

Parmak İzi Kullanarak Görüntü Şifreleme

Nazlı Akın¹, Büşra Takmaz², Erdal Güvenoğlu³

^{1,2,3}Maltepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

nazliakin88@gmail.com, busra.mix@hotmail.com, erdal@maltepe.edu.tr

Özet: Parmak izi tanıma, yüz tanıma, el geometrisi tanıma gibi tekniklerle karşımıza çıkan biyometri; günümüzde en çok yüksek güvenlik gerektiren alanlarda kullanılmaktadır. Güvenilirliği ve performansı bakımından kullanım kolaylığı sebebiyle çok sık kullanılan biyometrik teknik parmak izi tanımadır. Parmak izi okuyucusu yardımıyla veya dosyadan alınan parmak izi resimleri görüntü azalımı, kontrast iyileştirme, özellik çıkarma algoritmaları, inceltme algoritmaları gibi işlemlerden geçerek sayısal bir veriye dönüştürülüp, veritabanına kaydedilmektedir. Bu çalışmada, parmak izi tanıma algoritmalarından faydalanılarak elde edilen sayısal veri yardımı ile görüntü şifrelemek için kullanılabilir bir sistem mimarisi önerilmiştir.

Anahtar Sözcükler: Parmak İzi, Sayısal Görüntü, Görüntü Şifreleme

Image Encryption By Using Fingerprint

Abstract: Biometric which encountered in such as the fingerprint recognition, face recognition, hand geometry techniques are used in areas that require the very highest safety in this day and time. Due to the ease of use in terms of reliability and performance, biometric technique is used very often for fingerprint recognition. By means of fingerprint readers or taken from the fingerprint images file; noise reduction, contrast enhancement, feature extraction algorithms, through processes such as thinning algorithms is converted to a numeric data to the database are recorded. In this study, a system architecture is proposed to use for encrypt the image with the help numeric data which obtained utilizing the fingerprint recognition algorithms.

Keywords: Fingerprint, Digital Image, Image Encryption

1. Giriş

Sistemler arası bağlantılarda ya da iki nokta arasındaki haberleşmede, verilerin güvenli bir şekilde iletilmesi gerekmektedir. İletişimde, açık haberleşme kanalı kullanıldığında, gizli tutulmak istenen bilginin yetkisiz kişiler tarafından ulaşılabilirliği veya haberleşme kanalına girip veriyi bozabileceği ya da değiştirebileceği düşüncesi her zaman önemli bir problem oluşturmaktadır. Bu problemin giderilmesi, gönderilen verinin şifrelenmesi ile ortadan kaldırılabilir. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanmaktadır.

Şifreleme, askeri ve diplomatik ilişkide güvenliği sağlamak için uzun yıllardır kullanılmaktadır. Ancak günümüzde özel sektörde de verilerin güvenliğinin sağlanmasına gereksinim duyulmaktadır. Sağlık hizmetleri, finans, bankacılık gibi pek çok sektörde bilgisayarlar arasındaki haberleşme açık kanalları kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında veri iletiminin güvenliği ve gizliliğinin sağlanması için şifrelemeye vazgeçilemez bir ihtiyaç olmuştur. Yakın geçmişte bir sisteme kim olduğunuzu kanıtlamanızın ve veriye ulaşmanızın

geleneksel yolu şifreler ve PIN numaraları kullanmak idi. Fakat bu yöntemler, günümüzde süper bilgisayarların işlem kapasitelerinin artması ve şifrelerin kolaylıkla kırılabilmesinden dolayı güvenliğini kaybetmiştir. Bu durum, güvenliğin daha yüksek seviyelerde sağlanabileceği biyometrik tanıma sistemleri ile giderilebilmektedir.

Biyometrik sistemler temelde, kişinin sadece kendisinin sahip olduğu, değiştiremediği ve diğerlerinden ayırt edici olan, fiziksel veya davranışsal bir özelliğinin tanınması ile çalışmaktadırlar. “Bio” (yaşam) ve “metron” (ölçüm) kelimelerinden türeyen biyometrik, biyolojik veriyi ölçme ve istatistiksel olarak analiz etme bilimidir. Bilişim teknolojisi ile birlikte biyometrik genel olarak insan vücudunun parmak izi, el geometrisi, retina ve iris, ses, yüz şekilleri gibi özellikleriyle ilgilenir ve bunları doğrulama ve/veya kimlik tespiti için kullanır. Biyometri, kullanıcının fiziksel ve davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş bilgisayar kontrollü otomatik sistemler için kullanılan genel bir terimdir[1]. Bu çalışmada, biyometrik sistem olarak parmak izi kullanılmıştır. Parmak izi bilgisi her birey için farklıdır. Bu nedenle çalışmada, her bireyde farklı olan parmak izi bilgisini kullanan, parmak izinden elde

edilen sayısal veriler yardımıyla görüntülerin şifrenmesini sağlayan bir sistem mimarisi önerilmiştir.

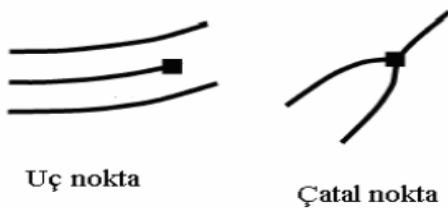
2. Parmak İzi

Biyometrik tanıma sistemlerinde en fazla kullanılan parmak izi, güvenlik ve personel takibi gibi pek çok alanda karşımıza çıkmaktadır. Parmak izi, parmak ucunda gözle görünen, girintili çıkıntılı bir haritaya benzeyen ve deri tabakasının parmak ucunun hafifçe bastırılması ile ortaya çıkan görüntüdür. Bu görüntü kişiye özel, yanık veya derin kesikler olmadığı sürece değişmeyen, yaşlanmayan ve taklit edilemeyen bir yapıdadır. Örnek bir parmak izi görüntüsü Şekil 1’de gösterilmektedir.



Şekil 1. Parmak izi görüntüsü[2],

Parmak uçları dikkatlice incelendiğinde birbirinden farklı birçok çizgi görülmektedir. Derinin epidermis tabakasında yer alan bu kavisli çizgilere tepe ve çizgilerin arasında kalan boşluklar ise vadi olarak tanımlanmaktadır[3]. Tepe çizgilerinin bazıları aniden sonlanırken bazıları ikiye ayrılarak devam etmektedir. Tepe çizgisindeki bu ani sonlanan noktaya uç, ikiye ayrılarak devam eden noktaya ise çatal nokta adı verilmektedir. Bu noktalar parmak izinin öznitelik noktalarıdır ve her bireyin parmak izinde farklı dizilişleri ve yönleri vardır. Şekil 2’de örnek bir uç ve çatal nokta gösterilmiştir.



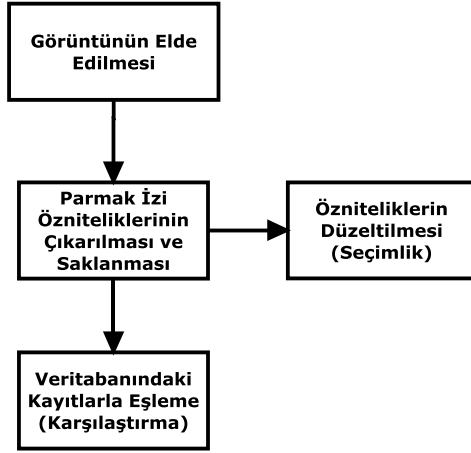
Şekil 2. Uç nokta ve çatal nokta[4]

2.1. Parmak İzi Tanıma Yöntemleri

Günümüzde parmak izi tanıma filtreleme ve öznitelik tabanlı olmak üzere iki yöntemle yapılmaktadır. Filtreleme tabanlı tanımda parmak izi gabor filtresinden geçirilmektedir. Gabor filtresi, görüntü analizinde kullanılan önemli yöntemlerden biridir. Filtre yardımıyla bir görüntü üzerinde belli bir yöne uzanan ayrıtlar tespit edilebilmektedir[5]. Gabor filtresinin kullanılmasıyla parmak izinin özellik vektörü oluşturulmaktadır. Oluşturulan bu özellik vektörü veri tabanındaki verilerle kıyaslanarak parmak izi eşleşmesi yapılmaktadır.

Öznitelik tabanlı parmak izi tanıma yönteminde öznitelik noktalarının birbirleriyle olan ilişkileri kullanılmaktadır. Bu yönteminin tam verimle kullanılabilmesi için parmak izi okuyucusundan alınan parmak izi görüntüsünün sorunsuz ve güvenilir olması gerekmektedir. Öznitelik tabanlı parmak izi tanımda, parmak izinin öznitelik noktaları bulunur. Bu nokta kümesiyle veri tabanındaki nokta kümeleri arasında bir dizi eşleme algoritmaları kullanarak parmak izi tanıma yapılır. Parmak izi görüntüsünden çıkarılan bu öznitelikler sonucundaki parmak izi tanıma başarısı, görüntünün kalitesi ile doğru orantılıdır. Genellikle alınmış olan parmak izi görüntüsü, özniteliklerin doğrudan ve güvenilir olarak bulunabileceği kadar kaliteli değildir. Bu sebepten dolayı görüntülerde iyileştirme algoritmaları kullanılarak gerekli olan minimum kalite sağlanarak öznitelik noktaları çıkartılmaktadır. Genel olarak parmak izi görüntüsünün iyileştirilmesi, parmak izinin inceltilmesi, yönsel histogramlar veya fourier dönüşümü, özellik noktalarının hizalanması, merkez nokta gibi yöntemlerle gerçekleştirilir.

Filtreleme tabanlı yaklaşımda, öznitelik tabanlı yaklaşımdan farklı olarak görüntüye ön işlem yani iz yönlerinin bulunması, görüntünün iyileştirilmesi, segmentasyon gibi aşamaları olmaksızın, parmak izi görüntüsünün öz yapısından elde edilen iz yönleri, frekansları gibi veriler üzerinden çalışılmaktadır. Görüntü üzerinde dalgacık (wavelet) dönüşümü yapılarak parmak izi tanıma çalışmaları yapılmaktadır. Filtreleme tabanlı tanıma yöntemi görüntünün büyüklüğü, dönüklüğü, açıklığı, kalite farkı gibi durumlardan etkilenmektedir. Ancak öznitelik tabanlı tanıma yöntemleri parmak izi görüntüsünün kalitesi, dönüklüğü, büyüklüğü gibi durumlardan etkilenmemektedir. Bir parmak izi tanıma sisteminin genel tanıma aşamaları Şekil 3’de gösterilmektedir.



Şekil 3. Parmak izi tanıma aşamaları[3]

3. Görüntü Şifreleme

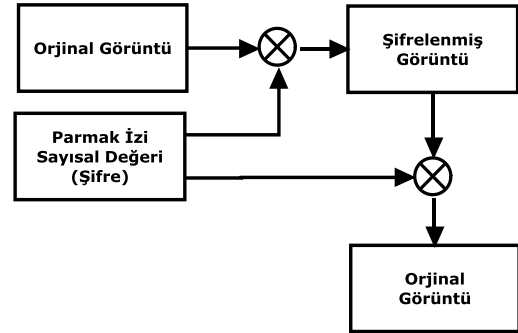
AES (Advanced Encryption Standard - Gelişmiş Şifreleme Standardı), elektronik verinin şifrenmesi için sunulan bir standarttır. Amerikan Hükümeti tarafından kabul edilen AES, uluslararası alanda da defacto şifreleme (kripto) standardı olarak kullanılmaktadır. DES' in (Data Encryption Standard - Veri Şifreleme Standardı) yerini almıştır [12]. Bu yöntemler aslında bir dizi sayısal veriden ibaret olan resim dosyalarının şifrenmesinde de kullanılabilir. Ancak bu yöntemlerle birlikte iki önemli sakınca ortaya çıkmaktadır. Bunlardan ilki; resim verileri metin verilerine göre çok büyüktür ve geleneksel yöntemlerle şifrenmesi çok zaman almaktadır. İkincisi, şifrenmiş metin tam olarak orijinal haline çevrilmedikçe içeriği anlaşılabilirken, resim verilerinin kısmen çözülmesi bile içeriğinin anlaşılması için yeterli olmaktadır. İnsan algısı çözümden kaynaklanan hatayı göz ardı edebilmektedir. Görüntülerin kısmen veya tamamen çözülmesini engellemek için çeşitli resim şifreleme teknikleri geliştirilmiştir [6].

Resim şifreleme algoritmalarının üç temel fikri vardır. Bunlar; değer dönüşümü[7-8-9], yerel permütasyon [10-11] ve değer dönüşümü ile yerel permütasyon yöntemlerinin kombinasyonlarıdır [10]. Değer dönüşümü, orijinal pikselin veri değerinin algoritmadaki işleme tabi tutulduktan sonra aldığı yeni değer olarak tanımlanmaktadır. Yerel permütasyon algoritmaları, orijinal piksel verisinin bulunduğu pozisyonunun yer değiştirmesi olarak ifade edilmektedir. Bunların kombinasyonları ise; her iki yöntemin birlikte kullanılması ile gerçekleştirilmektedir. Sonuçta resim şifreleme yaklaşımlarında esas olarak, resmi oluşturan pikselleri temsil eden sayısal değerlerin değiştirilmesini veya bu piksellerin resimdeki yerlerinin değiştirilmesini

sağlamaktır. Doğal olarak her iki yaklaşımda da geriye dönüşüm yapılarak orijinal resmin elde edilebilmesi beklenir. Bu çalışmada, görüntülerin şifrenmesi ve çözülebilmesi için değer dönüşümü yöntemi kullanılmıştır.

4. Gerçekleştirilen Sistem Mimarisi

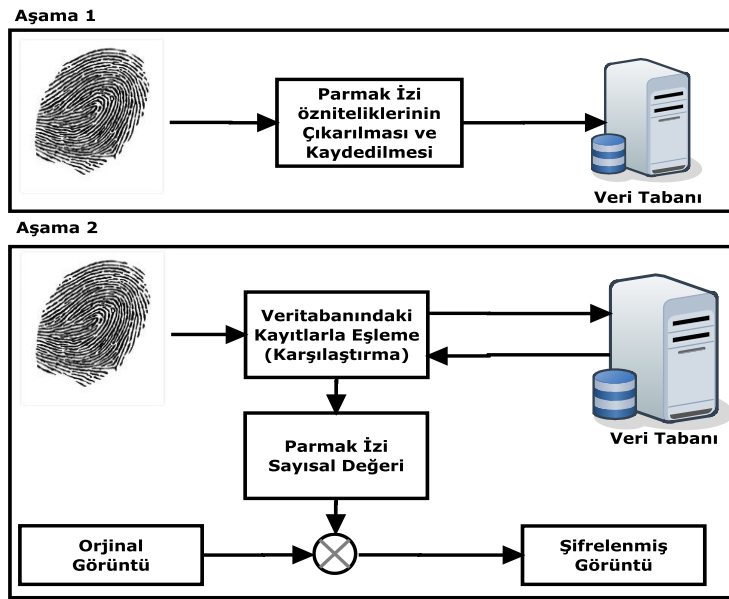
Parmak izi yardımı ile görüntülerin şifrenmesi için gerçekleştirilen sistemin genel işleyiş mimarisi Şekil 4'te gösterilmektedir. Mimari, parmak izi özniteliklerinin çıkarılması ve saklanması, özniteliklerden faydalanarak sayısal veri elde edilmesi ve görüntünün şifrenmesi bileşenlerinden oluşmaktadır. Görüntülerin şifrenmesi için değer dönüşümü yöntemi kullanılmıştır. Değer dönüşümü yöntemi, görüntünün (i,j) noktasındaki piksel değeri ve parmak izi sayısal değerinin XOR işlemine tabi tutulmasıyla gerçekleştirilmiştir. Bu işlem de orijinal görüntünün tekrar elde edilebilmesi için şifreli görüntünün (i,j) noktasındaki piksel değeri ile yine parmak izi sayısal değerinin XOR işlemine tabi tutulması yeterlidir. Şifreleme işleminin blok diyagramı Şekil 5'de gösterilmektedir.



Şekil 5. Görüntü şifreleme ve deşifreleme blok yapısı

Parmak izi verisi kullanılarak gerçekleştirilen şifreleme ve deşifreleme işlemlerinin Delphi kodu aşağıda verilmiştir. Orijinal görüntünün XOR işlemine tabi tutulması şifrenmiş görüntünün elde edilmesini, şifrenmiş görüntünün tekrar XOR işlemine tabi tutulması ise orijinal görüntünün elde edilmesini sağlamaktadır. Bu nedenle önerilen yöntemde şifreleme ve deşifreleme işlemleri aynı yöntemi kullanmaktadırlar.

```
procedure Sifreleme(const OrjinalResim: TBitmap;  
Key: Integer);  
  
var  
BytesPorScan: Integer;  
  
w, h: integer;  
  
giris,cikis: pByteArray;  
  
begin  
  
try  
  
SifreliResim:= TBitmap.Create;  
  
SifreliResim.Width := OrjinalResim.Width;  
  
SifreliResim.Height:= OrjinalResim.Height;  
  
Satir_Sayisi:= OrjinalResim.Width;
```



Şekil 4. Sistemin genel işleyiş mimarisi

5. Sonuçlar ve Öneriler

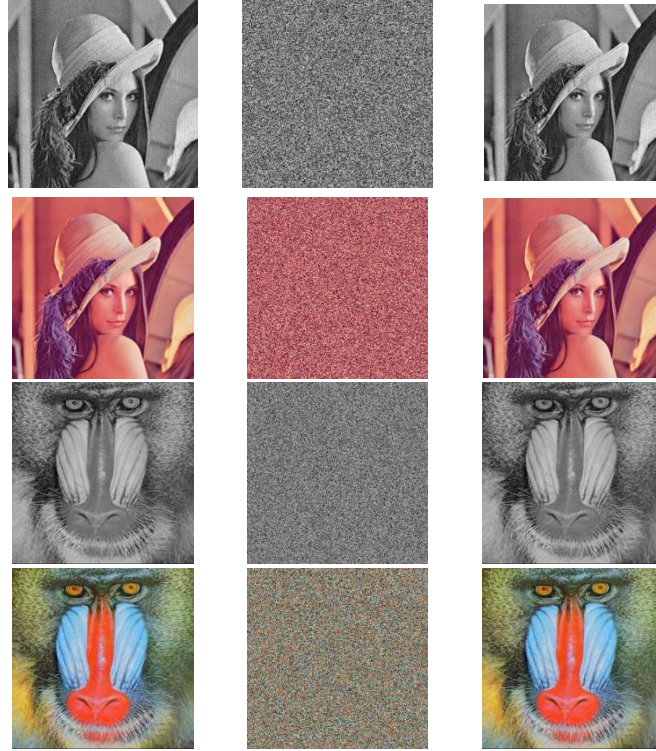
Bu bölümde önceki kısımlarında detayları verilen yöntemin uygulanması ile elde edilen sonuçlar ele alınmaktadır. Günümüzde bilinen birçok yöntemin uygulanması, kolay olması nedeni ile gri resimler üzerinde gerçekleştirilmektedir. Fakat önerilen sistemde, resmin türünün ve biçiminin önemli olmadığı görülmüştür.

Geliştirilen sistemi test etmek amacıyla oluşturulan yazılım, Delphi 2005 programlama dilinde kodlanıp ve

Windows 7 işletim sisteminde Intel Core 2 DUO 2.53 GHz işlemci ve 4GB ana belleğe sahip bilgisayar üzerinde çalıştırılmıştır. Uygulamanın hızına dair bir fikir olması bakımından elde edilen değerler Tablo 1’de, görüntü şifreleme alanında sık kullanılan gri ve renkli tonlamalı “lena.bmp” resimleri ile 24 bit gri ve renkli tonlamalı “baboon.bmp” resimlerinin şifrelenmiş ve şifresi çözülmüş görüntüleri ise Şekil 6’da gösterilmektedir.

Tablo1. Görüntü şifreleme ve deşifreleme süreleri ve veri miktarları

Resim	Resmin Boyutu	Şifrelenen Veri Miktarı[Byte]	Şifresi Çözülen Veri Miktarı [Byte]	Şifreleme Süresi [msn]	Şifre Çözme Süresi [msn]
Lena.bmp(gri)	256x256	196662	196662	70	69
Lena.bmp(renkli)	256x256	196662	196662	70	70
Baboon.bmp (gri)	256x256	196664	196664	69	69
Baboon.bmp(renkli)	256x256	196662	196662	79	86



Şekil 6. Şifrelenmiş ve deşifrelenmiş görüntüler

Şifreleme ve şifre çözme işlemlerinin başarılı olabilmesi için herhangi bir veri kaybının olmaması gerekmektedir. Bu nedenle şifreleme ve deşifreleme işlemleri yapıldıktan sonra şifreli ve orijinal resim arasındaki ortalama karesel hatanın (MSE - mean squared error) bulunması geliştirilen yöntemin başarısı hakkında fikir elde etmemizi sağlayacaktır.

MSE, iki resim arasındaki farkı belirlemek için kullanılmaktadır.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (Y_{ij} - S_{ij})^2$$

Yukarıda S orijinal görüntüyü ve Y şifrelenmiş görüntüleri, M ve N orijinal görüntünün gerçek boyutlarını göstermektedir. Elde edilen MSE değerleri ve orijinal görüntü ile şifresi çözülmüş görüntülerin piksel piksel karşılaştırılmasıyla elde edilen sonuçlar Tablo 2’de verilmektedir.

Tablo 2. Orijinal ve işlenmiş görüntülerin MSE değerleri

Görüntü	MSE	Şifrelenen Resim Piksel Sayısı	Şifresi Çözülmüş Resim Piksel Sayısı	Piksel Kaybı	Benzerlik (%)
Lena.bmp (gri)	0	65536	65536	0	100
Lena.bmp (renkli)	0	65536	65536	0	100
Baboon.bmp(gri)	0	65536	65536	0	100
Baboon.bmp(renkli)	0	65536	65536	0	100

MSE denklemi kullanılarak yapılan testte herhangi bir piksel kaybının olmadığı görülmüştür. MSE' nin 0'a yakınlığı, öne sürülen modelin yeterliliğini göstermektedir.

Önerilen yöntemde, her ne kadar görüntü şifreleme alanında sıklıkla kullanılan "Lena.bmp" ve "Baboon.bmp" kullanılmış olsa da, bilinen farklı görüntü formatlarını ve büyük boyutlardaki resimleri kolaylıkla şifreleyebilmekte ve deşifreleyebilmektedir. Orijinal görüntünün elde edilebilmesi ancak parmak izinden elde edilen anahtar verisinin bilinmesi ile mümkündür. Anahtarın deneme ile bulunması güçtür.

Yöntemde, görüntü piksellerinde çakışma mümkün olmadığından herhangi bir veri kaybı meydana gelmemektedir. Dolayısı ile Tablo 2 dikkate alındığında önerilen parmak izi ile görüntü şifreleme yönteminin başarılı olduğu söylenebilmektedir.

6. Kaynaklar

[1] <http://www.pitsteknoloji.com/biyometrik-sistemler.php>, Erişim Tarihi: 20.11.2012.

[2]<http://www.artelektronik.com/parmak-izi.html>, Erişim Tarihi: 20.11.2012.

[3] Ayan, K. And Demir, Y. E. "Öznitelik Tabanlı Otomatik Parmak İzi Tanıma" Eleco International Conference On Electrical And Electronics Eng. ,2004.

[4] Özkaya,N., Sağıroğlu, Ş., Beştok, E., "Genel Amaçlı Otomatik Parmak İzi Tanıma Sistemi Tasarım Ve Gerçekleştirilmesi", Politeknik Dergisi, 8, 3, 239-247, 2005.

[5] Varlık, A., Çorumluoğlu, Ö., "Dijital Fotogrametri Teknikleri İle Kişi Tanıma", Harita Teknolojileri Elektronik Dergisi, 3, 2, 1-24, 2011.

[6] Güvenoğlu, E., Esin, E.M., "Knutt / Durstenfeld Shuffle Algoritmasının Resim Şifreleme Amacıyla

Kullanılması", Journal of Polytechnic, 12(3), pp. 151-155, 2009

[7] Sinha,A., Singh, K., "A technique for image encryption using digital signature", Optics Communications, pp. 1-6, 2003.

[8] Maniccam, S.S., Bourbakis, N.G., "Lossless image compression and encryption using SCAN", Pattern Recognition , 34, 1229-1245, 2001.

[9] Chang, C. C., Hwang, M. S., Chen T. S., "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software, 58, 83-91, 2001.

[10] Guo, J. I., Yen, J. C., "A new mirror-like image encryption algorithm and its VLSI architecture", In Proc. 10th (Taiwan) VLSI Design/CAD Symposium, 319-322, 1999.

[11] Yen J.C., Guo, J.-I., "A new chaotic image encryption algorithm",In: Proceedings of (Taiwan) National Symposium on Telecommunications, pp. 358-362, 1998.

[12] <http://tr.wikipedia.org/wiki/AES>, Erişim Tarihi: 20.11.2012.