24 Bit Renkli Dokümanların Farklı Biyometri Teknoloji Kullanılarak Güvenliğinin Sağlanması

Mehmet Kıvılcım Keleş, Ali Güneş

***Özet* — Günümüzde fiziksel dokümanların saklanması, erişimi ve kullanım konularında çeşitli zorluklar vardır. Bilişim ve iletişim teknolojilerindeki gelişmeler fiziksel dokümanların dijital olarak saklanmasını gündeme gelmiştir. Sonuçta birçok kurum ve kuruluş dokümanlarını dijital ortama taşımıştır. Ancak dokümanların dijital ortama taşınması bu alandaki sorunları toptan çözmemiş, aksine yeni sorunların ortaya çıkmasına neden olmuştur. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması ve içindeki bilgilere erişilmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilir. Bu çalışmada, dijital doküman oluşturulma aşamasında veya oluşturulduktan sonra biyometrik yöntemlerle nasıl güvenliğinin sağlanabileceği üzerinde durulmuştur. Çalışmada, avuç damar izi okuyucular kullanılarak oluşturulan biyometrik veriyi, dijital filigran yöntemi ile saklamak ve dokümanı bu şekilde şifreleme konusu ele alınmıştır. Çalışmada 24 renkli dijital bir doküman avuç damar izi teknolojisi kullanarak Steganografi yöntemi ile şifrelenmektedir. Doküman güvenliğinin sağlanması, erişimi ve ilk oluşturanın tespit edilmesi konusunda da, Parmak izi ve avuç damar izi teknolojileri karşılaştırılarak başarı oranları ve süreleri karşılaştırılmaktadır.**

Anahtar Kelimeler — Avuç Damar izi, Doküman güvenliği, Dijital filigran, Şifreleme, , Parmak izi

Abstract — Today, storage, access and usage of the physical documents present various difficulties. The emergences of information and communication technologies have enabled physical documents to be stored as digitally. As a result, many agencies and institutions have moved their physical documents to digital environment. However, transformation of documents to digital media did not solve the problems relating to document, but has led to the emergence of new problems. When these documents are digitized, unauthorized access to the information may present risky consequences. This situation may result in violation of secrecy and theft of information on the document. In this study, we will discuss how security can be achieved by using biometric methods during or after the creation of 24 bit color digital documents. In this study, we will cover the use of palm vein biometric data being used as a digital watermark, in order to secure the document with this encryption method. Also, we will analyze how palm vein data is used as steganography method for encryption and recognition technology in 24 bit color digital documents. These methods are used in providing security of the document for access, and also to identify the creator. Fingerprint and palm vein technologies are compared in regards to their success rates and times.

Keywords— 24 Bit Document security, Biometry, Encryption, Palm Vein, Fingerprint, Watermarking.

I. GİRİŞ

SON yıllarda network altyapısının iyileşmesi ve bulut teknolojilerinin gelişmesi ile dijital ortamdaki dokümanlarda bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Özellikle internetin de yaygınlaşması güvenlik açıklarını beraberinde getirmiş, bunun sonucu olarak da dijital veri güvenliği önemli bir boyut kazanmıştır. Dijital ortama taşınan dokümanların çalınması, yetkisiz kullanıcılar tarafından açılması, içindeki bilgilere erişilmesi ve değiştirilmesi telafisi çok güç sonuçlar doğurabilmektedir. Bu durum dokuman gizliliğinin ihlali ve bilginin çalınması gibi durumlar doğurabilmektedir.

Dijital veri güvenliğini sağlamak amacıyla çeşitli koruma mekanizmaları geliştirilmiş, yeni teknoloji ve uygulamalar ortaya çıkmıştır. Günümüzde en sık kullanılan teknolojilerden biri şifrelemedir. Bu teknoloji de korunması istenen veri, şifreleme algoritmaları ve bir anahtar yardımı ile anlaşılmaz hale dönüştürülmektedir. Ancak şifrelerin zaman içinde kırılabilmesi, unutulması veya çalınması durumları sıklıkla karşımıza çıkmaktadır. Zaman içinde veri güvenliği için şifrelerin tek başına yeterli olmadığını göstermektedir. İşte bu noktada steganografi bilimi gündeme gelmektedir.

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [1]. Steganografi kökleri binlerce yıl öncesine dayanan bir bilim dalıdır [2]. Görüntü dosyaları üzerinde bilgi gizlemek için geliştirilmiş yöntemleri 3 başlık altında sınıflandırabiliriz. Bunlar En önemsiz bite ekleme, Maskeleme ve filtreleme, Algoritmalar ve dönüşümler [3].

II. DİJİTAL DOKÜMANLARIN YAPISI

Bilgisayar ortamında dijital dokümanlar 24 bit renkli, 8 bit renkli, 4 bit renkli, 8 bit gri tonlamalı, 4 bit gri tonlamalı veya 1bit siyah beyaz olarak saklanırlar. Görüldüğü gibi, 24 bit renkli dokümanlar bilgi saklamak için en fazla alanı sağlamakta ve farklı şifreleme algoritmaları kullanabilme imkânı vermektedir. 24 bit veya 8 bit Renkli dokümanlarda bütün renk değişimleri üç temel rengin birleşmesiyle elde edilir. Bu tip resimler, resimde kullanılan renkleri içeren 256 renkli bir palet taşırlar. Her piksel bu palette bir renge karşılık gelen 3 baytlık değer taşır.

III. BİYOMETRİ TEKNOLOJİSİ

Biyometrik sistemler temelde, kişinin sadece kendisinin sahip olduğu, değiştiremediği ve diğerlerinden ayırt edici olan, fiziksel veya davranışsal bir özelliğinin tanınması ile çalışmaktadırlar [4]. Biyometrik uygulamalar için de en yaygın olarak kullanılmaya başlanan özellik parmak izi tanıma yöntemidir [5]. Parmak izi, elde edilmesinin kolay olması ve kriminal alanda da kullanılabilir olması önemli tercih sebebidir. Biyometrik yaklaşımlar içinde avuç içi, diğer modellere göre yeni bir biyometrik özelliktir [6]. Avuç içi biyometri teknolojisi avuç içindeki damar yapısının sayısallaştırılması sonucu elde edilir. Avuç içi diğer biyometrilere göre en büyük avantajı taklit edilmesinin daha zor olması ve avuç içi özelliklerinin karakteristik, kalıcı ve dış faktörlerden daha az etkilenebilir olmasıdır. Şekil 1 de Avuç içi damar yapısı ile parmak izi görüntüleri gösterilmektedir.

Sekil 1. Avuç damar İzi ve Parmak izi resmi

Farklı biyometri teknolojileri geliştirilmiş olmasına rağmen genel yaklaşım olarak hepsi birbirine teknolojik olarak yakındır. Biyometrik tanıma sistemlerinde, ilk adım görüntüyü kaydetmektir. Bu görüntü sayısal koda çevrilir. Bu kod şifreleme algoritmaları kullanarak şifrelenir ve bilgisayara kaydedilir. Daha sonra kullanıcı herhangi bir biyometrik cihaz kullanarak kendini sisteme tanıtır. Kullanıcının kendini sisteme tanıttığı andaki duruşu ve çevre koşullarından dolayı sistem de kayıtlı olan sayısal kod ile doğrulama aşamasında üretilen kodun birbiriyle tamamıyla aynı olma olasılığı yoktur [7]. Biyometri teknolojilerinde kişi doğrulaması için kayıt olan sayısal kod ile üretilen kodun birbiriyle belirli oranda tutması yeterlidir.

IV. VERİ SAKLAMA YÖNTEMİ – EN ÖNEMSİZ BİTE EKLEME

En önemsiz bite ekleme yöntemi yaygın olarak kullanılan bir yöntemdir. Bu yöntemde; görüntüdeki her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri belirlenmiş olan bir fonksiyon ile birer birer yerleştirilmektedir. Bu yöntemde eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'nın en az anlamlı biti olmasından dolayı, değişimler insan tarafından algılanamaz boyutta olmaktadır [8].

Örnek olarak saklamak istediğimiz bir biyometrik verinin 1 byte'nın ikili sistemdeki değeri: 101101101 olsun.

Biyometrik verinin saklanacağı resmin 3 pikselinin değeri:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Resmin içine "101101101" biyometrik veri gizlendiğinde oluşan yeni piksel değerleri aşağıdaki gibi olmaktadır.

10010101 0000110**0** 11001001
1001011**1** 0000111**0** 1100101**1**
10011111 00010000 11001011

Bilginin gömülmesinden sonra bitlerin eklendiği sekiz bayttan sadece dördünde değişiklik meydana geldiği görülmektedir.

V. GÖRÜNTÜ ŞİFRELEME YÖNTEMİ – KARMAŞIK RESİM ŞİFRELEME ALGORİTMASI

Bu çalışmada görüntü şifreleme yöntemi olarak, karmaşık resim şifreleme algoritması kullanılmıştır. Bu algoritma, Chang ve Chen tarafından sunulan karmaşık bir sisteme dayalı yeni bir resim şifreleme yöntemidir [9]. Bu algoritma herhangi bir veri kaybı olmadan, yer değiştirme özelliğini kullanan bir şifreleme algoritmasıdır.

MXN büyüklüğündeki bir görüntüyü f fonksiyonu ile gösterirsek. (x, y) f görüntüsünün koordinatlarını göstermek üzere 0< x < M-1, 0< y < N-1 olacak şekilde f(x, y), görüntüsünün (x, y) noktalarındaki gri görüntü seviyesini göstermektedir,

Algoritma aşağıdaki gibi tanımlanmıştır.

Tanım 1: ROLRJp: f — f eğer /=0 ise f resmindeki i. satırı (0 < i < M-1), p piksel sola, /=1 ise p piksel sağa döndürmek için tanımlanmıştır [10].

Tanım 2: ROUDJ^p: f — f eğer /=0 ise f resmindeki j. sütun (0 < j < N-1), p piksel yukarıya, 1=1 ise p piksel aşağıya döndürmek için tanımlanmıştır [10].

Tanım 3: ROURf ^ p: f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x + y = k, 0 < k < M + N - 2, eğer 1=0 ise aşağı-sol yönünde p piksel, 1=1 ise yukarı-sağ yönünde p piksel döndürmek için tanımlanmıştır [10].

Tanım 4: ROULk^p: f — f f resmindeki (x, y) pozisyonundaki pikselleri döndürmek için tanımlanmıştır, öyle ki; x - y = k, -(N - 1) < k < M- 1, eğer 1=0 ise yukarı-sol yönünde p piksel, 1=1 ise aşağı-sağ yönünde p piksel döndürmek için tanımlanmıştır [9].

5x7 boyutunda verilen resmi aşağıda ele alalım.

$$\mathrm{ROLR}^{22}(f),\ \mathrm{ROUR}^{\wedge 2}(f)\ \text{ve}\ \mathrm{ROUL}_0^2 \setminus f)$$

İşlemlerinin sonuçları sırasıyla şekil 2'de gösterilmektedir [11].

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

a) Orjinal Resim

1	2	3	4	5	6	7
8	9	10	11	12	13	14
20	**21**	**15**	**16**	**17**	**18**	**19**
22	23	24	25	26	27	28
29	30	31	32	33	34	35

b) Sağa – Sola Öteleme

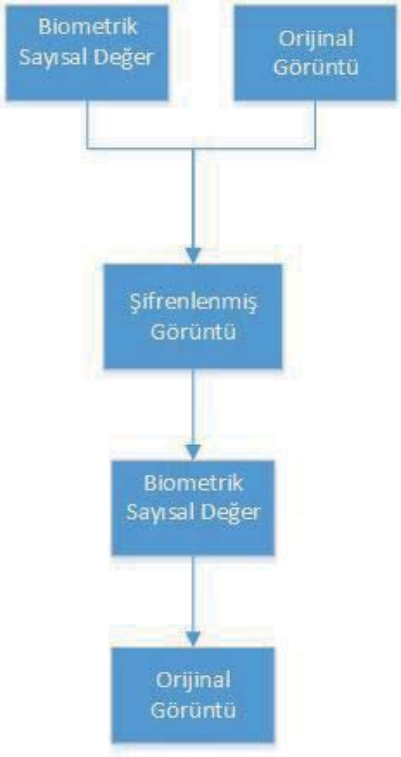
1	2	3	4	5	**18**	7
8	9	10	11	**24**	13	14
15	16	17	**30**	19	20	21
22	23	**6**	25	26	27	28
29	**12**	31	32	33	34	35

c) Sola Aşağı – Yukarı Öteleme

1	2	**19**	4	5	6	7
8	9	10	**27**	12	13	14
15	16	17	18	**35**	20	21
22	23	24	25	26	**3**	28
29	30	31	32	33	34	**11**

d) Sağa Aşağı – Yukarı Öteleme

Şekil 2. Karmaşık resim şifreleme algoritmasının matrislerde gösterilmesi



Şekil 3. Görüntü şifreleme ve çözme yapısı

VI. GERÇEKLEŞTİRİLEN SİSTEM MİMARİSİ

Parmak izi veya Avuç damar izi sayısal verileri ile görüntülerin şifrelenmesi ve görüntünün içine veri gizlenmesi için kullanılan sistem topolojisi şekil 3'de gösterilmektedir.

VII. SONUÇLAR

Bu çalışmada, kullanım oranı hızla artan dijital dokümanların güvenliği Parmak izi biyometrik verisi veya avuç damar izi biyometrik verisi kullanılarak şifrelenmesi anlatılmıştır.

Bu bölümde iki biyometrik verinin şifrelemede kullanılmasıyla elde edilen sonuçları ele alınmaktadır.

Program ile değişik boyutlardaki 24 bit resimler karmaşık şifre algoritması kullanılarak şifrelenmiş, parmak izi veya avuç damar izi veriler resmin içine gizlenmiştir.

Yapılan çalışmada gizlenmek istenen parmak izi verisi için farklı parmak izi sensörleri kullanılmış ve sensör cinsine göre parmak izi biyometrik verisinin 0,5-1 KB arası olduğu gözlemlenmiştir. Gizlenmek istenen Avuç damar izi biyometrik verisinin 2-3 KB arası olduğu tespit edilmiştir.

Biyometrik sayısal veri en önemsiz bite ekleme yöntemi kullanılarak resim içine gizlendiğin de resmin üzerinde gözle görünür bir bozulma olmadığı tespit edilmiştir.

Geliştirilen sistem, .net platformu üzerinde c# yazılım dili ile kodlanmıştır. Test amacıyla Windows 7 64 bit işletim sisteminde Intel i7 2.3 GHz işlemci ve 8GB ana belleğe sahip bilgisayar üzerinde çalıştırılmış ve Parmak izi veya Avuç Damar izi verisinin alınması dâhil şifreleme işleminin ortalama 2 saniye olduğu tespit edilmiştir.

Tablo 1 de, 24 bit renkli üç farklı bitmap resim için önce avuç damar izi sayısal verisi kullanılarak şifreleme işlemi yapılmış ve süreler ölçülmüştür. Aynı üç resim için parmak izi sayısal verisi kullanılarak işlem tekrar edilmiş ve bu süreler karşılaştırılmıştır.

Tablo 1. Avuç damar izi ve Parmak izi ile şifreleme karşılaştırma tablosu

Resim	Resmin Boyutu	Şifrelenen Veri Boyutu [Byte]		Şifreleme Süresi [sn]	Şifre Çözme Süresi [sn]
Örnek 1.bmp	2420X3464	Avuç Damar İzi	2393	2,6	2,5
		Parmak İzi	512	0,9	0,8
Örnek 2.bmp	1976X1147	Avuç Damar İzi	2142	2,1	2,2
		Parmak İzi	480	0,6	0,6
Örnek 3.bmp	1964X1101	Avuç Damar İzi	2215	2,0	1,9
		Parmak İzi	510	0,7	0,6

Oluşturulan yeni resim karmaşık resim şifreleme algoritması ile karıştırılmış olup orijinal görüntünün elde

edilebilmesi için parmak izi veya Avuç damar izi sayısal verisinin uygulama tarafından doğrulanması ile mümkündür.

KAYNAKLAR

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding–A Survey", Proceedings of the IEEE,Special Issue on Protection of Multimedia Content, 87(7):1062-1078,July 1999..

[2] Caldwell, 2nd Lt. J., "Steganography", CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).

[3] Sellars D., "An Introduction to Steganography", Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400 W/NIS04/papers99/dsellars/index.html

[4] Parmak İzi Kullanarak Görüntü Şifreleme Nazlı Akın1, Büşra Takmaz, Erdal Güvenoğlu Maltepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

[5] Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri 6th International Advanced Technologies Symposium (IATS'11), 16-18 May 2011, Elazığ, Turkey

[6] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. Pattern Anal. Mach. Intell. 955–966, 1995.

[7] J. D. Woodward, Jr., N.M. Orlans, P. T. Higgins,―Biometrics‖, McGraw-Hill, 2003

[8] Andaç ŞAHİN, Ercan BULUŞ, M.Tolga SAKALLI - 24-BİT RENKLİ RESİMLER ÜZERİNDE EN ÖNEMSİZ BİTE EKLEME YÖNTEMİNİ KULLANARAK BİLGİ GİZLEME Trakya Univ J Sci, 7(1): 17-22, 2006 ISSN 1305-6468

[9] CHANG C.C., Hwang M.S., Chen T.S.,2001, A new encryption algorithm for image cryptosystems, The Journal of Systems and Software.

[10] Erdal Güvenoğlu , Nurşen Suçsuz - Yer Değiştirme ve Değer Dönüştürme Özelliğine Sahip Görüntü Şifreleme Algoritmalarının Analizi - IX. Akademik Bilişim Konferansı Bildirileri 31 Ocak - 2 Şubat 2007 Dumlupınar Üniversitesi, Kütahya

[11] ÖZTÜRK İ, Soğukpınar İ, 2004. Analysis and Comparison of Image Encryption Algorithms, IJIT Volume 1 Number 2 ISSN:1305 - 239X.

Mehmet Kıvılcım KELEŞ (1986) Zonguldak Karaelmas Üniversitesinden 2011 yılında mezun oldu. Halen İstanbul Aydın Üniversitesinde yüksek lisansına devam etmektedir. Çalıştığı konular biyometrik sistemler ve görüntü işlemedir.

Ali GÜNEŞ (1952) Ortadoğu Teknik Üniversitesinden 1976 yılında mezun oldu. Halen İstanbul Aydın Üniversitesinde Bilgisayar mühendisliği bölümünde görev yapmaktadır.