(i, j) \in LH_1. \tag{5}$$

Next, the QSWTs are detected according to Algorithm 1.

Afterwards, summation of the coefficients of QSWT$[i]$ for $i = 0$ to t is calculated, and if the encrypted biometric signal is of size $a \times b$ (in case of 2-D signals), then the top $a \times b$ QSWTs (based on the summation results) are selected for embedding the signal. For this reason, initially, the gray level values of the encrypted biometric signal are sorted in descending order, producing a gray-levels vector. Then for $i = 1$ to $a \times b$ the coefficients $w(k, l)$ of the gray-levels matrix are embedded as follows:

$$x_2'(i, j) = x_2(i, j) * (1 + c_2 * w(k, l)), \tag{6}$$

where $x_2(i, j) \in LH_2$, c_2 is a scaling constant that balances unobstructedness and robustness, and $x_2'(i, j)$ is a coefficient of the LH_2 subband of the stego-object. This nonlinear insertion procedure is similar to [36] and adapts the message to the energy of each wavelet coefficient. Thereby, when $x_2(i, j)$ is small, the embedded message energy is also small to avoid artifacts while when $x_2(i, j)$ is large, the embedded message energy is increased for robustness. Similarly, for the coefficients of subband LH_1, we have

$$x_1'(i, j) = x_1(i, j) * (1 + c_1 * w(k, l)), \tag{7}$$

where $x_1(i, j) = \max\{x_1(2*i-1, 2*j-1), x_1(2*i-1, 2*j), x_1(2*i, 2*j-1), x_1(2*i, 2*j)\}$.

Finally, the 2-D IDWT is applied to the modified and unchanged subbands to form the stego-object.

4.2. Message Recovery. Considering that the stego-object (or a distorted version of it) has reached its destination, the encrypted biometric signal is initially extracted by following a reverse (to the embedding method) process. Towards this direction, let us assume that the recipient of the stego-object has also received the size of the encrypted 2-D biometric signal ($a \times b$), the scaling constants (c_1, c_2), and possesses the original host video object. Then the following steps are performed in the recipient's side.

Step 1. Initially, the received stego-object X' and original video object X, which we assume that every authentication authority could have locally stored or securely obtained for example, from a central authentication database, are decomposed into two levels with seven subbands using the DWT,

$$\begin{aligned} Y &= \mathrm{DWT}(X) \\ \mathrm{Y}' &= \mathrm{DWT}(X'). \end{aligned} \tag{8}$$

Step 2. Using the size $a \times b$, the embedded positions are detected by following the hiding process described in Section 4.1. Then the coefficients of subband LH_2 (LH_1) of Y are subtracted from the coefficients of subband LH_2 (LH_1) of Y', and the result is scaled down by the value of coefficient of LH_2 (LH_1) of Y, multiplied by $c_2(c_1)$.

$$\begin{aligned} &\text{For } i = 1 \text{ to } a \times b \\ &w_i^{(2)} = \frac{x'^{(2)}_i - x_i^{(2)}}{x_i^{(2)} * c_2} \\ &w_i^{(1)} = \frac{x'^{(1)}_i - x_i^{(1)}}{x_i^{(1)} * c_1} \end{aligned} \tag{9}$$

Step 3. The resulting hidden message coefficients $w_i^{(2)}$ and $w_i^{(1)}$ are averaged and rearranged to provide the encrypted biometric signal.

Step 4. The original biometric signal is recovered by decrypting the enciphered signal (see Section 3.3).

Here, it should be mentioned that if the same video object X is used for every authentication attempt, the scheme may become vulnerable to attacks. In order to confront this problem, the sender and receiver may share multiple video objects (poses) for each user. In each authentication session, the sender may select one pose and inform the receiver of the selected pose's ID. This is a methodology more resistant to attacks, which can become even more efficient if new poses of the users are periodically collected.

5. Experimental Results

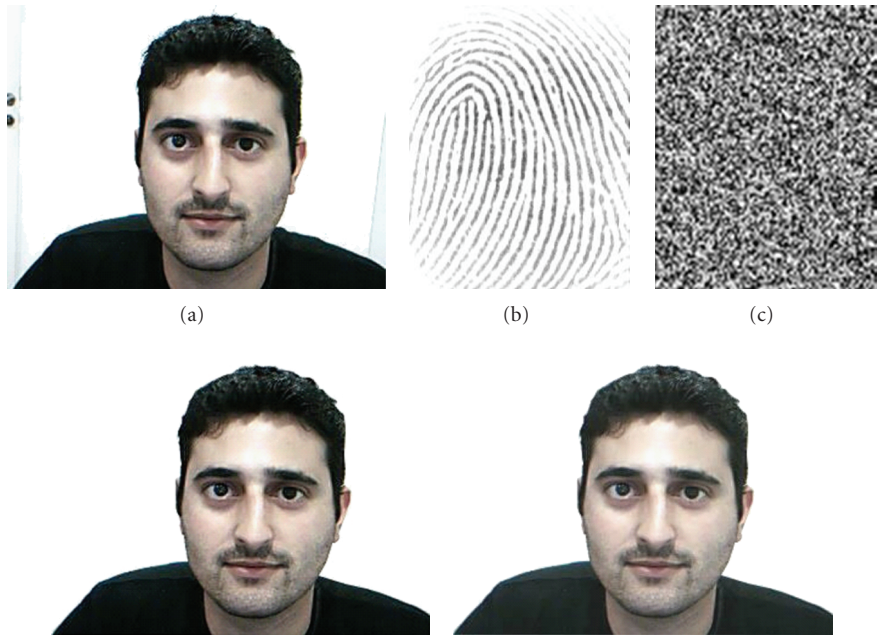
For evaluation purposes, the proposed video-objects oriented biometric signals hiding scheme is examined in terms of security and efficiency. In particular, the database of the POLY-BIO project [37] was used, which contains more than 1500 biometric signals, 300 of which are fingerprints. The authentication setting, which focused on fingerprints, was simulation-based and included three different scenarios that are described in the following paragraphs. The general methodology included (a) extraction of the host video object from a videoconference image and detection of the QSWTs to embed the encrypted signal, (b) encryption of the fingerprint, (c) embedding of the encrypted signal to the host video object, (d) compression of the final content and simulated noisy transmission, (e) decompression, and extraction of the encrypted signal, (f) decryption and (g) authentication.

In particular, for presentation purposes the proposed, scheme is applied to the images depicted in Figures 3(a) and 4(a), where each frame is of size 630×840 pixels. The respective 2-D fingerprint signals for these two persons are shown in Figures 3(b) and 4(b). Their size is 106×90 pixels.

Initially the images are analyzed according to the method proposed in [30], and the two extracted host video objects are presented in Figures 3(d) and 4(d). Afterwards, the encryption algorithm is activated for enciphering each biometric signal. In our experiments, the three chaotic maps that are incorporated (both in the C-PRBG module and the cipher module) are piecewise linear chaotic maps (PWLCMs) of the form:

$$F(x, p) = \begin{cases} \dfrac{x}{p}, & x \in [0, p) \\ \dfrac{x - p}{((1/2) - p)}, & x \in \left[p, \dfrac{1}{2}\right] \\ F(1 - x, p), & x \in \left(\dfrac{1}{2}, 1\right], \end{cases} \tag{10}$$

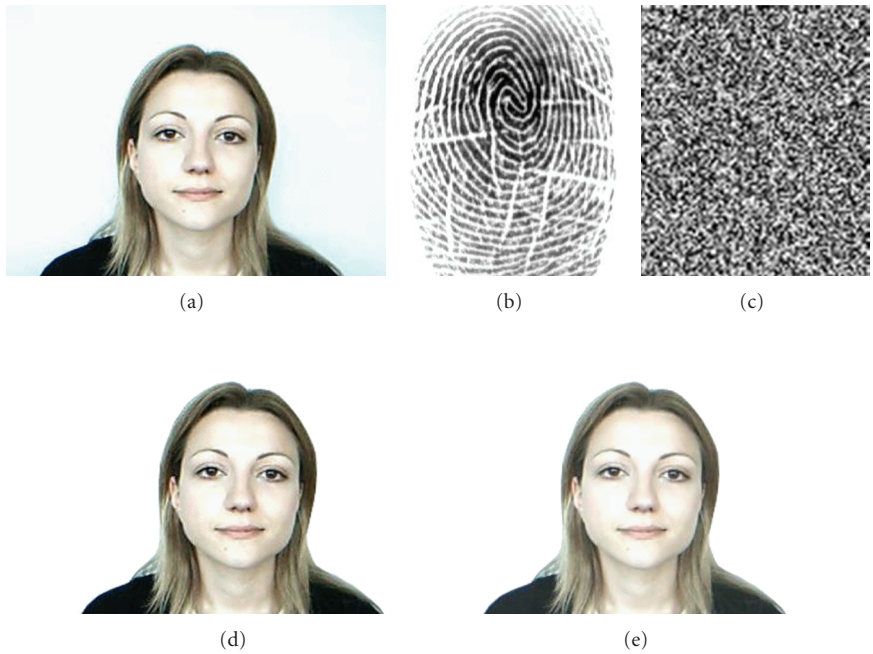
where $0 < P < 1/2$, with initial control parameters set as $p_1 = 0.15$, $p_2 = 0.27$, and $p_3 = 0.43$. The final encrypted biometric signals are depicted in Figures 3(c) and 4(c) (in 2-D form). As it can be observed, the encrypted content looks completely random and does not provide any clues relevant to the content or minutiae distribution. In particular, this fact is further illustrated in Figures 5(a) and 5(b), where the histograms of Figures 3(c) and 4(c) are presented, respectively. Both histograms approximate the histogram of



(a) (b) (c)

(d) (e)

Figure 3: (a) The first videoconference frame containing a man, (b) the fingerprint of the man of Figure 3(a), (c) encrypted biometric signal of Figure 3(b), (d) the automatically extracted man video object, (e) the stego-object containing the encrypted biometric signal of Figure 3(c).



(a) (b) (c)

(d) (e)

Figure 4: (a) The second videoconference frame containing a woman, (b) the fingerprint of the woman of Figure 4(a), (c) encrypted biometric signal of Figure 4(b), (d) the automatically extracted woman video object, (e) the stego-object containing the encrypted biometric signal of Figure 4(c).

a table with random values. This is a very important security merit, as the encrypted biometric signals approximate the statistics of a randomly generated 2-D signal, independently of the plaintext.

Here, it should be mentioned that due to the acyclic behavior of the encryption module, the output keystream has all the merits of one-time pads, and thus it is very difficult to cryptanalyze, using statistical attacks. For this reason

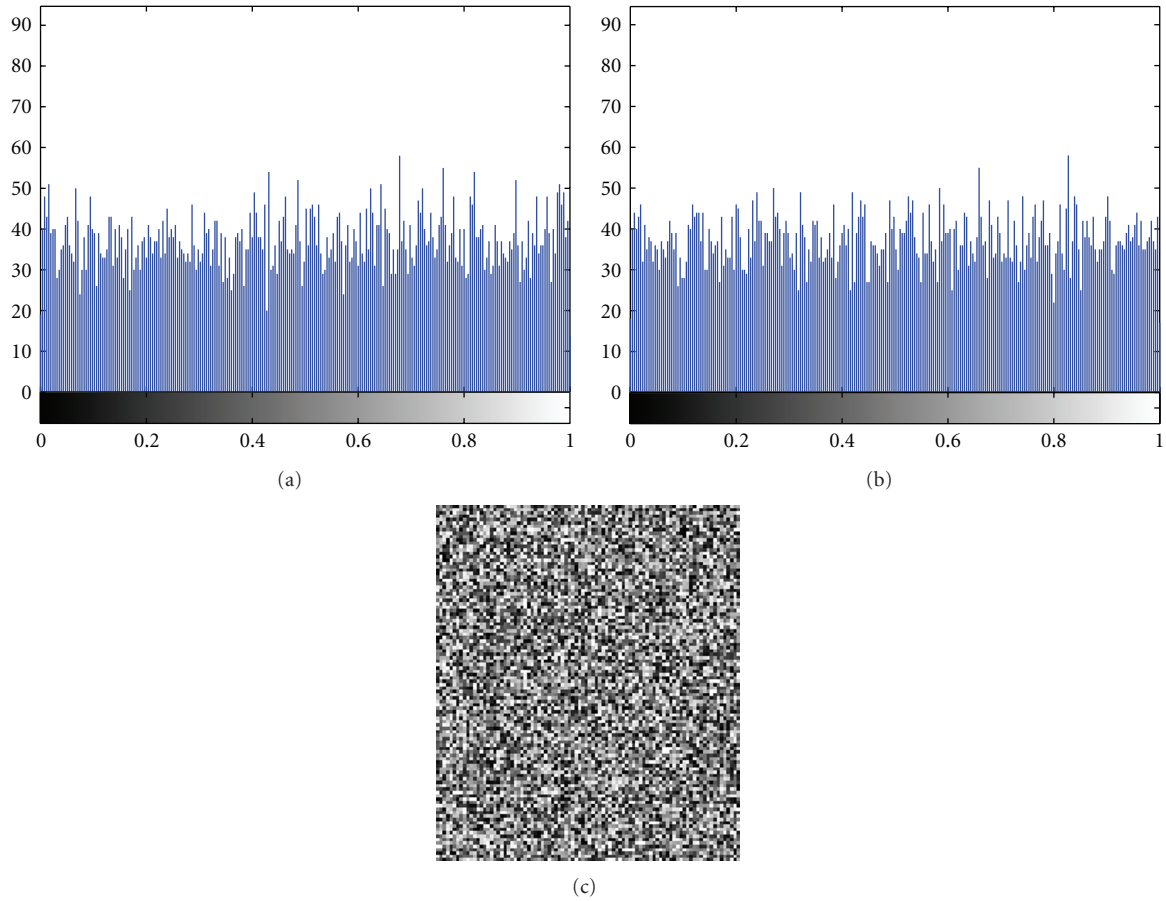


Figure 5: (a) Histogram of encrypted biometric signal of Figure 3(c), (b) histogram of encrypted biometric signal of Figure 4(c), and (c) decryption of pattern of Figure 3(c) using a key that differs by one bit.

some tests have been performed to check the security of the encryption system. Towards this direction, let us assume that an unauthorized user knows the QSWTs, where the encrypted biometric signal of Figure 3(c) is hidden and tries to decrypt it by, brute force attack. Let us also assume that he has also obtained a rearranged version of the image, where all pixels are on proper position. If the exact key is used, then the content can be decrypted. However, even if the key differs by just one bit, the content will not be decrypted as it can be seen in Figure 5(c).

Next, the robustness of the proposed biometrics hiding method has been extensively evaluated under various simulation tests, performed using MATLAB. In particular, during experimentation, the host video objects of Figures 3(d) and 4(d) were used, in which, the encrypted biometric signals of Figures 3(c) and 4(c) were hidden, respectively. Then according to the size of the encrypted biometric signals, the top 106×90 QSWTs were selected for both host video objects to embed the signals. For simplicity, in the performed experiments, c_1 and c_2 were fixed in all frequency bands and were chosen to be $c_1 = 0.15$ and $c_2 = 0.2$. The stego-objects can be seen in Figures 3(e) and 4(e), providing PSNRs of 46.17 and 45.44 dB, respectively. As it can be observed, the embedded encrypted biometric signals have caused imperceptible changes to the host video objects.

Afterwards, since the proposed system is designed for user authentication under error-prone transmissions, the case of mobile networks is further studied as a typical example, and the system's resistance is investigated under different JPEG compression ratios and various bit error rates (BERs). More particularly, compression ratios between 1.6 and 7.1 were used while BERs took values between 3×10^{-4} and 3×10^{-3}, considering that typical average BERs for cellular mobile radio channels are in the interval $[10^{-4}\ 10^{-3}]$ [38]. In our simulations, we assume unreliable connectionless mobile transmission protocols, where errors occur only in the data field of each packet (headers remain intact). Furthermore, here it should be mentioned that even though the majority of mobile applications use "closed" image formats, there are some that use JPEG (e.g., Image Converter by AOXUE.studio or Image Converter 5th v3.0.0 for Symbian s60 5th edition), while the market tendency for JPEG-enabled applications is increasing. Finally, in all experiments, fingerprint authentication is based on the minutiae string matching algorithm presented in [39].

Under these assumptions, in order to fully illustrate the authentication capabilities of the proposed scheme and to compare it to another steganographic method, three different scenarios have been investigated. In the first scenario (SC1), the original biometric data is compressed and transmitted

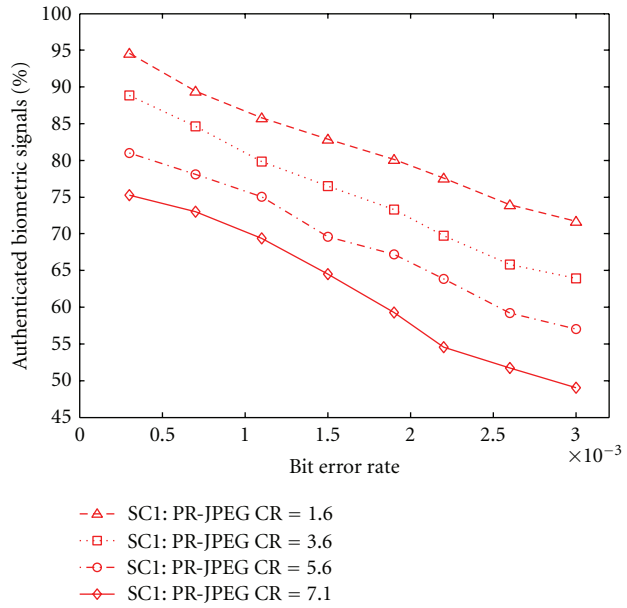


Figure 6: First Scenario. Authentication of 112 biometric signals, under four different JPEG compression ratios and various BERs. SC1: first scenario. PR: proposed scheme. CR: compression ratio.

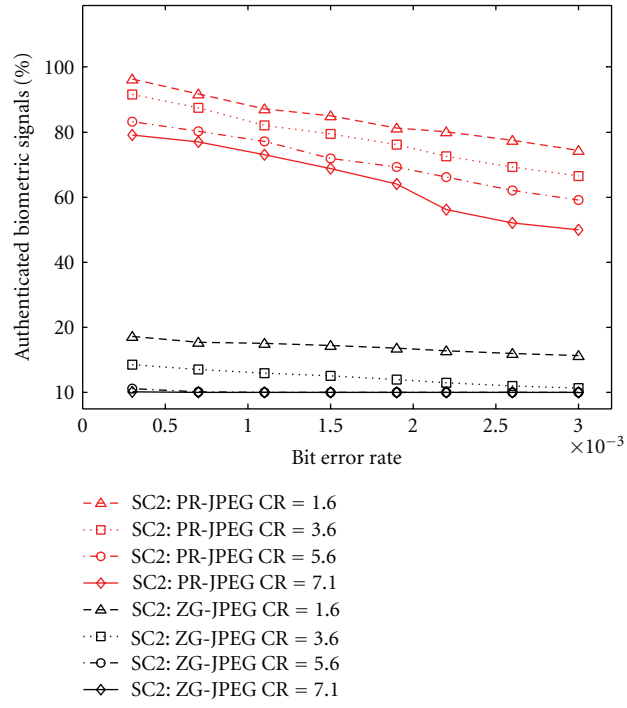


Figure 7: Second scenario. Biometric signals authentication for 112 stego-objects, under four different JPEG compression ratios and various BERs. SC2: second scenario. PR: proposed scheme (red). ZG: Scheme by Zhang et al. (black). CR: compression ratio.

over error-prone channels without being encrypted or hidden. In the second scenario (SC2), the original biometric data is hidden into their respective host-objects using either the proposed method (PR) or another interesting steganographic method (ZG), introduced by Zhang et al. [40]. The final content is compressed and transmitted over error-prone channels. In the third scenario (SC3), which is the full usage scenario of the proposed scheme, the original biometric data is initially encrypted, and now, in contrast to SC2, the encrypted data is hidden to the respective host-objects. The final stego-objects are compressed and transmitted. In all three scenarios, the authentication accuracy is examined.

In particular in Figure 6, the authentication results of SC1 for more than 100 biometric signals are presented. In this case, where the original biometric signal is not hidden to a host-object, the average authentication rate was 72.07%. Furthermore, as it can be observed, compression increase has a more significant impact on authentication results compared to BER increase. This is expected, since distortion due to BER is local while compression has more global effects. In Figure 7, the authentication results of SC2 for the same 112 biometric signals, hidden in their respective stego-objects, is presented, both for the proposed scheme (PR) and the scheme by Zhang et al. (ZG). In this case, the average authentication rate of PR is 74.62 while ZG provides a rate of 4.67%. It is clear that capacity-efficient schemes such as Zhang's cannot survive to signal distortions. This is typical if we focus on the details of such methods. In Zhang's method, in the first layer of the embedding, one secret bit is inserted into each host pixel. If a secret bit is identical to the LSB of the corresponding pixel, no modification is made. Otherwise, the pixel value should be added or

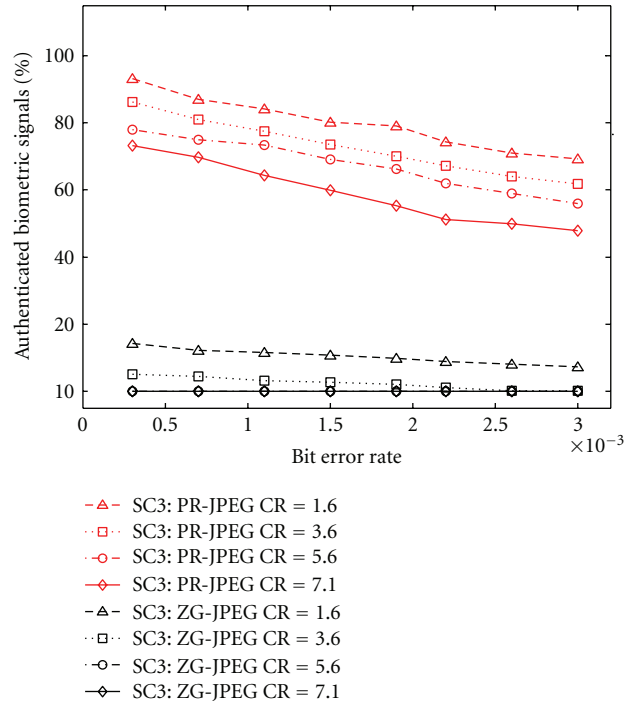


Figure 8: Third scenario. Biometric signals authentication for 112 stego-objects, under four different JPEG compression ratios and various BERs. SC3: third scenario. PR: proposed scheme (red). ZG: Scheme by Zhang et al. (black). CR: compression ratio.

Table 1: Biometric signal retrieval results for the stego-object of Figure 3(e), under different combinations of compression ratios and BERs.

Initial fingerprint	JPEG compression	Factor	BER1 (3×10^{-4})	BER2 (1×10^{-3})	BER3 (3×10^{-3})
	Ratio: 2.6	PSNR (dB)	39.9	38.4	36.1
		Retrieved fingerprint			
	Ratio: 5.1	PSNR (dB)	37.7	35.9	34.2
		Retrieved fingerprint			

Table 2: Biometric signal retrieval results for the stego-object of Figure 4(e), under different combinations of compression ratios and BERs.

Initial fingerprint	JPEG compression	Factor	BER1 (3×10^{-4})	BER2 (1×10^{-3})	BER3 (3×10^{-3})
	Ratio: 2.6	PSNR (dB)	39.1	37.3	35.4
		Retrieved fingerprint			
	Ratio: 5.1	PSNR (dB)	36.9	35.3	33.9
		Retrieved fingerprint			

subtracted by one, and the choice of addition or subtraction will be determined in the second layer embedding, thus both adding/subtracting change the LSB. If a pixel value is odd, adding and subtracting one flips and keeps the second LSB, respectively. On the other hand, if a pixel value is even, the two operations cause opposite results in the second LSB. Thus the hidden information is hosted by the LSBs of the final content, which are very sensitive to signal distortions.

Now, regarding SC3 (full usage scenario), the experiment is repeated for the same 112 biometric patterns, however, in this case the original signals are firstly encrypted and then hidden to host-objects. Results of the retrieved biometric signals for video objects of Figures 3(e) and 4(e) are provided in Tables 1 and 2, respectively. As it can be observed, the retrieved biometric signals are visually apprehensible for the examined combinations of compression ratios and BERs.

In Figure 8, the authentication results of SC3 is presented, both for the proposed scheme (PR) and the scheme by Zhang et al. (ZG). In this case, the average authentication rate of PR is 69.7 while ZG's rate is 3.18%. Considering the 3 different scenarios, it is observed that when the original biometric signal is compressed and transmitted (SC1), the authentication rate is higher than in case of encryption (SC3). This is expected, since an encrypted by a one-time pad signal is less resistant to the plain signal. One encrypted pixel error usually produces more significant visual artifacts during decryption. Furthermore, from the authentication side of view, the best results were accomplished for the settings of SC2. However, even though SC3 is not the most efficient in terms of authentication performance or complexity, compared to SC1 and SC2, it is the most secure, a merit that may make it the first choice in real-world applications. Finally, the proposed scheme is more robust to signal distortions, compared to typical steganographic schemes that are based on LSBs' manipulation.

6. Conclusions

Biometric signals enter more and more into our everyday lives, since governments resort to their use in accomplishing crucial procedures (e.g., citizen authentication). Thus there is an urgent need to further develop and integrate biometric authentication techniques into practical applications.

Towards this direction, in this paper, the domain of biometrics authentication over error-prone networks has been examined. Since steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, other than providing results that are imperceptible to human visual system, it also outputs a stego-object that can resist different signal distortions. Experimental results on the database of POLY-BIO project [37], which contains more than 1500 biometric signals, illustrate the performance of the proposed system. Experiments have been designed to fulfill the requirements of three different scenarios. In the first scenario (SC1), the original biometric data was compressed and transmitted over error-prone channels without being encrypted or hidden. In the second scenario (SC2), the original biometric data was hidden into their respective host-objects, and the final content was compressed and transmitted over error-prone channels. In the third scenario (SC3), the original biometric data was initially encrypted and hidden into the respective host-objects and the final stego-objects were compressed and transmitted. All experiments have been performed for JPEG compression and typical BERs of wireless links. By examining the three scenarios, it was found that SC2 provided the highest authentication rate (about 75%). However, even though SC3 did not result into the best authentication scores or lowest complexity, it is the most secure among the three. Finally, the proposed scheme was also compared to a typical steganographic scheme based on LSBs' manipulation, which it outperformed, for the specified signal distortion conditions.

In future research, the effects of compression and mobile transmission of other hidden biometric signals (e.g., voice or iris) should also be examined, or cases of other common signal distortions such as additive noise or image resize operations could be considered. Another very interesting research topic focuses on tackling the problem of lost biometric data. Several techniques could be examined from the areas of image error concealment, region restoration, or region matching. Based on the focus of the first area, the lost biometric data can be concealed from the authentication module, so that it attempts to perform authentication even though parts are missing (maybe parts that do not contain any crucial information, for example, terminations/bifurcations in case of fingerprints). Restoration aims at reproducing lost regions, usually using interpolation techniques. In this case also, if the restored region would not contain crucial information, results could be interesting. Finally, region matching and classification methods can also play an important role in authenticating a partially complete biometric signal.

Acknowledgment

This was funded by the Cyprus Research Promotion Foundation in the framework of PLHRO/0506/04: "POLY-BIO," *Multimodal Biometric Security System*.

References

[1] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[2] N. Haller, "The S/KEY one-time password system," in *Proceedings of the ISOC Symposium on Network and Distributed System Security*, pp. 151–157, 1994.

[3] C.-C. Lee, M.-S. Hwang, and W.-P. Yang, "A flexible remote user authentication scheme using smart cards," *Operating Systems Review*, vol. 36, no. 3, pp. 46–51, 2002.

[4] C. C. Chang and K. F. Hwang, "Some forgery attacks on a remote user authentication scheme using smart cards," *Informatica*, vol. 14, no. 3, pp. 289–294, 2003.

[5] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243–1245, 2003.

[6] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167–169, 2004.

[7] M. Kumar, "Some remarks on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 615–618, 2004.

[8] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Prentice-Hall, Upper Saddle River, NJ, USA, 3rd edition, 2003.

[9] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Workshop Security*, pp. 5–14, 1990.

[10] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[11] R. M. Bolle, J. H. Connell, and N. K. Ratha, *Guide to Biometrics*, Springer, New York, NY, USA, 2004.

[12] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.

[13] M. Ramkumar and A. N. Akansu, "Capacity estimates for data hiding in compressed images," *IEEE Transactions on Image Processing*, vol. 10, no. 8, pp. 1252–1263, 2001.

[14] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, pp. 86–90, 1994.

[15] J. J. K. Ó. Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," in *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, pp. 211–214.

[16] N. F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[17] J. Fridrich, R. Du, and M. Long, "Staganalysis of LSB encoding in color images," in *Proceedings of the IEEE International Conference on Multi-Media and Expo (ICME '00)*, pp. 1279–1282, New York, NY, USA, July-August 2000.

[18] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075–1083, 1999.

[19] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, "Steganography for a low bit-rate wavelet based image coder," in *Proceedings of the IEEE International Conference on Image Processing (ICIP '00)*, vol. 1, pp. 597–600, Vancouver, Canada, 2000.

[20] D. Kundur, Y. Zhao, and P. Campisi, "A steganographic framework for dual authentication and compression of high resolution imagery," in *Proceedings of the IEEE International Symposium on Circuits and Systems*, vol. 2, pp. II1–II4, Vancouver, Canada, May 2004.

[21] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494–1498, 2003.

[22] K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, "Protecting fingerprint data using watermarking," in *Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems (AHS '06)*, pp. 451–456, tur, June 2006.

[23] K. Zebbiche and F. Khelifi, "Region-based watermarking of biometric images: case study in fingerprint images," *International Journal of Digital Multimedia Broadcasting*, vol. 2008, Article ID 492942, 2008.

[24] T. Hoang, D. Tran, and D. Sharma, "Remote multimodal biometric authentication using bit priority-based fragile watermarking," in *Proceedings of the 19th International Conference on Pattern Recognition (ICPR '08)*, pp. 1–4, December 2008.

[25] N. N. Rao, P. Thrimurthy, and B. R. Babu, "A novel scheme for digital rights management of images using biometrics," *International Journal of Computer Science and Network Security*, vol. 9, no. 3, pp. 157–167, 2009.

[26] P. Campisi, "Object-oriented stereo-image digital watermarking," *Journal of Electronic Imaging*, vol. 17, no. 4, Article ID 043024, 2008.

[27] V. Q. Pham, T. Miyaki, T. Yamasaki, and K. Aizawa, "Robust object-based watermarking using feature matching," *IEICE Transactions on Information and Systems*, vol. 91, no. 7, pp. 2027–2034, 2008.

[28] K. S. Ntalianis and S. D. Kollias, "Chaotic video objects encryption based on mixed feedback, multiresolution decomposition and time-variant S-boxes," in *Proceedings of the International Conference on Image Processing (ICIP '05)*, vol. 2, pp. 1110–1113, Genova, Italy, September 2005.

[29] S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," in *Real-Time Imaging VI*, vol. 4666 of *Proceedings of SPIE*, pp. 149–160, January 2002.

[30] A. Doulamis, N. Doulamis, K. Ntalianis, and S. Kollias, "An efficient fully unsupervised video object segmentation scheme using an adaptive neural-network classifier architecture," *IEEE Transactions on Neural Networks*, vol. 14, no. 3, pp. 616–630, 2003.

[31] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875–882, 2001.

[32] K. S. Ntalianis, N. D. Doulamis, A. D. Doulamis, and S. D. Kollias, "Automatic stereoscopic video object-based watermarking using qualified significant wavelet trees," in *Proceedings of the International Conference on Consumer Electronics (ICCE '02)*, pp. 188–189, Los Angeles, Calif, USA, June 2002.

[33] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3445–3462, 1993.

[34] V. A. Protopopescu, R. T. Santoro, and J. S. Tollover, "Fast and secure encryption—decryption method based on chaotic dynamics," US Patent No. 5479513, 1995.

[35] S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," in *Real-Time Imaging VI*, vol. 4666 of *Proceedings of SPIE*, pp. 149–160, January 2002.

[36] X. Wu, W. Zhu, Z. Xiong, and YA. Q. Zhang, "Object-based multiresolution watermarking of images and video," in *Proceedings of the IEEE Internaitonal Symposium on Circuits and Systems*, vol. 1, pp. 545–550, Geneva, Switzerland, May 2000.

[37] A. Kounoudes, N. Tsapatsoulis, Z. Theodosiou, and M. Milis, "POLYBIO: multimodal biometric data acquisition platform and security system," in *Biometrics and Identity Management*, B. Schouten, N. C. Juul, A. Drygajlo, and M. Tistarelli, Eds., pp. 216–227, Springer, Berlin, Germany, 2009.

[38] V. Weerackody, C. Podilchuk, and A. Estrella, "Transmission of JPEG-coded images over wireless channels," *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 111–125, 1996.

[39] M. Kaur, M. Singh, A. Girdhar, and P. S. Sandhu, "Fingerprint verification system using minutiae extraction technique," in *Proceedings of World Academy of Science, Engineering and Technology*, vol. 36, pp. 497–502, December 2008.

[40] X. Zhang, W. Zhang, and S. Wang, "Efficient double-layered steganographic embedding," *Electronics Letters*, vol. 43, no. 8, pp. 482–483, 2007.