Pamukkale Univ Muh Bilim Derg, 24(2), 173-179, 2018

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

# Steganografi ve şifreleme kullanılarak çoklu biyometrik sistemlerle kimlik doğrulama için güvenli veri iletimi

# Secure data transmission for multibiometric identity verification systems using steganography and encryption

*Mehmet KILLIOĞLU*[1], *Murat TAŞKIRAN*[2], *Nihan KAHRAMAN*[3*]

[1,2,3]Elektronik ve Haberleşme Mühendisliği Bölümü, Elektrik-Elektronik Fakültesi, Yıldız Teknik Üniversitesi, İstanbul, Türkiye.
mehmetkillioglu@gmail.com, mrttskrn@yildiz.edu.tr, nicoskun@yildiz.edu.tr

Geliş Tarihi/Received: 01.07.2016, Kabul Tarihi/Accepted: 13.12.2016
doi: 10.5505/pajes.2016.39225
* Yazışılan yazar/Corresponding author
Araştırma Makalesi/Research Article

**Öz**

*Son yıllarda biyometrik sistemlerin günlük hayatımızda yaygınlaşması ile birlikte biyometrik verilerin güvenli bir şekilde gönderilmesi ve kullanıcı dışında herhangi bir şahıs tarafından ele geçirilememesi amacıyla biyometrik veri güvenliği üzerindeki çalışmalar hızla artmaktadır. Bu çalışmada şifreleme yöntemlerinden olan Gelişmiş Şifreleme Standardı (Advanced Encryption Standad, AES) ve RSA (Rivest, Shamir, Adleman) algoritması kullanılarak biyometrik veri güvenliğinin sağlanması amaçlanmıştır. Öncelikle güvenliği sağlanacak olan biyometrik veri olarak parmak izi görüntüsü elde edilmiştir. Elde edilen parmak izi görüntüsünde morfolojik işlemler kullanılarak resim arka planındaki gürültüler temizlenmiştir. Arka plandaki gürültüsü temizlenmiş olan parmak izi resmine inceltme işlemi uygulanarak ikinci derece özellik vektörü (çatal ve uç noktaları) elde edilebilecek hale getirilmiştir. Parmak izi görüntüsünde merkez bölgeye yakın yerler ilgili alan olarak tespit edilmiş (Region of Interest, ROI), bu bölgedeki çatal ve uç noktalarının hem 'x' ve 'y' eksenindeki konumları hem de çatallar için üç adet, uç noktaları için bir adet açı değerleri özellik vektörü olarak belirlenmiştir. Elde edilen her değer 16 bitlik tabana çevrilip, 128 bitlik bloklar halinde AES ile şifrelenmiştir. Elde edilen değerler termal görüntünün kırmızı katmanında en düşük değerlikli bitlerine gömülmüştür. Termal görüntünün hangi piksellerin değiştirileceği ise yeşil katmandaki adresleme için kullanılan bilgi ile belirlenmiştir. Alıcı tarafın termal resimdeki biyometrik verileri elde edebilmesi için AES'de kullanılan ilk anahtar RSA algoritması ile şifrelenerek alıcı tarafa iletilmiştir. Son olarak termal görüntüye gömülen biyometrik verinin orijinal resimde meydana getirdiği değişimi ile ilgili analizler yapılmıştır.*

**Anahtar kelimeler:** Steganografi, Parmak izi, Termal görüntü, Gelişmiş şifreleme standardı(AES), RSA

**Abstract**

*Effort on biometric data security in recent years in order to secure the transmission of biometric data along with the spread of biometric systems and can not be seized by any person other than the user is increasing rapidly. In this work, Advanced Encryption Standard (AES) and RSA (Rivest, Shamir, Adleman) algorithms were intended to ensure the security of biometric data using the algorithm. First fingerprint biometric data to be provided as security image is obtained. The noise in background of the resulting fingerprint image has been cleared using morphological operations. Thinning is applied to fingerprint image that background noise is cleared and the secondary feature vectors (minutiae points such as bifurcations and ridge endings) has obtained. The region of interest near the center of the fingerprint image is determined as the area of interest (ROI), the positions of the bifurcation and the ridge endings in this region along the x and y axes, as well as three angles for the bifurcation and one for the ridge endings in feature vectors. Each vector element has converted to 16 bit and then encoded by 128 bits blocks using AES. These encoded bits were embedded to least significant bits of red layer of the thermal image. Which pixels of the thermal image are to be replaced is determined by the information used for addressing in the green layer. In order to to obtain biometric data on the thermal image by the receiver side, the first used AES key was transmitted to the receiving side encrypted with RSA algorithm. Finally, original thermal image and biometric data embedded thermal image using steganography are compared by analyses.*

**Keywords:** Steganography, Fingerprint, Thermal image, Advanced encryption standard (AES), RSA

## 1 Giriş

Biyometri, kimlik saptamak amacıyla ortaya atılmış bir terimdir. Temelinde insanların fiziksel ve davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş otomatik sistemler yer almaktadır. Kimliklendirme için kullanılması düşünülen özelliklerin biyometrik özellik olarak tanımlanabilmesi için evrensel ancak kişiye özgü olması, ölçülebilir olması, kolay elde edilebilir olması gibi temel nitelikleri taşıması gereklidir. Biyometrik veriler, şifre veya şifre içeren kartların aksine değiştirilemediğinden bu verilerin gizliliği de önem arzetmektedir. Bir bilginin gizli olmasından kastedilen, bilginin tamamen gizli tutulması değil, iletilmesi amaçlanan kişiye bozulmadan, değiştirilmeden, başka birisinin eline geçmeden ulaşması demektir [1].

Literatürde farklı bilgilerin gizliliğinin korunması için biyometrik anahtarlama işlemleri kullanılmaktadır. Burada herhangi bir veri alıcı tarafa aktarılırken biyometrik anahtarla şifrelenip, ancak alıcı taraf bu anahtara sahip ise deşifrelenebilmektedir. Biyometrik verilerin güvenliği konusunda ise çalışmalar biyometrik özelliklerin herhangi bir resim içerisine gömülmesini içermektedir [2]. Steganografi ismi verilen bu yöntemin amacı, günlük hayatta rasgele kayda alınan görüntülerle gönderilmesi gereken biyometrik verilerin üçüncü kişilerde şüphe uyandırmayacak bir yaklaşımla iletilmesini sağlamaktır.

Biyometrik veri, resimlerde birçok farklı yol ile gömülebilir. Örneğin resmin her bir bitinin içine verinin şifrelenerek gömülmesi ya da dikkat çekmeyecek yoğun alanlarda resmin içinde gelişigüzel şekilde dağıtılarak ve ya resim içerinde birçok defa tekrarlanarak verinin gömülmesi sağlanabilir. En düşük

değerlikli bit uygulamaları ve resimlerin sayısal değerlere dönüştürülmesinden sonra piksel değerlerinde değişiklik yapma resimlerde veri saklamak için literatürde sıkça kullanılan yöntemlerdendir [3]-[5]. Bu yöntemler farklı formattaki dosyalara farklı başarı oranlarıyla uygulanabilir. Literatürde resimlerde veri saklamak ile ilgili olarak en sık kullanılan steganografi yöntemi 256 gri renk tonu olan resimlere uygulanan steganografi yöntemidir. Resme veri saklandıktan sonra baytlar arasında kademeli yoğunluk değişimi gözle görülemeyecek düzeyde olmaktadır. Literatürdeki çoğu çalışmada siyah-beyaz resimler yüksek başarım gösterse de bazı çalışmalarda renkli resimlerle de yüksek başarım elde edildiği görülmüştür. Bu çalışmada da renk dağılımı karmaşıklığı açısından veri gizlemeye avantaj sağlayabilecek termal yüz görüntüleri kullanılmıştır [6].

Termal yüz görüntüleri kullanılmasının bir diğer amacı da karanlıkta veya yeterli ışığın olmadığı durumlarda yüz tanıma işleminin yüksek başarımla gerçeklenebilmesidir [7]. Çalışmanın hedefinde termal yüz görüntüsünün içine bir başka biyometrik veri olan parmak izi özelliklerinin gömülmesi ve böylece çoklu biyometrik kimliklendirme sisteminin dışardan yapılabilecek saldırılara karşı daha güvenli olmasının sağlanması bulunmaktadır. Bu çalışmada iletilecek veri olarak bir insanın termal yüz görüntüsü seçilmiştir. Aynı kişinin parmak izi özellik noktaları da iletilen termal yüz görüntüleri içerisine gömülerek karşı tarafa gizli bilgi olarak gönderilmesi hedeflenmiştir. Böylece iletim hattına saldırıda bulunabilecek bir kişi hatta iletilen biyometrik veriyi ele geçirip alıcı tarafı kırabileceğini düşünse de, alıcı taraftaki çoklubiyometrik sisteme ikinci bilgiyi giremediği için bu sistemi kıramaz.

Çalışmanın ikinci bölümünde parmak izi özelliklerinin termal görüntü içerisine şifrelenmiş bir şekilde nasıl gömüldüğü açıklanmaktadır. Sonuçlar kısmında da orjinal termal yüz görüntüsü ile gizli bilgi gömülmüş termal yüz görüntüsü arasındaki farklar literatürde tanımlanmış olan yöntemlerle ortaya konmuştur.

## 2 Önerilen algoritma

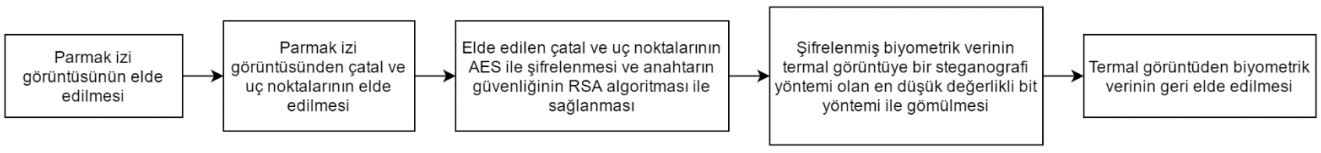
Çoklu biyometrik sistemlerinde kullanılmak üzere önerilen güvenli veri iletimi için oluşturulan algoritma temel olarak dört aşamayı içermektedir.

- Parmak izi görüntüsünden ikinci derece özellik olan çatal ve uç noktalarının elde edilmesi,
- Elde edilen çatal ve uç noktalarının AES ile şifrelenmesi ve anahtarın güvenliğinin RSA algoritması ile sağlanması,
- Şifrelenmiş biyometrik verinin termal görüntüye bir steganografi yöntemi olan en düşük değerlikli bit yöntemi ile gömülmesi,
- Termal görüntüden biyometrik verinin geri elde edilmesi.

Önerilen algoritmanın blok diyagramı Şekil 1'de verilmiştir.

### 2.1 Parmak izi görüntüsünden ikinci derece özellik olan çatal ve uç noktalarının elde edilmesi

Kullanıcıdan elde edilen parmak izi görüntüsünden çatal ve uç noktaları elde edebilmek amacıyla öncelikle morfolojik işlemler kullanılarak parmak izi görüntüsündeki gürültüler kaldırılmıştır. Elde edilen parmak izi görüntüsüne inceltme işlemi kullanılarak parmak izi şeklinin tek piksellerle ifade edilebilecek hale getirilmiştir. İnceltme işleminin amacı çatal ve uç noktalarının daha rahat şekilde elde edilmesini sağlamaktır. İnceltme işlemi gerçekleştirilmiş olan parmak izi görüntüsü üzerinde 3x3'lük pencereler gezdirilerek resimdeki çatal ve uç noktaları elde edilmeye çalışılmıştır. 3x3'lük boyuttaki matrisin merkez noktası referans alınarak komşuluklar incelenmiştir [8]. Merkez noktasının bir değerini aldığı durumlarda sadece bir komşulukta bir değeri varsa bu nokta uç noktası olarak işaretlenmiş, eğer komşuluklardaki bir değeri sayısı birden fazla ise bu nokta çatal noktası olarak işaretlenmiştir. Bu işlemler sonucunda parmak izi görüntüsünde birçok adet uç ve çatal noktası bulunmuştur. Parmak izi görüntüsündeki çatal ve uç noktalarını doğru bulmak amacıyla hatalı bulunmuş olan noktaların temizlenmesi için optimizasyon işlemi gerçekleştirilmiştir. Optimizasyon işlemi, özellik noktaları arasındaki öklid uzaklığını temel almaktadır. İki çatal arası uzaklık, iki uç arası uzaklık, çatal ve uç noktaları arasındaki uzaklıklar belirlenmiş eşik değerinden küçük ise o noktalar silinmektedir. Eşik değeri belirlerken parmak izi görüntüsünün boyutları göz önüne alınmıştır. Çeşitli eşik değeri denemeleri sonucunda 220x193 boyutlarına sahip parmak izi görüntüsünde eşik değerinin 6 kullanılması, parmak izi görüntüsünün önemli özelliklerini saklayarak hatalı noktaların kaldırılmasını sağlamıştır. Görüntünün çözünürlüğü değiştikçe iki parmak izi çizgisi arasındaki uzaklıkların ortalama değerleri değişeceği için eşik değerinin değiştirilmesi gerekmektedir. Eşik değeri bu ortalama değerden düşük olmalıdır. Elde edilen parmak izi görüntüsünde inceltme işlemi gerçekleştirildikten sonra görüntünün sınır piksellerinde inceltme işlemi sonucunda oluşan hatalı uç noktalarının biyometrik veri olarak kabul edilmemesini sağlamak amacıyla ilgili alan (ROI) belirlenmesi işlemi gerçekleştirilmiştir. İlgili alan belirlenirken elde edilen parmak izi görüntüsüne kapatma ve erozyon morfolojik işlemi gerçekleştirilerek parmak izi görüntüsündeki ilgili alan seçilmiştir. İlgili alandaki gürültülerin kaldırılması için beş pikselden küçük değere sahip noktalar ilgili alandan kaldırılmıştır. Elde edilen bu çatal ve uç noktaları, parmak izi resminin sol üst köşesi (0,0) belirlenerek x ve y eksenindeki koordinat değerleri belirlenmiştir. Çatal noktaları için 3 farklı açı, uç noktası için bir açı değeri bulunmuştur. Açı değerleri hesaplanırken 5x5'lik matris incelenmiştir. (3,3) noktası merkez alınmış ve kenar pikselleri haric diğer pikseller sıfır değerine çekilmiştir. 5x5'lik pencerede uç noktası için sadece bir piksel kalır iken çatal noktası için 3 piksel kalmaktadır. Uç noktası için açı hesaplanırken pikselin merkeze göre konumu dikkate alınmaktadır.

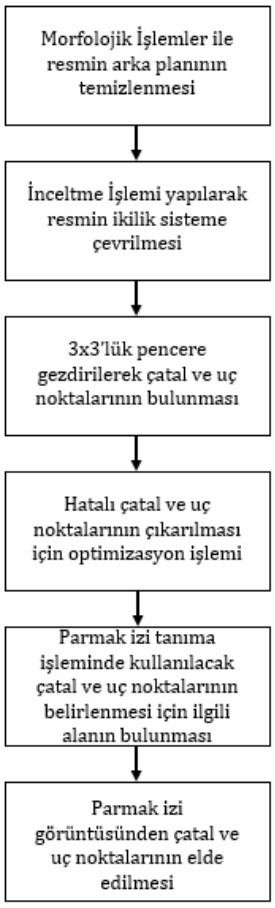



Şekil 1: Çoklu biyometrik sistemleri için önerilen algoritmanın blok diyagramı.

Çatal noktası için açı hesaplarken ise 3 farklı pikselin merkeze göre konumu dikkat alınmaktadır. Şekil 2'de örnek olarak kullanılan parmak izine ait ikinci derece özellikler parmak izi görüntüsü üzerinde gösterilmiştir. Kırmızı noktalar uç noktalarını, yeşil noktalar ise çatal noktalarını ifade etmektedir.

Elde edilen bu değerler 16 tabanına çevrilerek AES ile şifrelenmiştir. Şekil 3'te parmak izi görüntüsünden ikinci derece özellik olan çatal ve uç noktalarının elde edilmesi algoritmasına ait blok diyagramı verilmiştir. Şekil 3'te bulunan parmak izinin uç ve çatal noktalarıyla ilgili koordinat ve açı değerleri Tablo 1 ve Tablo 2'de verilmiştir.

Şekil 2: İkinci derece özellik noktaları. Yeşil noktalar çatal, kırmızı noktalar ise uç noktaları belirtmektedir.




Şekil 3: Parmak izi görüntüsünden ikinci derece özellik olan çatal ve uç noktalarının elde edilmesi adımının blok diyagramı.

Tablo 1: Örnek uç noktalarının x ve y koordinatları, $\theta$ açı değerleri.

| X | Y | $\theta$ |
|---|---|---|
| 134.0000 | 66.0000 | 360.0000 |
| 127.0000 | 79.0000 | 150.0000 |
| 95.0000 | 161.0000 | 60.0000 |
| 100.0000 | 174.0000 | 60.0000 |
| 194.0000 | 192.0000 | 120.0000 |
| 24.0000 | 196.0000 | 270.0000 |
| 76.0000 | 202.0000 | 240.0000 |
| 52.0000 | 238.0000 | 240.0000 |
| 138.0000 | 254.0000 | 45.0000 |
| 147.0000 | 262.0000 | 30.0000 |
| 27.0000 | 265.0000 | 240.0000 |
| 27.0000 | 285.0000 | 225.0000 |
| 29.0000 | 313.0000 | 225.0000 |
| 98.0000 | 320.0000 | 45.0000 |

Tablo 2: Örnek çatal noktaları, x ve y koordinatları, $\theta$ açı değerleri.

| X | y | $\theta 1$ | $\theta 2$ | $\theta 3$ |
|---|---|---|---|---|
| 165.0000 | 27.0000 | 330.0000 | 45.0000 | 180.0000 |
| 155.0000 | 39.0000 | 360.0000 | 240.0000 | 150.0000 |
| 145.0000 | 42.0000 | 360.0000 | 240.0000 | 135.0000 |
| 102.0000 | 43.0000 | 330.0000 | 60.0000 | 180.0000 |
| 102.0000 | 55.0000 | 30.0000 | 270.0000 | 180.0000 |
| 162.0000 | 64.0000 | 315.0000 | 60.0000 | 180.0000 |
| 159.0000 | 72.0000 | 360.0000 | 270.0000 | 135.0000 |
| 90.0000 | 86.0000 | 30.0000 | 60.0000 | 180.0000 |
| 169.0000 | 106.0000 | 45.0000 | 300.0000 | 150.0000 |
| 145.0000 | 110.0000 | 330.0000 | 60.0000 | 180.0000 |
| 139.0000 | 118.0000 | 330.0000 | 120.0000 | 225.0000 |
| 159.0000 | 120.0000 | 330.0000 | 120.0000 | 225.0000 |
| 145.0000 | 124.0000 | 330.0000 | 60.0000 | 210.0000 |
| 170.0000 | 134.0000 | 315.0000 | 90.0000 | 180.0000 |
| 147.0000 | 151.0000 | 45.0000 | 270.0000 | 135.0000 |
| 86.0000 | 155.0000 | 360.0000 | 120.0000 | 225.0000 |
| 70.0000 | 159.0000 | 360.0000 | 60.0000 | 240.0000 |
| 79.0000 | 211.0000 | 360.0000 | 60.0000 | 240.0000 |
| 198.0000 | 216.0000 | 45.0000 | 300.0000 | 135.0000 |
| 43.0000 | 219.0000 | 360.0000 | 270.0000 | 120.0000 |
| 29.0000 | 223.0000 | 30.0000 | 270.0000 | 120.0000 |
| 95.0000 | 244.0000 | 30.0000 | 120.0000 | 225.0000 |
| 142.0000 | 266.0000 | 300.0000 | 60.0000 | 225.0000 |
| 213.0000 | 270.0000 | 45.0000 | 270.0000 | 120.0000 |
| 225.0000 | 282.0000 | 60.0000 | 270.0000 | 150.0000 |
| 23.0000 | 298.0000 | 45.0000 | 300.0000 | 180.0000 |
| 154.0000 | 299.0000 | 360.0000 | 240.0000 | 120.0000 |

### 2.2 Elde edilen çatal ve uç noktalarının gelişmiş şifreleme standardı ile şifrelenmesi ve anahtarın güvenliğinin RSA algoritması ile sağlanması

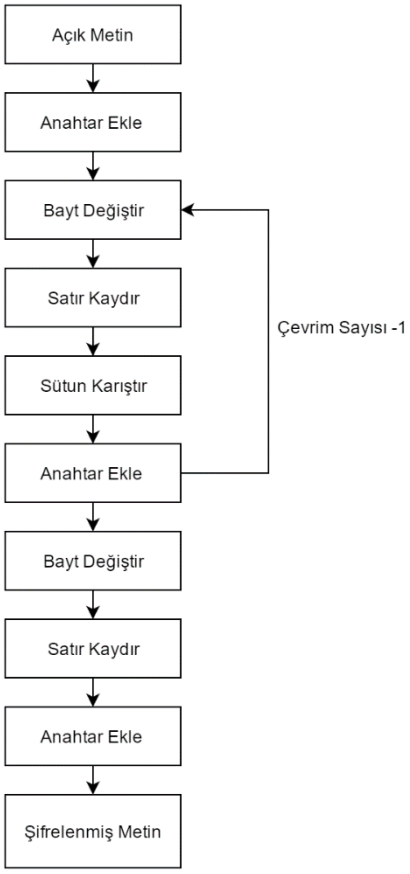
Gelişmiş Şifreleme Standardı (AES) Amerika Birleşik Devletleri tarafından optimize edilen bir blok şifreleme algoritmasıdır [9]. AES algoritmasının uygulanabilmesi için girişin 128-bit olması gerekmektedir. 128-bitlik giriş sonucunda 128-bitlik çıkış elde edilmektedir. Bunu sağlamak için biyometrik veri 128-bitlik parçalar halinde şifrelenmektedir. Bu çalışmada AES anahtar uzunluğu 128-bit seçilmiştir. Kullanılan anahtar RSA ile şifrelenip karşı tarafa iletilmektedir. Bu sayede anahtar iletimi de güvenli hale getirilmiştir. RSA şifreleme algoritması 1977 yılında R. Rivest, A. Shamir ve L. Adleman tarafından bulunmuş ve daha sonra asimetrik şifreleme algoritmalarına (genel anahtar şifrelemesi) uygun biçimde geliştirilmiştir. Bu algoritma, asimetrik şifreleme algoritmalarında ve dijital imza işlemlerinde güvenli bir şekilde kullanılmaktadır [10].

### 2.2.1 Gelişmiş şifreleme standardının genel yapısı

AES algoritması 4x4'lük durum matrisi üzerinde çalışır. Matristeki her hücre bir bayt ifade etmektedir. Anahtar ise 128-bit, 192-bit ve ya 256-bit olarak seçilebilmektedir. AES çevrimlerden oluşmaktadır. Anahtar uzunluğuna göre çevrim sayısı değişir. 128-bit için 10 çevrim, 192-bit için 12 çevrim, 256-bit için ise 14 çevrim gereklidir. AES algoritmasında son çevrim hariç her çevrim 4 adımdan oluşmaktadır. Bu adımlar *"Bayt Değiştir", "Satır Kaydır", "Sütun Karıştır"* ve *"Anahtar Ekle"* adımlarıdır. Son çevrimde *"Sütun Karıştır"* adımı bulunmamaktadır.

AES'de çevrimlerden önce ilk adım *"Anahtar Oluştur"* adımıdır. Bu adım sonunda çevrim sayısının bir fazlası kadar 128-bitlik anahtar oluşturulur [11]. Bu anahtarlar *"Anahtar Ekle"* adımında kullanılmaktadır. Çevrimlerden önceki bir adım ise Anahtar Ekle adımıdır.

Şekil 4'te AES algoritmasına ait blok diyagramı verilmiştir. Şifrelenecek olan biyometrik veri açık metin olarak belirtilmiştir.




Şekil 4: AES algoritmasının blok diyagramı.

### 2.2.2 Anahtar ekle adımı

Çevrimlerden önceki Anahtar Ekle adımında Anahtar Oluştur adımından gelen matristeki ilk 4x4'lük matris ile durum matrisi XOR işlemine girer. Bu işlem sonucu çıkan matris yeni durum matrisi olur. Bu işlemde oluşan yeni durum matrisi çevrime girer.

Çevrim içerisindeki Anahtar Ekle adımında ise durum matrisi ile Anahtar Oluştur adımından gelen, matrisin o çevrime denk gelen 4x4'lük matris XOR işlemine girer.

### 2.2.3 Bayt değiştir adımı

Bu adımda durum matrisi daha önceden oluşturmuş olan 8-bitlik bir değişim kutusu (Rijndael S-box) kullanılarak güncellenir. Bu değişim kutusu sonlu cisim olan GF üzerinde ters alma işleminden elde edilmiştir. Bu adım algoritmada doğrusallığı bozar ve doğrusal-olmayan bir dönüşüm haline gelmesini sağlar [12].

### 2.2.4 Satır kaydır adımı

Bu adımda 4x4'lük durum matrisindeki satırlar üzerinde işlem yapılır. Durum matrisine ait ilk satır sabit kalmaktadır, diğer satırlar satır sayısının bir eksiği kadar sola kaydırılır. İkinci satır 1 bayt sola, üçüncü satır 2 bayt sola, dördüncü satır ise 3 bayt sola kaydırılır.

Bu adımda önemli olan kolonların birbirinden lineer olarak bağımsızlaştırılmasıdır [13].

### 2.2.5 Sütun karıştır adımı

Sütun Karıştır adımında sütunlara yönelik işlem yapılmaktadır. Bu adımda her bir sütun birbirinden bağımsız olarak tersi olan doğrusal bir dönüşüm ile karıştırılır. Bu adımda sütun boyutlarında bir değişiklik olmamaktadır. Sütun Karıştır işleminde durum matrisindeki her sütun birbirinden bağımsız olarak Denklem (1) ile yeniden hesaplanır. Bu sayede girişteki her bayt, çıkıştaki baytlardaki değişimi etkilemektedir [14]-[16].

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2\,3\,1\,1 \\ 1\,2\,3\,1 \\ 1\,1\,2\,3 \\ 3\,1\,1\,2 \end{bmatrix} * \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (1)$$

Denklem (1)'de $b_0, b_1, b_2, b_3$ dönüşüm sonrası oluşan kolonun değerlerini belirtirken $a_0, a_1, a_2, a_3$ dönüşümü yapılacak kolonu belirtmektedir.

### 2.2.6 Anahtar güvenliğinin RSA algoritması ile sağlanması

AES için seçilen anahtar 128-bit uzunluğunda rastgele bir biçimde belirlenmiştir. Termal görüntüde gömülmüş olan biyometrik verinin alıcı tarafından tekrar elde edilebilmesi için AES anahtarının alıcıya ulaştırılması gerekmektedir. Bu anahtarın güvenli bir şekilde alıcıya iletilmesi için RSA algoritması ile şifreleme işlemi gerçekleştirilmiştir. RSA algoritmasının güvenliği, iki asal tam sayının çarpımını bulmak kolay iken oldukça büyük bir sayıyı çarpanlarını bulma zorluğuna dayanır. Alıcı sadece kendisinin bildiği iki büyük asal sayı üretir ve seçtiği asal sayıların çarpımını biyometrik veriyi şifreleyen göndericiye iletir. Şekil 5'te anahtar güvenliğinin RSA algoritması ile sağlanmasına ait blok diyagramı verilmiştir.

#### 2.2.6.1 RSA anahtarı oluşturma, şifreleme ve şifrelenmiş veriyi çözme

Alıcı taraf anahtar oluştururken p ve q olmak üzere iki büyük asal sayı seçmektedir. Denklem (2) kullanılarak n (çarpım) sayısı elde edilmektedir. Denklem (3)'de elde edilen n sayısının totienti olan ϕ(n) elde edilmektedir. ϕ(a), a'dan küçük ve a ile aralarında asal olan sayıların miktarını belirtmektedir. ϕ(n)'i hesaplamak p ve q değerleri bilindiği takdirde hesaplamak çok kolaydır, fakat sadece n sayısı ile büyük sayının totientini hesaplamak çok zordur. Denklem (4)'teki şart kullanılarak bir e sayısı elde edilir. $e$ sayısı ile $\phi(n)$ kendi aralarında asal olmak zorundadır. Elde edilen $e$ sayısı ve $n$ ortak anahtarı

oluşturmaktadır [17]. Denklem (5) kullanılarak bir $d$ değişkeni elde edilir.

$$n = p * q \quad (2)$$

$$\phi(n) = (p - 1) * (q - 1) \quad (3)$$

$$1 < e < \phi(n) \quad (4)$$

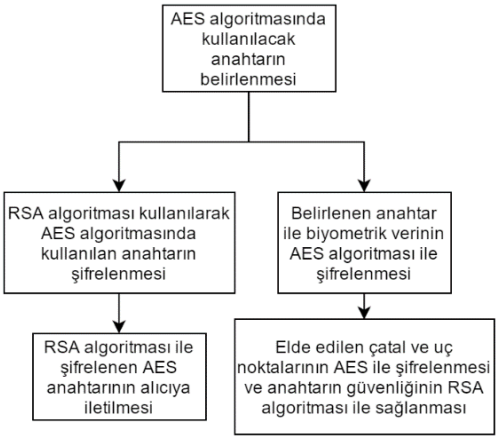
$$d * e = 1(mod\ \phi(n)) \quad (5)$$

$$c = m^e (mod\ n) \quad (6)$$

$$m = c^d\ (mod\ n) \quad (7)$$

Veri sayıya dönüştürülüp Denklem (6) kullanılarak şifrelenir. $m$ sayıya dönüştürülen şifrelenecek olan veriyi, $c$ ise şifrelenmiş veriyi ifade etmektedir.

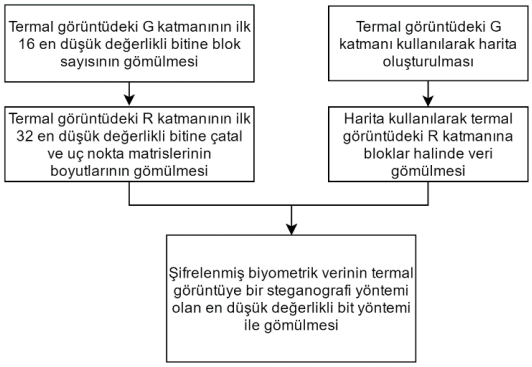
Alıcı taraf şifrelenmiş veri olan $c$'yi ve elindeki $d$'yi kullanarak Denklem (7) yardımıyla şifrelenmiş veri çözülür [18].




Şekil 5: Biyometrik verilerin AES algoritmasıyla şifrelenmesi ve AES algoritmasında kullanılan anahtarın RSA algoritması ile şifrelenmesine ait blok diyagramı

### 2.3 Şifrelenmiş biyometrik verinin termal görüntüye bir steganografi yöntemi olan en düşük değerlikli bit yöntemi ile gömülmesi

Biyometrik verisi gönderilmek istenen kullanıcının parmak izi görüntüsünde bulunan ikinci derece özellik olan çatal ve uçların koordinat ve açı bilgileri AES algoritması ile şifrelendikten sonra alıcıya bir arayüze gömülerek gönderilmektedir. Bu çalışmada arayüz olarak kullanıcının termal yüz görüntüsü kullanılmıştır. Bu çalışmada kullanılan termal yüz veri tabanı, Yıldız Teknik Üniversitesi Siber Güvenlik ve Biyometrik Araştırma Danışmanlık ve Test Merkezi'nde FLIR E8 MSX® Enhancement Kızılötesi Kamera kullanılarak toplanan on farklı pozda, farklı sıcaklık koşulları altında, gözlüklü ve/veya gözlüksüz toplamda 230 adet 320x240 boyutlarında termal görüntü verisi içermektedir [7]. Bu çalışmada termal yüz görüntüsünün çözünürlük değeri biyometrik verinin şifrelendikten sonra saklanabilmesi için minimum sayıda piksel değerini kapsayacak şekilde seçilmiştir. Bunun nedeni işlem hızını arttırmak ve karşıdaki kullanıcının şifrelenmiş biyometrik veriye erişmesini kolaylaştırmaktır. Aynı işlem yüksek çözünürlükteki termal görüntü üzerinde de uygulanabilmektedir. Şifrelenmiş biyometrik verilerin gömülmesi için termal yüz görüntüsünün RGB uzayındaki R katmanına en düşük değerlikli bit yöntemi kullanılarak gömülmesine karar verilmiştir. En düşük değerlikli bit yöntemi resimdeki bir katmandaki bir pikselin en düşük değerlikli bitine bir bitlik veri yazılmasıdır [19]. Bu bitlerin değiştirilmesi sonucunda termal fotoğraftaki değişiklik çok düşük boyutta olacaktır. Bu şekilde katmandaki her piksele bir bitlik veri yazılarak yeterince veri saklanılabilir. R katmanında hangi piksellere şifrelenmiş biyometrik verinin gömüleceğine termal yüz görüntüsünün RGB uzayındaki G katmanındaki en düşük değerlikli bitler kullanılarak karar verilmektedir. G katmanındaki her pikselin en düşük değerlikli bitleri kullanılarak her bit R katmanındaki 16-bitlik bloğu ifade edecek şekilde haritalandırma işlemi yapılmaktadır. G katmanının ilk en düşük değerlikli 16-bitine R katmanına kaç adet 16-bitlik blok yazılacağı bilgisi gömülmektedir. R katmanına kaç adet şifrelenmiş biyometrik verinin gömüleceği G katmanının ilk iki 16-bitlik bloğuna gömülmektedir. G katmanı ile oluşturulan harita kullanılarak R katmanına veri gömülüp gömülmeyeceğine o bloğa denk gelen bit ile karar verilir. Eğer o bloğa denk gelen bit bir ise o bloğa şifrelenmiş veri yazılmaktadır, eğer sıfır ise o R katmanındaki blok atlanmaktadır. Bu işlemler gerçekleştirilerek gönderici tarafından alıcıya yollanacak biyometrik verinin termal yüz görüntüsüne gömülmesi işlemi gerçekleştirilmiştir. Şekil 6'da şifrelenmiş biyometrik verinin termal yüz görüntüsünün en düşük değerlikli bit yöntemiyle gömülmesinin blok diyagramı verilmiştir.




Şekil 6: Şifrelenmiş biyometrik verinin termal yüz görüntüsünün en düşük değerlikli bit yöntemiyle gömülmesine ait blok diyagramı.

### 2.4 Termal görüntüden biyometrik verinin geri elde edilmesi

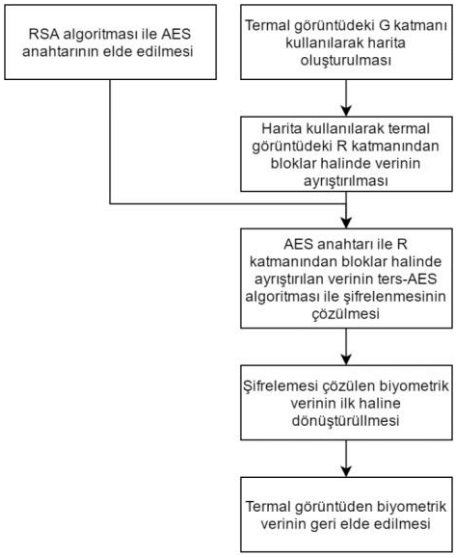
Bu aşamada ilk olarak RSA algoritması ile şifrelenmiş olan AES anahtarını geri elde edilmesi işlemi gerçekleştirilmektedir. Alıcı tarafın elindeki iki büyük asal sayıyı ve şifrelenmiş veriyi Denklem (7) kullanılarak AES anahtarı elde edilir.

İkinci adımda şifrelenmiş biyometrik verinin RGB uzayındaki G katmanının ilk 16 en düşük değerlikli biti okunmaktadır. Bu 16-bitlik veri R katmanına kaç tane blok yazılacağı bilgisini sakladığından harita oluşturmak için kullanılacaktır. Harita R katmanındaki blok sayısı kadar bir biti elde edene kadar G katmanında tarama işlemi gerçekleştirilerek elde edilmektedir.

Harita elde edildikten sonra R katmanındaki bitlerin ayrıştırılması gerekmektedir. Termal görüntünün R katmanındaki veriler G katmanından elde edilen harita yardımıyla bloklar halinde okunmaktadır. Tüm şifrelenmiş veriler okunduktan sonra AES anahtarı kullanılarak verilere ters-AES işlemi uygulanmaktadır. Şifrelenmiş veri çözüldükten sonra R katmanındaki ilk iki 16-bitlik veri okunmaktadır. Bu veri biyometrik verilerin boyutlarını tutmaktadır ve

şifrelenmesi çözülmüş verilerin düzenlenmesi için kullanılmaktadır.

İşlemler tamamlandıktan sonra termal görüntüden parmak izi görüntüsünün ikinci derece özellikleri herhangi bozulmaya uğramadan güvenli bir şekilde iletimi sağlanmıştır. Şekil 7'de içerisine biyometrik veri gömülmüş termal görüntüden biyometrik verinin ayrıştırılması ve ayrıştırılan biyometrik verinin şifrelenmesinin çözülmesine ait blok diyagramı verilmiştir.




Şekil 7: Termal görüntüden biyometrik verinin geri elde edilmesine ait blok diyagramı.

## 3 Sonuçlar

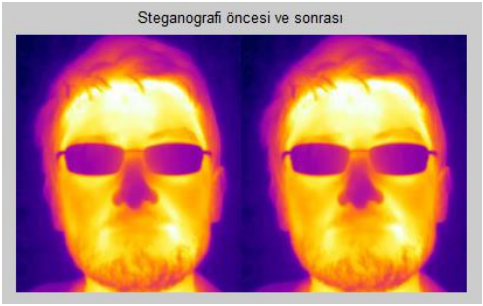
Bu çalışmada Gelişmiş Şifreleme Standardı kullanılarak biyometrik veri olarak kullanılan parmak izinin ikinci derece özellikleri şifrelenmiş ve Gelişmiş Şifreleme Standardında kullanılan rastgele belirlenen ilk anahtar matrisi RSA algoritması ile şifrelenmiştir. Şifrelenen biyometrik veri termal yüz görüntüsüne steganografi yöntemlerinden biri olan en düşük değerlikli bit yöntemi ile gömülmüştür. Bu işlemler sayesinde hem kullanıcının biyometrik verisinin güvenliği sağlanmış, hem de Gelişmiş Şifreleme Standardında kullanılan ilk anahtar matrisi RSA algoritması ile şifrelendiği için anahtarın da güvenliği sağlanmıştır.

Termal yüz görüntüsünde şifrelenmiş biyometrik verinin R katmanında hangi bloklara gömüleceği termal yüz görüntüsünün G katmanındaki en düşük değerlikli bitler kullanılarak belirlenmiş ve bu işlem ile alıcı ve gönderici arasındaki biyometrik veri aktarım işleminin güvenliği daha da arttırılmıştır. Şekil 8'de, steganografi işlemi uygulanmamış termal görüntü ile Şekil 9 (a)'da verilen parmak izi görüntüsünden elde edilen ikinci derece özelliklerin şifrelenip steganografi işlemi uygulanmış termal görüntünün karşılaştırılması verilmiştir. Şekil 9 ve Şekil 10'da sırasıyla çalışmada kullanılan üç farklı termal görüntü ve iki farklı parmak izi görüntüsü verilmiştir. Bu parmak izleri ve termal görüntüler üzerinde önerilen yöntem kullanılarak parmak izleri termal görüntülerin içine gömülmüştür. İşlem sonrası termal görüntülerdeki bozulmaların gözetlenebilmesi için üç farklı test yapılmıştır. Bağımsız Özellik Benzerliği (Independent Feature Similarity, IFS), doğal resimler ile eğitilmiş bir özellik dedektörü ile iki resim arasındaki benzerlikleri kullanarak resim kalitesini değerlendirmektedir [20]. Test sonucunun bir ve ya bire yakın olması termal resimdeki bozulmanın çokaz olduğunu belirtmektedir. Yapılan tüm testlerde IFS sonucu bir değerine çok yakındır.

$$PSNR = 10 * \log_{10}(\frac{MAX_I^2}{MSE}) \quad (8)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (9)$$

Sinyal gürültü oranı (Signal-to-Noise Ratio, SNR) sinyalin gürültüye olan oranını vermektedir. En yüksek SNR değeri (Peak Signal-to-Noise Ratio, PSNR) Denklem (8) ile hesaplanmaktadır [21]. $MAX_I$ bir pikselin alabileceği maksimum değeri belirtmektedir. Ortalama karesel hata (Mean Square Error, MSE) değerinin hesaplanmasına Denklem (9)'da yer verilmiştir. Denklem (9)'da m,n resim boyutlarını, I ve K ise aralarındaki MSE değeri hesaplanacak iki farklı resimi belirtmektedir. PSNR değerinin yüksek olması bozulmanın daha az olduğunu belirtmektedir. PSNR değeri dB cinsinden verilmiştir. Tablo 3'te çalışmada kullanılan termal yüz görüntüleri ve bu görüntülerine gömülen parmak izleri verileri ile ilgili PSNR ve IFS test sonuçları verilmiştir. Şekil 12'de termal görüntünün işlem öncesi ve sonrası histogramları verilmektedir. Şekil 13'te ise histogramların farkı verilmiştir. Yapılan hesaplamalar sonucu işleme uğramamış termal görüntü ile işleme uğramış termal görüntünün histogramları arasındaki fark maksimum %0.5 olmaktadır. Görüldüğü üzere işlem sonucu termal görüntü üzerindeki değişiklik çok düşük olmakla beraber doğru AES anahtarı ve önerilen algoritmanın işleyişi bilinmeden biyometrik veriyi okumanın karmaşıklığı oldukça yüksektir.




Şekil 8: Termal görüntünün steganografi işlemi öncesi ve işlem sonrası karşılaştırma.

Tablo 3: Ek A'da bulunan termal görüntüler ve parmak izleri için test sonuçları.

| Termal görüntüler | Parmak izleri | IFS sonucu | PSNR | MSE |
|---|---|---|---|---|
| Şekil 10 (a) | Şekil 9 (a) | 0.999995971 | 67.36 | 0.012443 |
| Şekil 10 (a) | Şekil 9 (b) | 0.999995699 | 68.11 | 0.016344 |
| Şekil 10 (b) | Şekil 9 (a) | 0.999995499 | 67.27 | 0.012435 |
| Şekil 10 (b) | Şekil 9 (b) | 0.999995673 | 68.07 | 0.016344 |
| Şekil 10 (c) | Şekil 9 (a) | 0.999994751 | 67.19 | 0.012301 |
| Şekil 10 (c) | Şekil 9 (b) | 0.999996525 | 67.97 | 0.016172 |

## 4 Kaynaklar

[1] Akademik Bilişim Konferansları, "Biyometrik Güvenlik Sistemleri". http://ab.org.tr/ab09/sunum/102.pdf (01.07.2016).

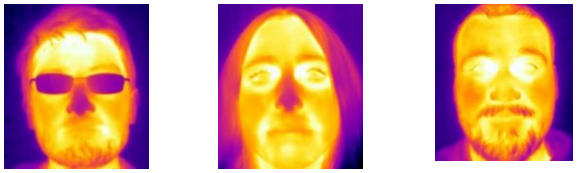
[2] Hao RAF, Daugman J. "Combining crypto with biometrics effectively". *IEEE Transactions on Computers,* 55(9), 1081-1088, 2006.

[3] Champakamala BS, Padmini K, Radhika DK. "Least significant bit algorithm for image steganography". *International Journal of Advanced Computer Technology (IJACT),* 3(4), 34-38, 2012.
[4] Gupta S, Gujral G, Aggarwal N. "Enhanced least significant bit algorithm for image steganography". *International Journal of Computational Engineering & Management,* 15, 40-42, 2012.
[5] Gupta S, Goyal A, Bhushan B. "Information hiding using least significant bit steganography and cryptography". *International Journal of Modern Education and Computer Science*, 4(6), 27, 2012.
[6] Elçi B. Bir Steganografi (Resmin İçine Veri Gizleme) Sisteminin FPGA Üzerinde Tasarımı ve Gerçeklenmesi. Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2008.
[7] Kahraman N, Özcan GS, İbişhükçü R. "Infrared face recognition in forensics via texture analysis". *Proceedings of 2016 Annual International Conference on Innovative Technologies and Advanced Computing (ICIAC-16),* Londra, UK, 24-25 March 2016.
[8] Sojan S, Kulkarni R.K. " Fingerprint Image Enhancement and Extraction of Minutiae and Orientation ". *International Journal of Computer Applications,* 145(4), 14-19, 2012.
[9] Xiao Y, Sun B, Chen H, Guizani S, Wang R. "Performance Analysis of Advanced Encryption Standard (AES)". *IEEE Globecom 2006,* San Francisco, CA, USA, 27 November - 1 December 2006.
[10] Yerlikaya T, Buluş E, Buluş N. "Kripto algoritmalarinin gelişimi ve önemi". *Akademik Bilişim Konferansları*, Denizli, Türkiye, 9-11 Şubat 2006.
[11] Subramanyan B, Chhabria VM, babu TGS. "Image encryption based on aes key expansion". *2nd International IEEE Conference on Emerging Applications of Information Technology,* Washington, DC, USA, 19-20 February 2011.
[12] Rouvroy G, Standaert FX, Quisquater JJ, Legat JD. "Compact and efficient encryption/decryption module for FPGA implementation of the AES rijndael very well suited for small embedded applications". *Information Technology: Coding and Computing,* 2, 583-587, 2004.
[13] Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R. "A modified AES based algorithm for image encryption". *International Journal of Computer Science and Engineering*, 1(1), 70-75, 2007.
[14] Granado-Criado JM, Vega-Rodríguez MA, Sánchez-Pérez JM, Gómez-Pulido JA. "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration". *Integration, the VLSI Journal,* 43(1), 72-80, 2010.
[15] National Institute of Standards and Technology, Federal Information "Processing Standards Publication 197 (FIPS197)". http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (01.07.2016).
[16] Xintong KC. "Understanding AES Mix-Columns Transformation Calculation". *University of Wollongong*, 2014.
[17] Boneh D, Franklin M. "Efficient generation of shared RSA keys". *Annual International Cryptology Conference*, Springer Berlin Heidelberg, California, USA, 17-21 August 1997.
[18] Zhou, X, Tang X. "Research and implementation of RSA algorithm for encryption and decryption" *6th International Forum* in *Strategic Technology (IFOST),* Heilongjiang, Harbin, 22-24 August 2011.
[19] Neeta D, Snehal K, Jacobs D. "Implementation of LSB steganography and its evaluation for various bits". *1st International Conference on Digital Information Management*, Bangalore, India, 6 Dec 2006.
[20] Chang HW, Zhang QW, Wu QG, Gan Y. "Perceptual image quality assessment by independent feature detector". *Neurocomputing*, *151*, 1142-1152, 2015.
[21] Hore A, Ziou D. "Image quality metrics: PSNR vs. SSIM". *20th International Conference on Pattern Recognition (ICPR),* İstanbul, Turkey, 23-26 August 2010.

## Ek A

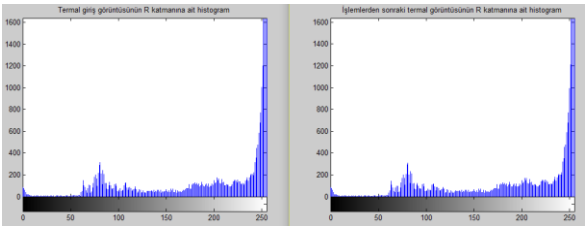
(a) (b)

Şekil 9: Parmak izi görüntüsü örnekleri.

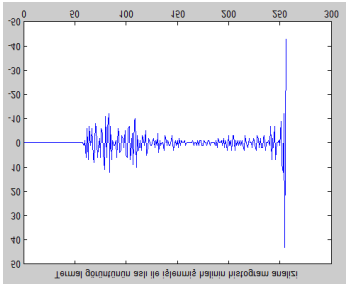


(a) (b) (c)

Şekil 10:Kullanılan termal görüntüler.



Şekil 11: Soldaki grafik işlem görmemiş termal görüntüye ait histogram grafiğidir. Sağdaki grafik ise içerisine AES algoritması ile şifrelenmiş biyometrik verinin termal görüntüye gömülmüş görüntüye ait histogram grafiğidir.



Şekil 12: Verilen grafik içerisine orijinal giriş olan termal görüntü ve biyometrik veri gömülmüş görüntü histogramlarının farkıdır.