Güvenilir Biyometrik Kıyım Yöntemi
Trustworthy Biometric Hashing Method

Cagatay Karabat[1,2],Hakan Erdogan[1]

1. Muhendislik ve Doga Bilimleri Fakultesi, Sabanci Universitesi, Istanbul, Turkiye
2. TUBITAK UEKAE, Kocaeli, Turkiye

cagatay@uekae.tubitak.gov.tr, haerdogan@sabanciuniv.edu

Özetçe

Bu bildiride yeni bir biyometrik kıyım yöntemi önerdik. Bir parola tarafından üretilen rastgele izdüşüm matrisini yüz imgelerinden çıkartılan özellikler yerine doğrudan yüz imgesine uyguladık ve literatürdeki yöntemleri geliştirdik. Biyometrik doğrulama sistemlerinde, mahremiyeti korurken istenilen doğruluk oranına ulaşmayı amaçladık. Doğrulama işlemini kıyım alanında yaparak tersine çevrilemezliği temin ettik. Bununla birlikte, sadece parola değiştirip yeni bir kıyım değeri elde ederek iptal edilebilir biyometrik özelliğini sağladık. Carnegie Mellon University yüz veritabanında sıfır eşit hata oranı (EHO) elde ettik. Ayrıca, saldırganlar parola ve rastsal sayı üretecini (RSÜ) ele geçirse bile, 0.0061 EHO'nı elde ettik. Bunun yanısıra, önerilen sistemin çeşitli algılayıcı ve çevresel kaynaklı bozulumlar karşısında dayanılıklığını test ettik. Tüm bozulumlarda hatanın normu EHO'nında elde edilen optimum eşik değerinden düşüktür.

Abstract

In this paper, we propose a novel biometric hashing method. We employ a password-generated random projection matrix applied to the face images directly instead of applying to the features extracted from face images and improve the methods in the literature. We aim to preserve privacy while achieving desirable accuracy in a biometric verification system. We do the verification in the hash domain and ensure irreversibility. In addition, we can get a new hash value by only changing the password which ensures cancelable biometrics property. We achieve zero equal error rate (EER) on Carnegie Mellon University face database. Furthermore, we achieve an EER of 0.0061, even if the attackers compromise the password and the random number generator. Besides, we test robustness of the proposed system against possible degradations due to sensor and environment imperfections. The norm of error is below optimum threshold obtained at EER for all distortions.

1. Giriş

Son yıllarda, biyometrik veriler kredi kartları ve kimlik kartları gibi kimlik doğrulaması gerektiren birçok yerde kullanılmaktadır. Bu sistemlerde, biyometrik verilerin veritabanında yada akıllı kartta açık metin halinde saklanması çeşitli güvenlik problemlerini doğurmaktadır [1]-[3]. Yetkisi bulunmayan kullanıcılar (saldırgan) biyometrik verileri ele geçirirlerse doğrulama sistemine de rahatlıkla çalışmaz hale getirebilirler. Biyometrik veri değiştirilemeyeceği ve yerine yenisi konulamayacağı için yasal kullanıcı kendi biyometrik verisi üzerindeki kontrolünü ömür boyu kaybeder. Bunun yanısıra, biyometrik veriler pek çok mahremiyet problemini de beraberinde getirir.

Bahsi geçen tehditlere karşı akla gelen ilk olarak kriptolojik çözümler gelmektedir. Bu durumda, saldırganın biyometrik verilere erişebilmesi için şifreleme anahtarını ele geçirmesi gerekir [4],[5]. Bu sistemlerin dezavantajı, doğrulamanın şifrelenmiş biyometrik veriler üzerinden yapılamamasıdır. Klasik şifreleme algoritmalarında, açık metin verisindeki bir bitlik değişim bile şifrelenmiş veriyi tamamen değiştirmektedir. Kişi, doğrulama sistemine her girişte aynı veriyi veremediği için bu yöntemler kullanışlı değildir. Doğrulama işlemi açık metin biyometrik veriler üzerinden yapıldığında saldırganın verileri ele geçirme olasılığı yüksektir. Bunların yanısıra, yöntemin şifreleme anahtarını saklama ve yönetme gibi sorunları da mevcuttur.

İptal edilebilir biyometrikler yukarıda bahsi geçen sorunlar için umut vaad edici bir çözüm olabilir. Literatürde, çeşitli biyometrik kıyım (biometic hash) algoritmaları iptal edilebilir biyometrik konusu kapsamında önerilmiştir [6]-[8]. Bu yöntemlerde, önce biyometrik veri bir ön işleme tabi tutulur ve bir özellik vektörü elde edilir. Örneğin, Ngo *et al.* yüz imgelerinden özellik vektörü elde etmek için ana bileşenler analizi (PCA), dalgacık dönüşümü, Fisher doğrusal ayırtaç, ve Fourier-Mellin dönüşümünü kullanmıştır [6]. Lumini and Nanni ise ayrık kosinüs dönüşümü kullanarak parmak izi imgelerinde özellik vektörü elde etmiştir [7]. Sonrasında, elde ettikleri özellik vektörlerine *rastgele izdüşüm* uygulamışlardır. En sonunda, biyometrik imgenin kıyım (hash) değerini hesaplamışlardır. Ngo *et al.* önerdiği sistemin uyguladığı ön işleme göre 0 dan 0.0678'e kadar eşit hata oranları (EHO) elde ettiğini açıklamıştır [6]. Lumini ve Nanni ise kendi sistemlerinin EHO'larının kulladıkları veri tabanına ve parametre seçimine bağlı olarak 0.01 dan 0.183'e kadar değiştiğini belirtmiştir. Diğer taraftan, Kong *et al.* literatürde bahsi geçen sistemlerin, saldırganın gizli anahtarı (parola veya PIN) ve rastgele sayı üretecini (RSÜ) ele geçiremeyeceği varsayımını kullandıklarını vurgulamıştır. Ayrıca, bu sistemlerin EHO'larının ancak bu varsayım altında 0 olabileceğini belirtmiştir [8]. Oysaki, parola ve RSÜ'nin gizli kalabilmesinin mümkün değildir. Günümüzde, birçok saldırgan bunları rahatlıkla ele geçirebilmektedir. Literatürde bahsi geçen sistemlerin performansı gizli anahtar ve/veya RSÜ ele geçirildiği zaman oldukça düşmektedir. [8].

Bu bildiride, biyometrik verilerin güvenlik ve mahremiyet sorunlarını ele aldık. İptal edilebilir biyometrik doğrulama sistemi tasarlamak amacıyla yeni bir biyometrik kıyım algoritması önerdik. Önerilen yöntemin literatürdeki yöntemlerden temel farkı; imgeden elde edilen özellik vektörünü kullanmak yerine rastgele izdüşüm doğrudan imgenin üzerine uyguluyor olmasıdır. Bunun yanısıra,

978-1-4244-4436-6/09/$25.00 ©2009 IEEE

kullandığımız değişik nicemleme yöntemleri biyometrik doğrulama sistemine ekstra güvenlik ve tahmin edilememezlik katmaktadır. Önerilen sistem, Carnegie Mellon üniversitesi (CMU) yüz veri tabanı üzerinde yaptığımız çalışmalarda sıfır EHO'na ulaşmıştır. Bu benzetimlerde, saldırganın biyometrik veri, parola ve RSÜ'ini bilmediği varsayılmıştır. Önerilen sistemin en büyük özelliği; saldırganın hem parolayı hem de RSÜ'ni ele geçirdiği durumlar için yaptığımız benzetimlerde 0.0061 EHO elde etmemizdir. Bu değer [6]-[8] ile karşılaştırıldığında umut vericidir. Diğer taraftan, Kumar *et al.* un önerdikleri ve öz-yüz yönteminden [10] daha iyi sonuç veren "bireysel öz-yüz alt uzay yöntemi" [9], benzetimlerde kullandığımız CMU yüz veritabanında ancak 0.0085 EHO'na ulaşabilmiştir. Böylece, önerilen yönteminin hem bireysel öz-yüz alt uzay yönteminden [9] daha iyi çalıştığı hem de biyometrik verilerin güvenlik ve mahremiyet sorunlarına çözüm olabileceği açıkça görülmektedir.

Önerilen yöntemde, biyometrik verinin kıyım değeri biyometrik imge ve gizli anahtar ile oluşturulmaktadır. Önerilen sistemin avantajları: 1) Hem parola hem de RSÜ'nin ele geçirildiği durumlarda bile güvenlidir, 2) Biyometrik veriler akıllı kartta açık metin halinde tutulmaz, 3) Saldırgan, akıllı kartta varolan biyometrik kıyım değerine ulaşırsa, yasal kullanıcıya yeni bir kıyım değeri verilebilir, 4) Akıllı kartta bulunan biyometrik kıyım değeri kartın sahibi hakkında herhangi bir bilgi vermez; kıyım değeri sözde rastgele bir dizi gibi davranır, 5) Kimlik doğrulama kıyım değerleri üzerinden yapılır, 6) Kıyım değerinden biyometrik veriye ulaşılamaz (geri dönüşümsüzdür). Bunların haricinde, önerilen sistemin başarımını Karar Eğrileri (Receiver Operation Characteristic (ROC)) and EHO grafiklerini kullanarak da gösterdik. Ayrıca, biyometrik algılayıcı ve çevresel etkilerden dolayı oluşan bozulmalara karşı sistemin dayanıklılığını test ettik. Elde edilen benzetim sonuçlarından, önerilen yöntemin bu bozulmalara karşı dayanıklı olduğu anlaşılmaktadır. Bildirinin geri kalanı: Bölüm 2'de biyometrik imge kıyımından bahsedilmiştir. Bölüm3'te önerilen sistem anlatılmıştır. Bölüm 4 te benzetimlere verilerek Bölüm 5 te sonuçlar verilmiştir.

2. Biyometrik İmge Kıyımı

Biyometrik imge kıyım yöntemleri, indeksleme ve iptal edilebilir biyometrikler gibi birçok uygulamada kullanılabilir. Bu yöntemler, kriptolojik kıyım yöntemleri gibi büyük elemanlı bir uzaydan daha az ve sabit elemanlı bir alt uzaya eşleme yapsa da birbirlerinden farklıdırlar. Kriptolojik kıyım yöntemlerinde, girişte oluşacak bir bitlik değişim bile çıkışta tamamen farklı bir değer elde etmemize sebep olduğundan imge tabanlı uygulamalar için elverişli değildir.

2.1. Önerilen Biyometrik Kıyım Yönteminin Özellikleri

I. ***İptal Edilebilirlik ve Değiştirilebilirlik***

Yasal kullanıcı parolasını değiştirmek suretiyle biyometrik verisinin kıyım değerini de değiştirebilir.

II. ***Algısal Dayanıklılık***

Aynı kişiden farklı oturumlarda alınmış biyometrik verilerin kıyım değerleri, belli bir uzaklık ölçevinde çok büyük olasılıkla birbirine yakındır.

III. ***Farklı İmgelere Karşı Duyarlılık***

Önerilen yöntem içerik değişimlerine karşı hassastır.

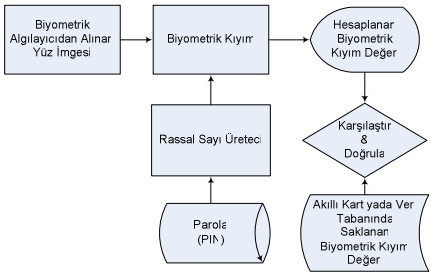
IV. ***Tahmin Edilememezlik ve Geri Çevrilemezlik***

Biyometrik kıyım değeri sözde rastgele bir dizi gibi davranmaktadır. Böylece, tahmin edilemezdir.

3. Önerilen Biyometik Doğrulama Sistemi

Bu bölümde, önerilen biyometrik imge kıyım yöntemine dayalı biyometrik doğrulama sistemini ele alacağız. Öncelikle, bu sisteme kaydolmak isteyen kişinin, bir adet yüz imgesi alınır. Sistem, kişinin gizli anahtarını (parola yada PIN) ve yüz imgesini kullanarak bir kıyım değeri elde eder ve bunu kişinin akıllı kartı içerisine gömer. Herhangi bir kişi sisteme giriş yapmak istediğinde (doğrulama sürecinde); biyometrik algılayıcı kişinin yüz imgesini çeker ve sisteme (sunucu) gönderir. Sonrasında, giriş yapmak isteyen kişi gizli anahtarını girer. Sistem, biyometrik algılayıcıdan gelen imge ile giriş yapmak isteyen kişinin girdiği gizli anahtardan bir kıyım değeri elde eder. Bu değeri, akıllı kartta saklı olan değer ile karşılaştırır. Şekil 1'de görüldüğü gibi, eğer bu iki kıyım değeri arasındaki uzaklığın (Öklit veya Hamming uzaklığı gibi) belirlenmiş eşik değerinden az ise sistem kişiyi doğrular.

Önerdiğimiz sistemde, aynı biyometrik imgeden farklı gizli anahtarlar kullanarak farklı kıyım değerleri elde edebiliriz. Böylece, saldırgan gizli anahtarı ele geçirse bile, yasal kullanıcı için yeni bir gizli anahtar ve kıyım değeri atanabilir. Bunun yanısıra, önerdiğimiz sistem, saldırganın hem gizli anahtarı hem de RSÜ'ini ele geçirdiği durumlarda bile umut vaad edici sonuçlar vermektedir.



*Şekil 1:*Önerilen Biyometrik Doğrulama Sisteminin Genel Şeması

3.1. Önerilen Biyometrik Kıyım Yöntemi

Bu bölümde, rastgele izdüşümlerine dayanan, önerilen biyometrik kıyım yönteminden bahsedeceğiz. Rastgele izdüşüm, basit ve etkili bir boyut indirgeme yöntemidir. Bu yöntem, sütunları birim uzunlukta olan rastgele izdüşüm matrislerini kullanarak, veriyi yüksek boyutlu uzaydan düşük boyutlu uzaya yansıtır. Rastgele izdüşümünün avantajı; hesap hızının yüksek olması ve verinin yapısını büyük bir bozuluma yol açmadan korumasıdır. Johnson and Lindenstrauss teoremi bu yöntem için teorik dayanak sağlamaktadır [12].

Farzedelim, elimizde NxN (benzetimlerde N=64) boyutunda bir yüz imgesi **X** olsun. Öncelikle, bu 2 boyutlu yüz imgesini vektör olarak (lexicographic) sıraladık. Böylece, $1xN^2$ boyutunda bir yüz vektörü $\boldsymbol{x}$ elde ettik.

Sonrasında, yüz vektörü $\boldsymbol{x}$ in boyutunu rastgele izdüşüm matrisini kullanarak azalttık. Bunun için öncelikle JL teoremini sağlayacak şekilde, boyutu N^2xk (benzetimlerde k=256) olan rastgele izdüşüm matrisini **P** oluşturduk. Literatürde JL teoremini sağlamak için çeşitli yöntemler vardır [12]-[14]. Önerdiğimiz yöntemde, kullandığımız rastgele izdüşüm matrisinin elemanları $P(i,j)$, $i = 1,2,..,\ k$ and $j = 1,2,...N^2$, ortalaması sıfır varyansı bir olan Gauss dağılımından bağımsız özdeşçe dağılmış şekilde (iid) örneklenmiştir. Bu rastgele sayılar kişinin gizli anahtarının (parola) rastsal sayı üretecinde tohum (seed) olarak kullanılması ile elde edilmiştir.

Bir orthonormal taban üzerine daha ayırıcı izdüşümleri elde edebilmek için rastgele izdüşüm matrisi P orthonomalize edilmelidir. Bu amaçla, **P** matrisine Gram-Schmidt prosedürünü uygulayarak orthonormal izdüşüm $\mathbf{P}_{GS}$ yi elde ettik. Sonrasında, sisteme girilen yüz imgesini daha düşük *k*-boyutlu bir alt uzaya aşağıdaki gibi indirgedik:

$$\boldsymbol{v} = \boldsymbol{x}\mathbf{P}_{GS} \tag{1}$$

burada boyutu *1xk* olan $\boldsymbol{v}$ vektörü giriş yüz imgesi **X** in ham kıyım vektörünü belirtir. Şunu belirtelim ki, biz direkt olarak yüz imgesini ham kıyım vektörüne yansıttık. Önceki çalışmalarda [6]-[8], önce yüz imgesinden indirgenmiş özellik vektörü elde edilir (PCA, dalgacık dönüşümü gibi yöntemler kullanılarak), sonar bu özellik vektörüne rastgele izdüşüm uygulanarak ham kıyım değeri elde edilmiştir.

En sonunda, yüz imgesi **X** in ara kıyım vektörünü, $\boldsymbol{d}$, elde etmek için, ham kıyım vektörü $\boldsymbol{v}$ nin elemanlarını nicemledik. Nicemleme için min-max yöntemini kullandık [15]. Bu yöntem, ham kıyım vektörü $\boldsymbol{v}$ nin elemanlarını [0,1] aralığına atar. Biyometrik kıyım algoritmasına eklediğimiz ve algoritmaya ekstra tahmin edilememezlik getiren nicemleme fonksiyonu aşağıdaki gibidir;

$$d(i) = \frac{v(i) - \min(\boldsymbol{v})}{\max(\boldsymbol{v}) - \min(\boldsymbol{v})} \tag{2}$$

burada $i=1,2,...,k$ ve $\boldsymbol{d} \in [0,1]^k$, *min*(.) ve *max*(.) fonksiyonları giriş vektörünün sırasıyla en küçük ve en büyük değerli elemanını hesaplarlar. En sonunda, ara kıyım vektörünün $\boldsymbol{d}$ elemanları belli bir eşik değerine göre 0 yada 1 e yuvarlanır.

$$h(i) = \begin{cases} 1, & if\ d(i) \geq \mu \\ 0, & if\ d(i) < \mu \end{cases} \tag{3}$$

burada μ (eşik değeri) ara kıyım vektörü $\boldsymbol{d}$ nin elemanlarının ortalama değerini belirtir. Böylece, sisteme girilen yüz imgesi **X** için ikili kıyım vektörünü h (kıyım değeri) bulmuş oluruz.

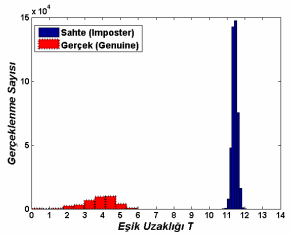
4. Benzetim Sonuçları

Bu bölümde, önerilen yöntem için yapılan benzetim sonuçlarını ele alacağız. Önerilen yöntemi Carneggie Mellon University (CMU) yüz veritabanı üzerinde test ettik [15]. Bu veritabanındaki imgelerin boyutları *64x64* tür. Benzetimlerde, *N*=64, N^2=4906 ve kıyım vektörünün boyu *k*=256 tür. Veri tabanında, her kişiden 75 imge olmak üzere 13 farklı kişiden toplam 975 imge bulunmaktadır. Böylece, ((74x75)/2)x13=36075 gerçek (genuine) çiftimiz ve 75x75x((12x13)/2)=438750 sahte (imposter) çiftimiz vardır. Yüz imgelerinin kıyım değerleri arasındaki mesafeyi Öklit uzaklığı ile ölçtük. Benzetimlerde, herhangi bir imgeyi eğitim verisi diğer bir imgeyi de test verisi (gerçek yada sahte) olarak alıp, tüm olası çiftleri göz önünde bulundurarak önerilen sistemin performansını test ettik.

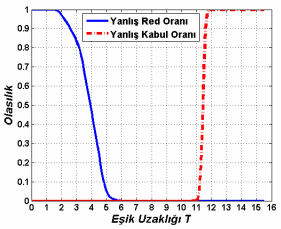
4.1. Deneysel Sonuçlar

Bu bölümde, önerilen biyometrik kıyım yönteminin başarımını çeşitli başarı ölçülerini kullanarak ölçtük. Bahsedeceğimiz iki senaryo için çeşitli benzetimler yaptık.

1. Senaryo: Burada, saldırganın gizli anahtarı ve biyometrik veriyi bilmediğini varsaydık. Şekil 2'de gerçek ve sahte çiftlerin uzaklıklarının deneysel dağılımları gösterilmektedir. Ayrıca, Şekil 3'ten EHO durumunda optimal eşik değerini bulabiliriz. Bu durumda, Şekil 3'te görülen EHO sıfırdır.

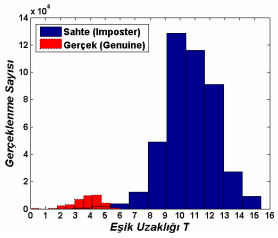


Şekil 2: Gerçek ve Sahte veriler gruplarının deneysel dağılımları.

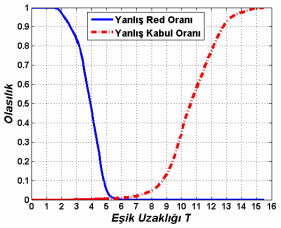


Şekil 3: Önerilen yöntemin Hata - Eşik Uzaklığı *T* grafiğidir. EHO'ı sıfırdır.

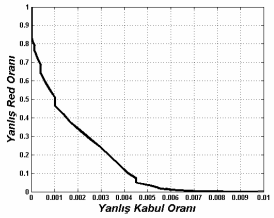
2. Senaryo: Burada, saldırganın gizli anahtarı ve RSÜ'ini ele geçirdiği durumlar ele alınmıştır. Böylece, saldırgan rastgele izdüşüm matrisi **P** yi oluşturabilmektedir fakat yasal kullanıcıya ait biyometrik veriye sahip değildir. Şekil 5'ten EHO'nında optimal eşik değerinin yaklaşık 5.56 olduğu görülmektedir. Ayrıca, Şekil 6'da görülen karar eğrisinde EHO'ı yaklaşık 0.0061 dir.



Şekil 4: Gerçek ve Sahte veri gruplarının deneysel dağılımları.



Şekil 5: Önerilen yöntemin Hata- Eşik Uzaklığı T grafiği. EHO'nında optimum eşik uzaklığı yaklaşık 5.56.



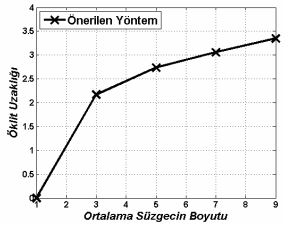
Şekil 6: Önerilen yöntemin karar eğrisidir (ROC curve). EHO'ı yaklaşık 0.0061 dir.

4.2. Algılayıcı ve Çevresel Kaynaklı Bozulum Benzetimleri

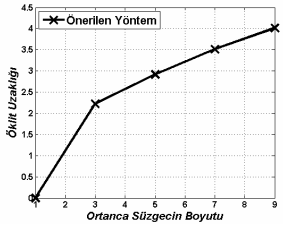
Bu bölümde, algılayıcıların, çevresel kaynaklı etkilerin ve çeşitli değişimlerin biyometrik imge üzerinde oluşturduğu bozulumların önerilen sistem başarımı üzerindeki etkilerini inceledik. Farklı oturumlarda, algılayıcının farklı pozisyon alması, kötü çevre şartları, insanlarda yaşlanma ve kazaya bağlı deformasyonlar, gürültü ve insan-algılayıcı etkileşiminin kötü olması gibi nedenlerden dolayı algılanan biyometik imgede çeşitli sorunlar olabilir. Algılayıcı, kullandığı kameranın özelliklerine bağlı olarak biyometrik imgeye çeşitli süzgeçleme işlemleri uygulayıp imgenin kalitesini düşürebilir. Ayrıca, biyometrik imge, algılayıcı ile veritabanı arasındaki kanalda çeşitli bozulumlara maruz kalabilir. Bunlar gibi pek çok sebepten ötürü, farklı oturumlarda, aynı kişiye ait biyometrik imgeler birbirinden tamamen farklı olabilir.

Biyometrik imgenin ortalama, ortanca ve Gauss süzgeçleme bozulumlarına uğrayabileceğini farzettik. Değişen ortalama, ortanca ve Gauss süzgeç boyutlarında, orjinal ve bozuluma uğramış imgelerin kıyım değerleri arasındaki Öklit uzaklığı

sırasıyla Şekil 8, Şekil 9 ve Şekil 10 gösterilmektedir. Benzetim sonuçlarında görüleceği üzere, bu uzaklıklar Şekil 4 ve Şekil 6 da gösterilen EHO grafiklerindeki optimum eşik uzaklıklarını (1. senaryoda yaklaşık 10 ve 2. senaryoda yaklaşık 5.56) geçmemektedir. Böylece, bu bozulumların önerilen sistemin başarımını etkilemediğini gösterilmiştir.



Şekil 7: Ortalama süzgeci bozulumu

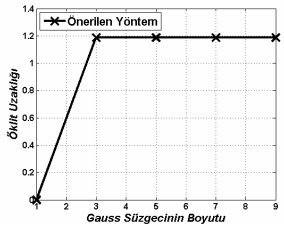


Şekil 8: Ortanca süzgeci bozulumu

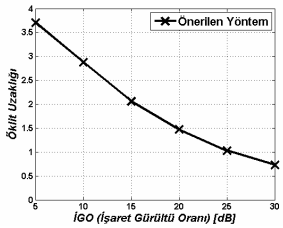
Diğer bir olası durumda ise, biyometrik algılayıcı imgeyi gürültülü olarak kaydedebilir yada algılayıcı ile veritabanı arasındaki kanal gürültülü olabilir. Bu gürültü, doğrulama sisteminin başarımını düşürebilir. Şekil 11'deki benzetimde, biyometrik imgeye farklı İşaret-Gürültü Oranlarında (İGO) eklenebilir beyaz Gauss gürültü (EBGG) ekleyip, sistemin başarımını ölçtük. Burada, İGO'yu aşağıdaki gibi hesapladık:

$$İGO = 10\log_{10}\left(\frac{\frac{1}{MxN}\sum_{m=1}^{M}\sum_{n=1}^{N}(\mathbf{X}[m,n])^2-\left(\frac{1}{MxN}\sum_{m=1}^{M}\sum_{n=1}^{N}(\mathbf{X}[m,n])\right)^2}{\frac{1}{MxN}\sum_{m=1}^{M}\sum_{n=1}^{N}(\mathbf{N}[m,n])^2-\left(\frac{1}{MxN}\sum_{m=1}^{M}\sum_{n=1}^{N}(\mathbf{N}[m,n])\right)^2}\right) \quad (4)$$

burada **X** biyometrik imgeyi, **N** toplanır beyaz Gauss gürültüsünü belirtir. Bu benzetimdeki en büyük uzaklık değeri 1. ve 2. senaryodaki EHO'larında elde edilen optimum eşik uzaklıklarından daha küçüktür. Buradan, gürültünün önerilen sistemin başarımını düşürmediği açıkça görülmektedir.

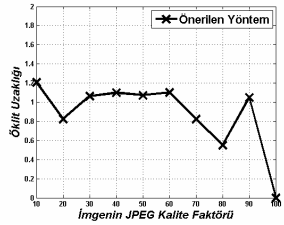


Şekil 9: *Gauss Süzgeci Bozulumu*

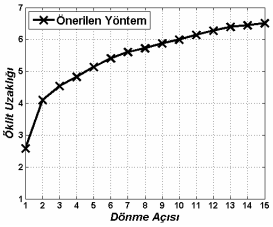


Şekil 10: Değişen İGO oranlarında EBGG bozulumu

Biyometrik imgelerin boyutları çok büyük olduğu için, algılayıcı yakaladığı imgeyi veri tabanına gönderirken çeşitli oranlarda kayıplı sıkıştıma (JPEG sıkıştırması gibi) uygulayabilir. Şekil 12 de gösterildiği gibi önerilen sistem JPEG sıkıştırması karşı dayanıklıdır çünkü oluşan en büyük Öklit uzaklığı değeri 1.2'dir.



Şekil 11: JPEG Sıkştırması Bozulumu



Şekil 12: Döndürme ve Kırpma Bozulumu

Biyometrik algıyıcıların en önemli problemlerinden biri de uyumlu (misalignment) olmama sorunudur. Yüz imgesi, veri toplama esnasında, orjinal haline göre dönmüş yada kırpılmış olarak kaydedilebilir. Şekil 13'teki benzetimde, orjinal imge ile bozuluma uğramış imgenin kıyım değerleri arasındaki uzaklık gösterilmektedir.

5. Sonuçlar

Bu bildiride, yeni bir gürbüz biyometrik imge kıyım yöntemi önerilmiştir. Buradaki amacımız, biyometrik kimlik doğrulama sistemlerinde hem mahremiyeti korumak hem de güvenliği sağlamaktır. Saldırganın, biyometrik veriyi ve gizli anahtarı bilmediği durumlarda sıfır EHO'ı elde ettik. Ayrıca, saldırganın gizli anahtarı ve RSÜ'ni ele geçirdiği durumlarda 0.0061 EHO'ı elde ettik. Diğer taraftan, önerilen sistemin, algılayıcı ve/veya çevresel nedenli çeşitli bozulumlara karşı dayanaklı olduğunu çeşitli benzetimlerle gösterdik.

6. Kaynakça

[1] J. Woodward, "Biometrics: Privacy's foe or privacy's friend?," In *Proceedings of IEEE*, volume 85, 1997.

[2] G. Moko, "Biometrics as a privacy enhancing technology: Friend or foe of privacy?," In *Pr. Laws& Business 9th Pr. Comm./Data Proct. Auth. Workshop,* Spain, 1998.

[3] M. Crompton, "Biometrics and privacy: The end of the world as we know it or white knight of privacy?," In *1st Biometrics Institute Conference,* 2003.

[4] G.I. Davida, Y. Frankel, and B.J. Matt, "On enabling secure applications through off-line biometric identification," *In Proc. of the IEEE 1998 Symp. on Security and Privacy*, pp.148–157, Oakland, Ca., 1998.

[5] G. I. Davida, Y. Frankel, B.J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an off line biometrics based identification scheme," Workshop on Coding and Cryptography, 1999. pp. 129 - 138.

[6] D.C.L.Ngo, A.B.J. Teoh, A.Goh, "Biometric Hash: High Confidence Face Recognition," *IEEE Trans. on Circ. and Sys. for Video Tech.*, Vol.16, No.6, June 2006.

[7] A.Lumini, L.Nanni, "An Improved BioHashing for Human Authentication," *The Journal of the Pattern Recognition*, Elsevier, 2007.

[8] A.Kong, K.H. Cheung, D. Zhang, M. Kamel, J. You, "An Analysis of BioHashing and Its Variants," *The Journal of the Pattern Recognition Society*, Elsevier, 2007.

[9] X. Liu, T. Chen, B.V.K. Vijaya Kumar, "Face Authentication for Multiple Subjects Using Eigenflow," *The Journal of Pattern Recog.*, special issue on Biometrics, 2003.

[10] M. Turk, A. Pentland, "Eigenfaces for Recognition", *Journal of Cognitive Neuroscience*, 3(1), pp.71-86, 1991.

[11] M. Savvides, B.V.K. Vijaya Kumar, P.K. Khosla, "Face verification using correlation filters," Proceedings of the 3rd IEEE Aut. Id. Adv. Tech., pp. 56-61, Tarrytown, NY, 2002.

[12] S. Dasgupta and A. Gupta, "An elementary proof of the Johnson-Lindenstrauss lemma," Tech. Rep. TR-99-006, International Computer Science Institute, Berkeley, CA, 1999.

[13] D.Achlioptas, "Database-friendly random projections," in *Sym. on Prnc. of Database Sys.(PODS)*, 2001, pp. 274-281.

[14] S. Dasgupta, "Experiments with random projection," in *Proc. Confc. on Uncertainty in Artificial Intelligence*, 2000.

[15] P.J. Huber, *Robust Statistics*, Wiley, 1981.

[16] http://amp.ece.cmu.edu - Advanced Multimedia processing Lab web page at CMU.