VERİ ŞİFRELEME ALGORİTMALARININ KULLANIMI İÇİN AKILLI BİR SEÇİM SİSTEMİ GELİŞTİRİLMESİ

Menduh YILMAZ[1], Serkan BALLI [2]

Muğla Sıtkı Koçman Üniversitesi,
[1]Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı,
[2]Teknoloji Fakültesi / Bilişim Sistemleri Mühendisliği Bölümü, 48000,Muğla,Türkiye
menduhyilmaz@outlook.com, serkan@mu.edu.tr

ÖZET

Günlük hayatta zamanı ve enerji parametrelerini verimli kullanmak çok önem kazanmıştır. Yapılan her çalışmada bu parametreler seçimleri doğrudan etkilemektedir. Şifreleme algoritmalarında da kaynakları verimli kullanmak için dosya türlerine göre hangi algoritmayı seçmek gerektiği başlı başına bir sorun olabilmektedir. Bu çalışmada, şifreleme algoritmaları arasında karşılaştırma yapabilmek ve çeşitli performans parametrelerini ölçmek için C# tabanlı bir program geliştirilmiştir. Buna göre metin, ses ve video dosyalarının şifrelenmesinde en verimli şifreleme algoritmasının seçilmesini sağlayan akıllı bir seçim sistemi oluşturulmuştur. Bu sistemde kullanıcıya "Hızlı", "Performanslı" ve "Güvenli" olmak üzere 3 adet profil sunulmaktadır. Bu profiller sayesinde kullanıcı istediği profili seçerek beklentisine cevap bulmaktadır. Programdan elde edilen veriler bulanık mantık kullanılarak bulanık değerlere dönüştürülmüştür. Oluşturulan bulanık değerler BAHS, TOPSIS ve PROMETHEE çok kriterli karar verme yöntemleri kullanılarak ayrı ayrı değerlendirilmiş ve uzman tarafından oluşturulan sıralamaya en yakın sonucu veren sıralama yöntemi olarak PROMETHEE yöntemi seçilmiştir. Akıllı seçim sistemine göre performans değerlendirmesi yapılarak geliştirilen sistemde süre, kaynak ve güvenlik gibi kriterlerin verimli bir şekilde kullanılması sağlanmıştır.

Anahtar Kelimeler: Kripto, veri şifreleme, yapay zeka, bulanık mantık, akıllı seçim

AN INTELLIGENT SELECTION SYSTEM DEVELOPMENT FOR THE USE OF DATA ENCRYPTION ALGORITHMS

ABSTRACT

In daily life, it has become more important to use time and energy efficiently. The selections made in each study are directly influenced by these parameters. In encryption algorithms, it can constitute a problem in itself that for using resources efficiently which algorithm should be chosen according to file types. In this study, to make comparison along encryption algorithms and to measure various performance parameters, a C# language based program has been developed. According to this, an intelligent selection system providing the most efficient encryption algorithm selection in encryption of text, audio and video files has been developed. In this system, three different profiles were offered to the users including "Fast", "Performance" and "Secure". Thanks to these profiles user expectation is satisfied. Data achieved via written program were converted to fuzzy values by using fuzzy logic. These fuzzy values were evaluated under three different multi-criteria decision making methods FAHP, TOPSIS and PROMETHEE, independently and PROMETHEE method produced most relevant result with respect to the ranking created by expert was selected as sorting method. Performance evaluation according to intelligent selection system was made and using criteria such as time, resource and security efficiently were ensured in the developed system.

Keywords: Crypto, data encryption, artificial intelligence, fuzzy logic, intelligent selection

1. GİRİŞ (INTRODUCTION)

Günlük hayatta önemli olan verilere başkalarının ulaşmasını engellemek, ulaşsa bile verinin içeriğine erişmelerinin önüne geçmek için şifreleme teknolojisinin kullanılması kaçınılmaz olmaktadır [1]. Bir mesajın içeriğini saklamak üzere yapılan gizleme işlemi de şifreleme olarak tanımlanmaktadır. Elektronik iletişim, günümüzde kâğıt üzerinde yazı

yazarak yapılan her türlü iletişimin yerine geçmeye adaydır. Kişi/kuruluş/toplumların, özel/kamusal/resmi haberleşmelerini elektronik iletişim ağları üzerinden yapabilmeleri, açık ağlar üzerinden iletilen bilginin güvenliği ve güvenilirliğiyle yakından ilgilidir. Açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar [2]. Bir dosyayı herhangi bir algoritmayla şifrelemek mümkün olmaktadır. Ancak algoritmanın her türlü kaynak ve süreyi verimli kullanması bize hangi algoritmayı seçmemiz gerektiği konusunda belirleyici bir rol üstlenmektedir. Bu bağlamda kripto sistemleri arasında somut olarak bir değerlendirme yapmak için performans ölçülmesi son derece önemlidir.

Performans yönetimi konusunda simetrik şifreleme algoritmaları, asimetrik şifreleme algoritmalarına göre daha hızlıdır [3]. Simetrik ve asimetrik şifreleme algoritmalarının özelliklerinin karşılaştırılmasıyla ilgili olarak Tablo 1 aşağıda sunulmuştur.

Tablo 1. Simetrik Ve Asimetrik Şifreleme Algoritmalarının Özelliklerinin Karşılaştırılması [3]**.**

Özellik	Simetrik Şifreleme algoritmaları	Asimetrik şifreleme algoritmaları
Gizlilik	*Sağlamaktadır*	*Sağlamaktadır*
Bütünlük	-	*Sağlamaktadır*
Kimlik doğrulama	-	*Sağlamaktadır*
İnkar edilememezlik	-	*Sağlamaktadır*
Performans	*Hızlı*	*Yavaş*
Güvenlik	*Anahtar uzunluğuna bağlı*	*Anahtar uzunluğuna bağlı*

Bu çalışmada kıyaslama yapmak için şifreleme algoritmalarının performans ölçümleri yapılacaktır. Bundan dolayı daha performanslı olduğu için şifreleme algoritma türü olarak "Simetrik Şifreleme Algoritmaları" seçilmiştir.

Literatür incelendiğinde şifrelemede performans konusuyla ilgili olarak; Güvenoğlu [4] tarafından yapılan çalışmada, sayısal imza, SCAN, MLIE, CIE, BRIE resim şifreleme algoritmaları incelenmiştir. Bu algoritmaların genel yapısı ve performansları hakkında çalışma yapılmıştır. Performans testi için; CIE, BRIE algoritmaları için "Delphi" programında, MLIE ve SCAN algoritmaları için MATLAB'da yazılım geliştirilmiştir. Yerlikaya [5] tarafından yapılan çalışmada günümüzde yaygın olarak kullanılan simetrik ve asimetrik şifreleme algoritmalarının yapıları ve bu algoritmalar üzerine yapılan saldırılar incelenmiştir. Şifreleme algoritmalarının anlaşılır olması için matematiksel teoremler ve anahtarlarda kullanılan asal sayılar hakkında inceleme yapılmıştır. Şifreleme algoritmalarından RSA, ECC, DES, AES algoritmanın yapısı ve üzerine yapılan saldırı teknikleri, performans analizleri, kripto analizleri ve Stenografi uygulamaları incelenmiştir. Günden [2] tarafından yapılan çalışmada bilgi güvenliğini sağlama amaçlı simetrik ve asimetrik şifreleme algoritmalarından en sık kullanılan algoritmalara göre işlemci, zaman ve hafıza karmaşıklıkları test edilmiş ve performans sıralamaları yapılmıştır. Çalışmada kullanılan simetrik algoritmalar; Blowfish, Twofish, IDEA, TEA, DES, AES, 3DES, RC2 şifreleme algoritmaları kullanılmış, asimetrik şifreleme algoritmalarından da RSA algoritması tercih edilmiştir. Elminaam [6] vd. tarafından yapılan çalışmada simetrik şifreleme algoritmalarından AES (Rijndael), DES, 3DES, RC2, Blowfish ve RC6 algoritmaları kıyaslanmıştır. Bu algoritmalar farklı ayarlarda her biri için farklı boyuttaki veri blokları, farklı veri türleri, batarya tüketimi, anahtar uzunluğu ve şifreleme/şifre çözme hızları bakımından karşılaştırılmıştır. Kumar vd. [7] tarafından yapılan çalışmada simetrik anahtarlı şifreleme algoritması olan DES, AES ve Blowfish algoritmaları "hız, blok uzunluğu ve anahtar uzunluğu" parametrelerine göre bir kıyaslama yapılmıştır. Kıyaslama Java programlama dili kullanılarak tasarlanmıştır. Ciğer [8] tarafından yapılan çalışmada data şifreleme algoritmaları ve performans analizleri incelenmiştir. Çalışmada simetrik ve asimetrik algoritmaların kullandıkları anahtarlar bakımından farklılıklar gösterenler arasında karşılaştırma yapılmış ve performans değerlendirmeleri yapılmıştır. Çalışmada RSA, DES ve AES şifreleme algoritmalarının şifreleme ve şifre çözme kabiliyetleri için hız ve bellek parametreleri için bir değerlendirme yapılmıştır. Ayrıca çalışmada Ses, video ve gerçek zamanlı veri için şifreleme algoritmalarına da değinilmiştir.

Önceki çalışmalarda, farklı dosya türleri için farklı parametrelere göre değerlendirmeler yapılmış ancak kullanıcıya seçim konusunda yardımcı bir sistem geliştirilmemiştir. Bu çalışmada Akıllı Bir Seçim Sistemi geliştirilerek kullanıcıya anlık olarak, şifreleyeceği dosya türüne göre hangi algoritmayı seçmesi gerektiği konusunda yardımcı olmak amaçlanmıştır.

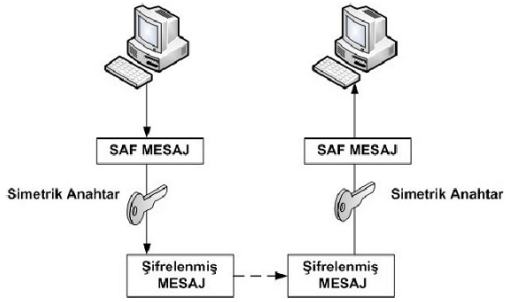
2. ŞİFRELEME ALGORİTMALARI (ENCRYPTION ALGORITHMS)

Şifrelenmiş bir mesajın güvenliği kadar şifrelerken kullanılan yöntem ve tekniklerinde gizliliği de bir o kadar önemlidir. Üçüncü şahıslar, şifreleme yöntemlerini öğrenseler dahi o yöntemleri çalıştırmak için gerekli olan kelimeyi (anahtar) bilmiyorlarsa mesajı çözemeyeceklerdir. Şifrelemede kullanılan algoritmaların işlevinin çözülme riskine karşın şifreleme anahtarı denilen ek bilgilerle güvenlik arttırılmıştır [5]. Şifrelemede simetrik ve asimetrik anahtarlı olmak üzere iki çeşit şifreleme türü kullanılmaktadır.

2.1. Simetrik Şifreleme (Symmetric Cryptography)

Simetrik şifrelemede, şifrelenerek iletilmek istenen mesaj şifreleme algoritması tarafından bir dizi işleme tabi tutulur. Bu işlemler sırasında mesaj, alıcı tarafında da bulunan aynı şifreleme anahtarıyla

şifrelenir. Alıcı kendisine ulaşan şifreli mesajı orijinal haline döndürürken kendisinde bulunan şifreleme anahtarıyla mesajı çözer. Yani simetrik anahtarlı şifreleme algoritmalarında şifreleme-çözme işlemlerinde aynı anahtarlar kullanılır [8]. Simetrik anahtarlı şifreleme Şekil 1'de gösterilmektedir.



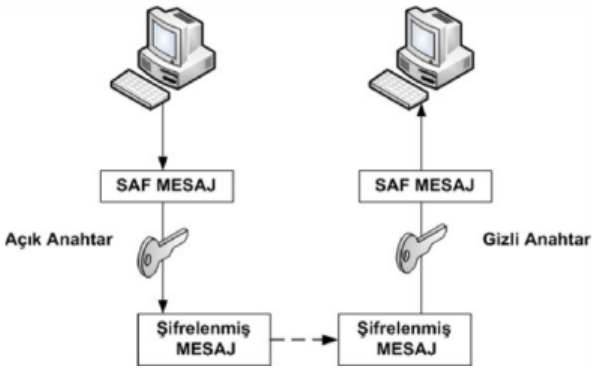
Şekil 1. Simetrik şifreleme [8].

Çok fazla sayıda simetrik şifreleme algoritması olmakla birlikte başlıca simetrik şifreleme algoritmaları şunlardır:

- AES (Advanced Encryption Standard)
- DES(Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- RC2 (Rivest Cipher)

2.2. Asimetrik Şifreleme (Asymmetric Cryptography)

Asimetrik anahtarlı şifrelemede kullanılan şifreleme anahtarı gönderici ve alıcıda farklıdır. Mesaj şifrelenirken kullanılan anahtar, mesaj çözülerken kullanılamaz. Bundan dolayı güvenlik daha yüksektir. Örneğin 1. Kişi tarafından şifrelenen mesaj A anahtarıyla şifrelenmişse, 2. Kişi ancak bu şifreli mesajı B anahtarıyla çözebilir. Yine aynı şekilde 2. Kişinin B anahtarıyla şifrelediği mesajı 1. Kişi A anahtarıyla çözebilir. Bu tür şifreleme algoritmanda şifreleme-çözme anahtarları farklıdır [8]. Şekil 2'de Asimetrik şifreleme şeması görülmektedir.



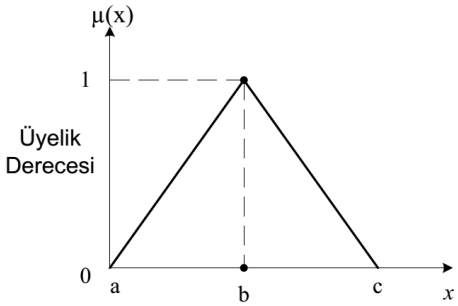
Şekil 2. Asimetrik şifreleme [8]

Başlıca asimetrik şifreleme algoritmaları şunlardır:

- RSA (Rivest-Shamir-Adleman)
- El Gamal
- PGP (Pretty Good Privacy)
- Diffie-Hellman
- DSA (Digital Signature Algorithm)

3. BULANIK MANTIK (FUZZY LOGIC)

Bulanık mantık, Azeri Matematikçi Lotfi A. Zadeh'in [9] yayınladığı makalenin sonucu olarak ortaya çıkmıştır. Klasik mantıkta üyelik değerleri sadece 0 ve 1 değerini alırken, bulanık mantıkta ara değerlerde işleme alınır. Böylece değerlendirme aşamasında daha çok olasılık hesaplamaya dâhil edilmiştir [10]. Bulanık mantık konusunun temel elemanı bulanık kümedir [11]. Bulanık kümlerin kullanışlılığı değişik durumlara uygun üyelik fonksiyonu meydana getirebilme kabiliyetiyle doğrudan ilgilidir. Literatürde en sık kullanılan üyelik fonksiyonları; üçgen, yamuk, genelleştirilmiş-çan ve gauss tipi üyelik fonksiyonlarıdır [12]. Üçgen tipi üyelik fonksiyonu Şekil 3'te gösterilmiştir.



Şekil 3. Üçgen Üyelik Fonksiyonu [12]

Bulanık karar verme sisteminin yapısı Şekil 4'de verilmiştir.

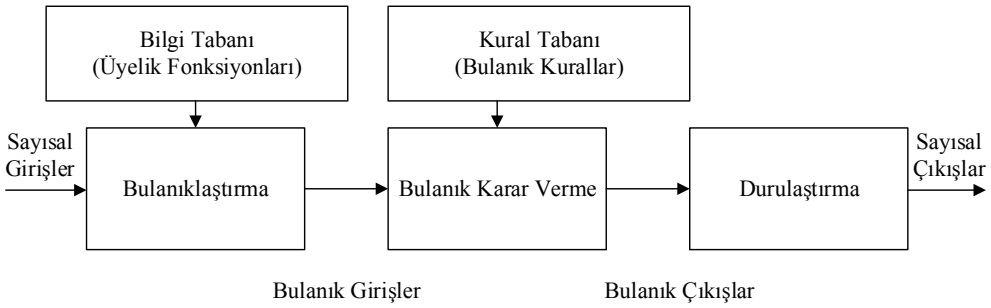
4. ÇOK KRİTERLİ KARAR VERME (MULTI-CRITERIA DECISION MAKING)

Bir problemin çözümünde alternatifleri seçerken karar vermek için birden fazla kriter kullanılıyor olabilir. Bu durumda karar vericiye, tanımlayıcı karar verme teorisi ve modelleri belli alanlar içerisinde karar verme yetisi verir. Burada amaçlanan davranışı en iyi hale getirmek değil bir karar verebilmektir [14]. Bu tür problemlerde ÇKKV yöntemlerini kullanmaktaki amaç kriter ve alternatiflerin sayısının fazla olduğu karar verme durumlarında karar vericiye kolay ve hızlı bir karar verme süreci oluşturmaktır [15]. Başlıca ÇKKV yöntemleri olan AHS, Bulanık AHS, TOPSIS ve PROMETHEE aşağıdaki alt bölümlerde anlatılmıştır.

4.1. Bulanık AHS (Fuzzy AHP)

Analitik hiyerarşik süreci (AHS), çok sayıda alternatif arasında seçim ya da sıralama yaparken, çok sayıda karar vericinin bulunabildiği, çok kriterli, çok amaçlı, belirlilik ya da belirsizlik durumunda karar vermede kullanılır [16]. Günlük hayatta problemleri nitelendirirken dilsel terimlerle ifade etmek göreceli

bir yaklaşım sergilememize neden olmaktadır. Yani bir matematik sorusuna "kolay" dememiz farklı



Şekil 4. Bulanık karar verme sisteminin yapısı [13]

kişilerce değerlendirildiğinde "zor" şeklinde yorumlanabilir ki bu durumda bir belirsizlik ortaya çıkmaktadır. Çok kriterli karar verme metotlarından biri olan AHS, belirsizlik durumunda karar vermeye tam uygun olmadığından, bulanık mantıkla AHS birleştirilerek bulanık analitik hiyerarşik süreci ortaya konmuştur [16].

4.2. TOPSIS

TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) yöntemi, Chen ve Hwang [17] tarafından Hwang ve Yoon [18]'un çalışmaları referans gösterilerek ortaya çıkmış çok kriterli karar verme yöntemlerinden biridir [19]. Bu yöntemde alternatif seçeneklerin bazı kriterlere göre ve kriterlerin alabileceği minimum ve maksimum değerler arasında ideal duruma göre karşılaştırılması gerekmektedir [20]. TOPSIS yönteminin çözüm süreci 6 temel adımdan oluşur. Bunlar;

Adım 1: Karar Matrisinin Oluşturulması
Adım 2: Standart Karar Matrisinin Oluşturulması
Adım 3: Ağırlıklı Standart Karar Matrisinin Oluşturulması
Adım 4: İdeal ve Negatif İdeal Çözümlerin Oluşturulması
Adım 5: Ayırım Ölçülerinin Hesaplanması
Adım 6: İdeal Çözüme Göreli Yakınlığın Hesaplanması

4.3. PROMETHEE

PROMETHEE (The Preference Ranking Organization METHod for Enrichment Evaluation) metodu literatürdeki mevcut önceliklendirme yöntemlerinin uygulamasındaki zorluklar nedeniyle çok kriterli karar verme problemlerinin çözümünde kullanılmak üzere geliştirilmiş bir yöntemdir [21]. GAIA (Geometrical Analysis for Interactive Aid) düzlemi, PROMETHEE sonuçlarının grafik olarak gösterilerek karar vericiye basit bir anlatım sağlamaktadır. Karar verici, GAIA geometrik gösterim ile karşılaştığı problemin sonuçlarını bir düzlem üzerinde görerek daha kolay ve çabuk bir değerlendirme yapabilir [22]. PROMETHEE yönteminin avantajları [23]:

- Verileri, karşılaştırma yapmaya gerek kalmadan doğrudan kullanması,
- Her bir kritere göre yapılan sınıflandırmanın doğruluğunun otomatik olarak hesaplanması,
- Ölçeklendirmenin sabit bir aralıkta değil istenilen aralıkta yapılabilmesi,
- Problemin görsel olarak ortaya konabilmesidir.

PROMETHEE yönteminde her bir alternatif için pozitif (Phi+) ve negatif (Phi-) üstünlük değeri belirlenir. Elde edilen pozitif üstünlük değeri, seçilmiş alternatifin diğer alternatiflere göre ne kadar üstün olduğunu gösterir. Negatif üstünlük değeri ise seçili alternatifin diğer alternatiflerden ne derece zayıf olduğunu göstermektedir [24]. Alternatifler arasında tam bir sıralama yapmak için Phi değerinin tespit edilmesi gerekmektedir [25]. Phi değerini tespit etmek için pozitif ve negatif üstünlük değerlerinden faydalanılır. Phi formülü aşağıda verilmiştir.

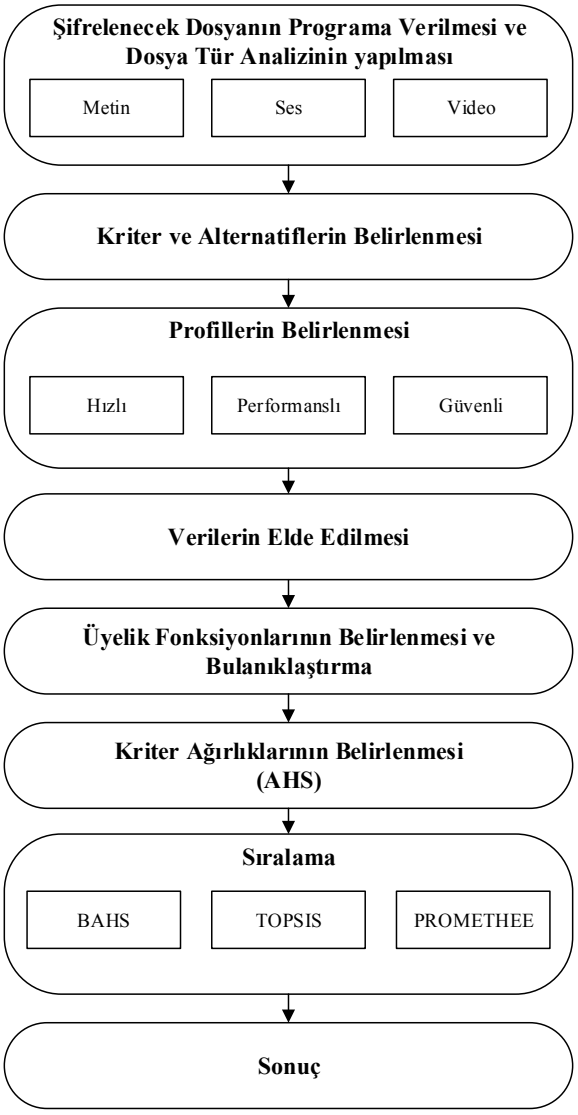
$$Phi = (Phi+) - (Phi-) \quad (1)$$

5. VERİ ŞİFRELEME ALGORİTMALARININ KULLANIMI İÇİN AKILLI BİR SEÇİM SİSTEMİ GELİŞTİRİLMESİ (AN INTELLIGENT SELECTION SYSTEM DEVELOPMENT FOR THE USE OF DATA ENCRYPTION ALGORITHMS)

Seçilen dosya türüne ve şifreleme algoritmasına göre belirlenen parametreler doğrultusunda ölçülecek değerlerin, akıllı bir seçim sistemi kullanılarak uygun şekilde değerlendirilmesiyle, kullanıcıya şifreleyeceği dosya türüne göre hangi algoritmayı seçmesi gerektiği konusunda en verimli algoritmayı seçmesini sağlamayı hedefleyen bu çalışmanın akış şeması Şekil 5'te gösterilmiştir.

Bu şemaya göre ilk olarak şifrelenecek dosya programa verilmeli buna göre dosya tür analizi yapılmalıdır. Bir sonraki adımda değerlendirmede kullanılacak kriterler ve alternatifler tespit edilmelidir. Daha sonra gerçek zamanlı olarak veriler elde edilmelidir. Bir sonraki aşamada üyelik fonksiyonu ve bulanıklaştırma sağlanmalıdır. Daha sonra değerlendirmede kullanılacak olan kriterlerin ağırlıkları bulunmalıdır. Bu aşamada ise şifreleme algoritmalarını, elde edilen veriler doğrultusunda uygun bir şekilde sıralamak için BAHS, TOPSIS ve

PROMETHEE yöntemleri kullanılarak sıralanmalıdır. Son aşamada ise elde edilen bu tüm veriler ışığında, kullanıcıya seçmiş olduğu profile uygun olan en iyi şifreleme algoritması sunulmalıdır.



Şekil 5. Akış Şeması

Şekil 5'deki akış şeması aşağıdaki alt başlıklarda ayrıntılı olarak anlatılmaktadır.

5.1. Kriter ve Alternatiflerin Belirlenmesi (Determination of Criteria and Alternatives)

Çalışmada kullanılacak olan kriterler ve alternatifler bu adımda belirlenmiştir. Literatürde Ciğer [8], Günden [2] "süre", "kaynak (RAM ve CPU)" parametrelerini ölçmüşlerdir. Buna göre bu çalışmada değerlendirme için kullanılacak kriterler;

1. Süre: Verilen dosyayı şifreleyip, şifre çözerken geçen süreyi milisaniye (ms) cinsinden ölçmektedir.

2. Kaynak: Kripto sırasında kullanılan CPU ve RAM kullanımını yüzde cinsinden ortalaması ile ölçmektedir.

3. Gizlilik: Kriptolama sırasında kullanılan şifreleme anahtar uzunluğunun bit cinsinden ifadesidir.

Kripto işlemleri için seçilen şifreleme algoritmaları 6 tanedir. Bunlardan 4 tanesi kendi başına 2 tanesi de melez algoritmalardır. Bunlar;

- AES
- 3DES
- RC2
- DES
- RC2+DES
- AES+3DES+RC2

5.2. Profillerinin Belirlenmesi (Determination of Profiles)

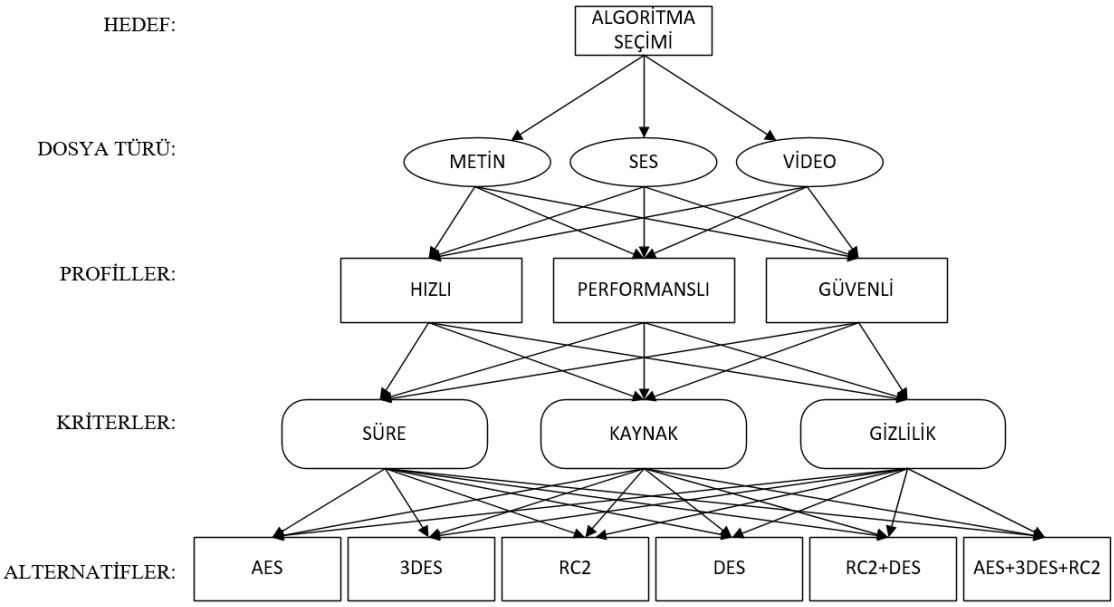
Bu çalışmadaki ulaşılmak istenen hedef, dosya şifreleme esnasında en verimli şifrelemeyi yapan algoritma tespit edilerek kullanıcıların en verimli algoritmayı kullanmasıdır. Buradaki verim, profile göre değişkenlik gösteren göreceli bir kavramdır. Bazı profilde süre kullanımı verim sayılırken bir başka profilde gizlilik durumu verim sayılmıştır. Kullanıcıya çalışmada 3 farklı profil seçeneği sunulmuştur. Bunlar; "Hızlı", "Performanslı" ve "Güvenli" profilleri olarak ele alınmıştır. Bu profiller ayrıntılı olarak aşağıda açıklanmıştır.

Profil-1: Hızlı: Bu profilde kullanıcıya sunulmak istenen durum, şifreleme-çözme yaparken en az süreyi kullanan algoritmayı bularak seçenek olarak kullanıcıya sunmaktır. Bu profilde ön plana çıkan kriterler önemlilikleri sırasıyla; süre, kaynak ve gizliliktir. Buradaki belirleyici kriter süre olarak gözükse de kaynak kullanımı da sonucu etkilemektedir. Diğer iki kritere göre daha az öneme sahip olan kriter gizliliktir.

Profil-2: Performanslı: Belirtilen bu kullanıcı profilindeki seçenek kripto sırasında en az kaynak kullanımı yapan algoritmayı seçenek olarak sunmaktır. Bu profilin kriter önemlilik sırası da; kaynak kullanımı, süre ve gizliliktir. Kaynak kullanımı önemli bir belirleyicidir. Ancak süre de performans değerlendirme bakımından önemli bir değerlendirme kriteri olduğu için gizliliğe göre bir adım daha önde durmaktadır.

Profil-3: Güvenli: Son profil olan bu seçenekte, kripto sırasında en fazla bit uzunluğuna sahip şifreleme anahtarını kullanılan algoritma tercih edilmektedir. Bu profil için en belirleyici kriter gizliliktir. Daha sonraki sıralama ise kaynak kullanımı ve süre şeklinde gözükmektedir. Burada kaynak kullanımı doğrudan olmasa da dolaylı olarak süreye göre daha ön plana çıkmaktadır.

Problemin hiyerarşik şeması; alternatifler, kriterler, profiller ve dosya türleri doğrultusunda Şekil 6'daki gibi oluşturulmuştur.



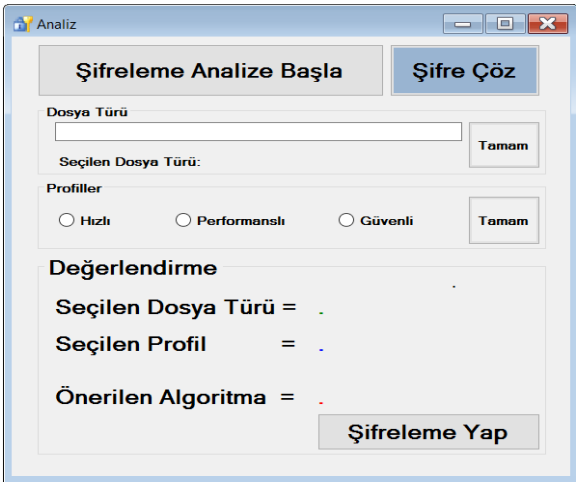
Şekil 6. Problemin Hiyerarşik Yapısı

5.3. Verilerin Analiz Edilmesi (Data Analysis)

Her bir algoritma için parametreler gerçek zamanlı olarak, uzman tarafından geliştirilen program vasıtasıyla elde edilmiştir. Parametre değerlerinde ortalama bir değer yakalamak için her bir dosya türü bazında 250 toplamda 1500 örneklem üzerinde çalışılmıştır. Parametre verileri oluşturulurken program aracılığıyla her bir parametre şifreleme ve şifre çözme olarak iki gurupta değerlendirip veriler elde edilmiştir. Örneğin "süre" parametre verisi şifreleme süresi ve şifre çözme süresi olarak ilk etapta elde edilmiştir. Ayrıca "kaynak" parametresinde İşlemci kullanımı ve Ram kullanımı ölçülmüş olup bunlarda kendi içlerinde daha önce bahsedilen iki grup (şifreleme-şifre çözme) olarak ele alınmıştır. Tüm parametreler için bu şekilde veri elde edildikten sonra bu gruplar kendi içlerinde birleştirilmiş olup "süre, kaynak ve gizlilik" olarak 3 parametre türü ortaya çıkmıştır. Parametrelerin ölçü birimleri: "Süre" için *milisaniye(ms)*, "Kaynak" için *yüzde (%)*, "Gizlilik" için *bit* olarak belirlenmiştir.

Veri elde etmek için kullanılan program görseli Şekil 7'de gösterilmiştir.

Yazılım ile elde edilen veriler Tablolar 2-4'te verilmiştir. Buradaki değerler tüm dosya türleri için gerçek zamanlı olarak ölçülmüştür. Bu değerler kullanılan bilgisayarın özelliklerine göre değişkenlik gösterebilir. Bu değerlendirmeler yapılırken Intel Core i7 2.4 GHz İşlemci, 8GB Bellek ve 64 Bit işletim Sistemi özelliklerine sahip bilgisayar kullanılmıştır.



Şekil 7. Tasarlanan Programın Ekran Görüntüsü

Tablo 2. Metin dosyası için elde edilen parametre değerleri

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	0,61100	29,94600	192
3DES	0,69800	27,37500	160
RC2	0,65800	20,23500	84
DES	0,74700	25,22700	64
RC2+DES	0,81600	29,58600	148
AES+3DES+RC2	0,88000	31,34700	436

5.4. Üyelik Fonksiyonlarının Belirlenmesi ve Bulanıklaştırma
(Determination of Membership Functions and Fuzzification)

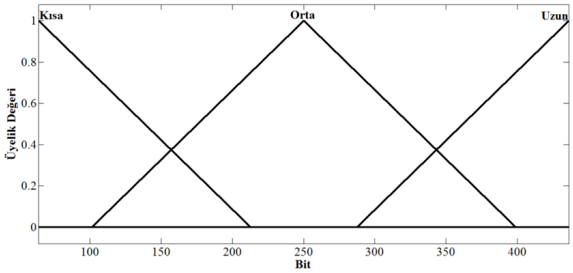
Elde edilen verileri bulanık değerlere dönüştürmek için Şekil 8'deki üçgen tipi üyelik fonksiyonu kullanılmıştır. 3 dosya türüne için parametrelere ait olan bulanık değerler Tablolar 5-7'de verilmiştir.

Tablo 3. Ses dosyası için elde edilen parametre değerleri

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	0,75600	31,79800	192
3DES	0,93900	25,51100	160
RC2	0,89500	27,33100	84
DES	1,17600	28,60600	64
RC2+DES	1,29800	30,74900	148
AES+3DES+RC2	1,39900	33,23600	436

Tablo 4. Video dosyası için elde edilen parametre değerleri

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	2,36300	31,27300	192
3DES	5,43800	27,65900	160
RC2	4,34500	28,56500	84
DES	5,37700	26,86300	64
RC2+DES	8,16400	31,45700	148
AES+3DES+RC2	9,51100	32,11400	436



Şekil 8. Güvenlik kriterine ait üyelik fonksiyonu

5.5. Kriter Ağırlıklarının Belirlenmesi
(Determination of Criteria Weights)

Bu işlem basamağında yapılacak işlem her bir kullanıcı profili için kullanılacak kriter ağırlıklarının belirlenmesi aşamasıdır. Bulanık Analitik Hiyerarşi Süreci (BAHS) için üçgensel bulanık sayılar kullanılmıştır. Dilsel ölçek değeri ve bu ölçeğe karşılık gelen üçgensel bulanık değerler Tablo 8'de sunulmuştur.

Tablo 5. Metin dosyası için parametrelere ait bulanık değerler

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	0,87000	0,21400	0,47700
3DES	0,53400	0,48400	0,41900
RC2	0,68400	0,87000	0,13200
DES	0,50000	0,50000	0,13000
RC2+DES	0,39900	0,28700	0,38600
AES+3DES+RC2	0,13000	0,13100	0,87000

Profiller için belirlenen kriterlerin bulanık karşılaştırma matrisi uzman tarafından oluşturulmuştur. Profiller için uzman tarafından oluşturulan bulanık dilsel karşılaştırma matrisi Tablo 9'da verilmiştir. Tablo 8'de verilen bu dilsel değerlere karşılık gelen ikili karşılaştırma matrisi de Tablo 10'da verilmiştir.

Tablo 6. Ses dosyası için parametrelere ait bulanık değerler

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	0,87000	0,33500	0,47700
3DES	0,56000	0,87000	0,41900
RC2	0,62500	0,60300	0,13200
DES	0,47900	0,50000	0,13000
RC2+DES	0,28600	0,46700	0,38600
AES+3DES+RC2	0,13000	0,13000	0,87000

Tablo 7. Video dosyası için parametrelere ait bulanık değerler

Algoritmalar	Süre (ms)	Kaynak (%)	Gizlilik (bit)
AES	0,87000	0,29100	0,47700
3DES	0,50000	0,72600	0,41900
RC2	0,56500	0,53300	0,13200
DES	0,50000	0,87000	0,13000
RC2+DES	0,33800	0,21300	0,38600
AES+3DES+RC2	0,13000	0,13000	0,87000

Tablo 8. Dilsel ölçeklendirme değerleri

DİLSEL ÖLÇEK	AÇIKLAMA	ÜÇGEN	TERS ÜÇGEN	TERS DİLSEL ÖLÇEK
Eşit Önemli (EÖ)	Her iki alternatif amaç için eşit	(1,1,1)	(1,1,1)	TEÖ
Az Önemli (AÖ)	Bir alternatif diğerine göre biraz daha	(1,3,5)	(1/5,1/3,1)	TAÖ
Yeterince Önemli (YÖ)	Bir alternatif diğerine göre yeterince	(3,5,7)	(1/7,1/5,1/3)	TYÖ
Çok Önemli (ÇÖ)	Bir alternatif diğerine göre çok iyidir.	(5,7,9)	(1/9,1/7,1/5)	TÇÖ
Mutlak Önemli (MÖ)	Bir alternatif diğerine göre en yüksek derecede iyidir.	(7,9,11)	(1/11,1/9,1/7)	TMÖ

Tablo 9. Profiller için bulanık karşılaştırma matrisi

Profiller		Süre	Kaynak	Gizlilik
Profil-1	Süre	EÖ	AÖ	YÖ
	Kaynak	TAÖ	EÖ	AÖ
	Gizlilik	TYÖ	TAÖ	EÖ
Profil-2	Süre	EÖ	TAÖ	AÖ
	Kaynak	AÖ	EÖ	YÖ
	Gizlilik	TAÖ	TYÖ	EÖ
Profil-3	Süre	EÖ	TAÖ	TAÖ
	Kaynak	AÖ	EÖ	TAÖ
	Gizlilik	AÖ	AÖ	EÖ

Tablo 10. Profiller için bulanık ikili karşılaştırma matrisi

Profiller		Süre	Kaynak	Gizlilik
Profil-1	Süre	(1,1,1)	(1,3,5)	(3,5,7)
	Kaynak	(1/5,1/3,1)	(1,1,1)	(1,3,5)
	Gizlilik	(1/7,1/5,1/3)	(1/5,1/3,1)	(1,1,1)
Profil-2	Süre	(1,1,1)	(1/5,1/3,1)	(1,3,5)
	Kaynak	(1,3,5)	(1,1,1)	(3,5,7)
	Gizlilik	(1/5,1/3,1)	(1/7,1/5,1/3)	(1,1,1)
Profil-3	Süre	(1,1,1)	(1/5,1/3,1)	(1/5,1/3,1)
	Kaynak	(1,3,5)	(1,1,1)	(1/5,1/3,1)
	Gizlilik	(1,3,5)	(1,3,5)	(1,1,1)

BAHS yöntemine göre profiller için hesaplanan tüm kriter ağırlık değerleri Tablo 11'de verilmiştir.

Tablo 11. BAHS yöntemi ile hesaplanan kriter ağırlıkları

Profiller	Süre	Kaynak	Gizlilik
Profil-1	0,63291	0,32304	0,04406
Profil-2	0,32304	0,63291	0,04406
Profil-3	0,17987	0,34052	0,47961

Değerlendirmede kullanılacak olan sıralama işlemi için üç farklı yöntem kullanılmıştır. Bunlar BAHS, TOPSIS ve PROMETHEE yöntemleridir. Aday algoritmalar için hazırlanan; "metin" dosya türüne ait Tablo 5'deki bulanık değerler, "ses" dosya türüne ait Tablo 6'daki bulanık değerler, "video" dosya türüne ait Tablo 7'deki bulanık değerler Tablo 11'de bulunan BAHS yöntemine göre profiller için hesaplanan tüm kriter ağırlık değerleriyle çarpılarak aday algoritmaların BAHS yöntemine göre olan ağırlıklı değerleri elde edilmiş ve Tablo 12'de sunulmuştur.

5.6. Sıralama (Ranking)

Kullanıcıya sunulacak olan "Profil-1, Profil-2 ve Profil-3" te kullanılacak olan algoritmaların, hangi sıralama yöntemi kullanılarak nasıl bir sıralama yapılacağı bu kısımda ele alınmıştır.

Uzman tarafından oluşturulan sıralamaya en yakın sonucu veren sıralama yöntemi ön plana çıkmıştır. Uzman tarafından oluşturulan sıralamanın hangi kriterlere göre belirlendiği Tablo 15'deki verilerden de yaralanarak her bir profil için ayrı ayrı ele alınmıştır.

Profil-1 için en önemli belirleyici kriter "hız" olarak karşımıza çıkmaktadır. Hız kriteri için Tablo 15'deki verilerden blok ve anahtar uzunluğun az olması uzman görüşüne göre hız açısından ön plana çıkmıştır. Ayrıca 3DES şifreleme, DES şifrelemesinin 3 kere art arda çalışması sonucunda oluştuğu için DES şifreleme yöntemine göre 3 kat daha yavaş çalışmaktadır [2].

Profil-2 için belirleyici kriter "performans" olarak karşımıza çıkmaktadır. Performans kriteri için, Tablo 15'deki verilerden; blok, anahtar uzunluğunun az olması ve profil-1 deki hız parametresi uzman tarafından performansı doğrudan etkileyen parametreler olarak değerlendirmiştir.

Profil-3 için belirleyici kriter "güvenlik" olmuştur. Güvenlik kriteri için, Tablo 15'deki veriler incelendiğinde anahtar uzunluğu en yüksek olan algoritma uzman tarafından en güvenli olarak değerlendirilmiştir.

Bu veriler sonucunda uzman tarafından Profil-1, Profil-2, Profil-3 için Tablo 16'daki sıralama uygun görülmüştür.

Tablo 12. BAHS yöntemi için sonuçlar

Dosya Türü	Algoritmalar	Profil-1	Profil-2	Profil-3
METİN	AES	0,64077	0,43750	0,45813
	3DES	0,51278	0,49729	0,46182
	RC2	0,71977	0,77740	0,48259
	DES	0,48370	0,48370	0,32254
	RC2+DES	0,36225	0,32754	0,35463
	AES+3DES+RC2	0,16292	0,16323	0,48525
SES	AES	0,67986	0,51408	0,49934
	3DES	0,65393	0,74999	0,59793
	RC2	0,59617	0,58936	0,38106
	DES	0,47041	0,47692	0,31877
	RC2+DES	0,34888	0,40496	0,39559
	AES+3DES+RC2	0,16260	0,16260	0,48491
VİDEO	AES	0,66565	0,48623	0,48435
	3DES	0,56944	0,63947	0,53811
	RC2	0,53559	0,52567	0,34643
	DES	0,60322	0,71787	0,44853
	RC2+DES	0,29973	0,26100	0,31846
	AES+3DES+RC2	0,16260	0,16260	0,48491

Tablo 13. TOPSIS Yöntemi için Sonuçlar

Dosya Türü	Algoritmalar	Süre	Kaynak	Gizlilik
METİN	AES	0,25491	0,03200	0,00973
	3DES	0,15646	0,07238	0,00855
	RC2	0,20042	0,13011	0,00269
	DES	0,14650	0,07478	0,00265
	RC2+DES	0,11691	0,04292	0,00787
	AES+3DES+RC2	0,03809	0,01959	0,01774
SES	AES	0,25002	0,04914	0,00954
	3DES	0,16093	0,12761	0,00838
	RC2	0,17961	0,08845	0,00264
	DES	0,13765	0,07334	0,00260
	RC2+DES	0,08219	0,06850	0,00772
	AES+3DES+RC2	0,03736	0,01907	0,01740
VİDEO	AES	0,25223	0,04306	0,00963
	3DES	0,14496	0,10743	0,00846
	RC2	0,16381	0,07887	0,00266
	DES	0,14496	0,12874	0,00262
	RC2+DES	0,09799	0,03152	0,00779
	AES+3DES+RC2	0,03769	0,01924	0,01756

Tablo 14. PROMETHEE Yöntemi için elde edilen Değerler

DOSYA TÜRÜ	ALGORİTMALAR	PROFİL-1			PROFİL-2			PROFİL-3		
		Phi	Phi+	Phi-	Phi	Phi+	Phi-	Phi	Phi+	Phi-
METİN	AES	0,35930	0,40630	0,04700	0,80020	0,90010	0,09990	0,48000	0,48000	0,00000
	3DES	0,14250	0,28850	0,14590	0,27090	0,63540	0,36460	0,28800	0,38400	0,09600
	RC2	0,07900	0,25670	0,17770	0,20000	0,60000	0,40000	0,09600	0,28800	0,19200
	DES	-0,03450	0,23290	0,26750	-0,02980	0,48510	0,51490	-0,09600	0,19200	0,28800
	RC2+DES	-0,11920	0,16400	0,28320	-0,32930	0,33530	0,66470	-0,28800	0,09600	0,38400
	AES+3DES+RC2	-0,42710	0,04400	0,47120	-0,91190	0,04400	0,95600	-0,48000	0,00000	0,48000
SES	AES	0,35810	0,39940	0,04130	0,70610	0,85310	0,14690	0,47790	0,47790	0,00000
	3DES	0,21820	0,33360	0,11540	0,54710	0,77360	0,22640	0,28670	0,38230	0,09560
	RC2	0,01580	0,22830	0,21250	0,01780	0,50890	0,49110	0,09560	0,28670	0,19110
	DES	-0,02400	0,24350	0,26750	-0,02980	0,48510	0,51490	-0,09560	0,19110	0,28670
	RC2+DES	-0,15150	0,15680	0,30840	-0,32930	0,33530	0,66470	-0,28670	0,09560	0,38230
	AES+3DES+RC2	-0,41660	0,04400	0,46060	-0,91190	0,04400	0,95600	-0,47790	0,00000	0,47790
VİDEO	AES	0,27930	0,32330	0,04400	0,58860	0,76200	0,17340	0,48000	0,48000	0,00000
	3DES	0,20280	0,28510	0,08230	0,38840	0,66190	0,27350	0,28800	0,38400	0,09600
	RC2	0,03820	0,20280	0,16460	0,29410	0,64700	0,35300	0,09600	0,28800	0,19200
	DES	-0,03820	0,16460	0,20280	0,22320	0,61160	0,38840	-0,09600	0,19200	0,28800
	RC2+DES	-0,20280	0,08230	0,28510	-0,58240	0,20880	0,79120	-0,28800	0,09600	0,38400
	AES+3DES+RC2	-0,27930	0,04400	0,32330	-0,91190	0,04400	0,95600	-0,48000	0,00000	0,48000

İkinci değerlendirme yöntemi olan TOPSIS yöntemi için oluşan değerler Tablo 13'de verilmiştir.

Üçüncü değerlendirme yöntemi olan PROMETHEE yöntemi için hesaplanan değerler Tablo 14'de verilmiştir. Phi değerleri Eşitlik 1'e göre hesaplanmıştır.

Tablo 15. Algoritmaların Özellikleri

Algoritma Numarası	Algoritmalar	Veri Blok Uzunluğu(bit)	Anahtar Uzunluğu	
			min(bit)	max(bit)
1	AES	128	128	256
2	3DES	64	128	192
3	RC2	64	40	128
4	DES	64	64	64
5	RC2+DES	64	104	192
6	AES+3DES+RC2	86	296	576

Tablo 16. Uzman İçin Algoritmaların Tercih Sıralaması

Sıra No	Uzman Sıralaması		
	Profil-1	Profil-2	Profil-3
1	3	3	6
2	4	4	1
3	2	2	2
4	1	1	5
5	5	5	3
6	6	6	4

Değerlendirmede kullanılacak olan sıralama işlemi için BAHS, TOPSIS ve PROMETHEE yöntemlerine ait Tablolar 12-14'deki veriler ışığında her bir profil için ayrı ayrı olmak üzere Tablolar 17-19 oluşturulmuştur.

Tablolar 17-19 incelendiğinde görülmüştür ki BAHS ve TOPSIS yöntemlerine göre yapılan sıralamada algoritmaların sırası aynı, PROMETHEE yöntemine göre yapılan sıralama farklıdır. Tablolar 17-19 ye göre 3 farklı yöntem ayrı ayrı ele alındığında uzman sıralamasına en yakın sonucu veren sıralama yöntemi PROMETHEE olarak karşımıza çıkmaktadır. Tablo 17-19 de görülen BAHS, TOPSIS ve PROMETHEE yöntemleriyle UZMAN sıralaması arasındaki "Korelasyon" incelendiğinde en yüksek korelasyon PROMETHEE yönteminde elde edilmiştir. Bu veriler ışığında kullanıcıya önerilecek olan sıralaması PROMETHEE yöntemidir.

Profillere göre 3 dosya türünü beraber incelenirse:

Profil-1 için: Metin dosya türünde "RC2" algoritması, ses dosya türünde "3DES", video dosya türünde "DES" algoritması ilk sırayı almaktadır. Bu profilde istenen durum işlemin hızlı olmasıdır. Bunda dolayı süre ve kaynak parametreleri sonucu belirlemektedir.

Profil 2 için: Bu profilde istenen öncelik performanstır. Bundan dolayı kaynak ve süre parametreleri sonuçta belirleyici olmuştur. Metin dosya türü için "RC2", ses türü için "3DES" ve video türü için "DES" algoritması ilk sırada bulunmaktadır. Görüldüğü gibi her tür için farklı bir algoritma ön plana çıkmıştır.

Tablo 17. Profil-1 için BAHS, TOPSIS ve PROMETHEE yöntemlerinin kıyaslanması

Dosya Türü	Profil-1			
	BAHS	TOPSIS	PROMETHEE	UZMAN
METİN	3	3	3	3
	1	1	4	4
	2	2	2	2
	4	4	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.48	0.48	1.00	
SES	1	1	2	3
	2	2	3	4
	3	3	4	2
	4	4	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.48	0.48	0.82	
VİDEO	1	1	4	3
	4	4	2	4
	2	2	3	2
	3	3	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.77	0.77	0.82	

Tablo 18. Profil-2 için BAHS, TOPSIS ve PROMETHEE yöntemlerinin kıyaslanması

Dosya Türü	Profil-2			
	BAHS	TOPSIS	PROMETHEE	UZMAN
METİN	3	3	3	3
	2	2	4	4
	4	4	2	2
	1	1	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.77	0.77	1.00	
SES	2	2	2	3
	3	3	3	4
	1	1	4	2
	4	4	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.65	0.65	0.82	
VİDEO	4	4	4	3
	2	2	2	4
	3	3	3	2
	1	1	1	1
	5	5	5	5
	6	6	6	6
Korelasyon	0.82	0.82	0.82	

Profil 3 için: Bu profil içinde istenilen durum güvenliktir. Metin, ses ve video dosya türünde "AES+3DES+RC2" algoritması ilk sırada bulunmaktadır. Bu profil için ilk öncelikli parametremiz gizlilik, ikinci sıradaki parametremizde kaynaktır. 3 türde de gizlilik parametresi sıralaması "AES+3DES+RC2" yi göstermektedir.

Tablo 19. Profil-3 için BAHS, TOPSIS ve PROMETHEE yöntemlerinin kıyaslanması

Dosya Türü	Profil-3			
	BAHS	TOPSIS	PROMETHEE	UZMAN
METİN	6	6	6	6
	3	3	1	1
	2	2	2	2
	1	1	5	5
	5	5	3	3
	4	4	4	4
Korelasyon	0.31	0.31	1.00	
SES	2	2	6	6
	1	1	1	1
	6	6	2	2
	5	5	5	5
	3	3	3	3
	4	4	4	4
Korelasyon	0.08	0.08	1.00	
VİDEO	2	2	6	6
	6	6	1	1
	1	1	2	2
	4	4	5	5
	3	3	3	3
	5	5	4	4
Korelasyon	-0.25	-0.25	1.00	

6. SONUÇ (CONCLUSION)

Günlük hayatta kullanıcılar her dosyayı her şifreleme algoritmasıyla şifreleyebilirler. Bu çalışmada dosya türlerine göre belirlenen profiller doğrultusunda seçilen 6 tane şifreleme algoritmasının değerlendirilmesi yapılmıştır.

Değerlendirmelerde ele alınan bir profili sadece bir kritere göre değerlendirmek her zaman avantaj sağlamamaktadır. Göz önüne farklı kriterleri de dahil ettiğimizde farklı sonuçlara ulaşılabilmektedir. Kriterleri farklı önceliklerle değerlendirmeye dahil etmek için 3 farklı profil geliştirmiştir. Bu sayede kriterler profillerde farklı öncelik sıralarına tabi tutularak değerlendirmelerde daha sağlıklı sonuçlar elde edilmiştir. Değerlendirme yöntemlerinden BAHS ve TOPSIS yöntemlerinin sıralaması benzerlik göstermekte iken PROMETHEE yöntemi ise farklılık göstermiştir. Ancak uzman sıralaması ile karşılaştırıldığında en iyi sonucu veren yöntem PROMETHEE yöntemi olmuştur. PROMETHEE yöntemi, ÇKKV yöntemlerinin çözümü için geliştirildiği için ve diğer yöntemlere göre daha esnek olmasından dolayı ön plana çıkmıştır.

Akıllı Seçim Sisteminde, seçilen profile göre kriterlerin ağırlıkları hesaplanmış ve kriter ağırlarına göre elde edilen veriler sıralama yöntemlerine göre kıyaslanarak profile en uygun olan algoritma kullanıcıya sunulmuştur. Yani performans değerlendirmesi yapılarak geliştirilen sistem sayesinde süre, kaynak ve güvenlik gibi kriterlerin verimli bir şekilde kullanılması sağlanmıştır.

Gelecekte ki çalışmalarda; kullanıcı gereksinimlerine göre farklı dosya türleri ve profiller sisteme dahil edilebilir. Ayrıca değerlendirmede daha farklı yöntem ve yaklaşımlar kullanılarak sistemin kararlılığı daha da güçlendirilebilir.

KAYNAKLAR (REFERENCES)

[1] Yılmaz, M. ve Ballı, S., **"Veri Şifreleme Algoritmalarının Bulanık AHS Yöntemine Göre Performans Değerlendirmesi"**, Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı, Tekirdağ Namık Kemal Üniversitesi, pp. 646-653. ISBN:978-605-86904-5-5, 2016.

[2] Günden, Ü., **"Şifreleme Algoritmalarının Performans Analizi"**,Yüksek Lisans Tezi, Sakarya Üniversitesi, 2010.

[3] Kodaz, H. ve Botsalı, F., **"Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması"**, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi, cilt 9, no. 1-2010, 2010.

[4] Güvenoğlu, E., **"Görüntü Şifreleme Algoritmaları ve Performans Analizleri"**, Yüksek Lisans Tezi, Trakya Üniversitesi, 2006.

[5] Yerlikaya, T., **"Yeni Şifreleme Algoritmalarının Analizi"**, Doktora Tezi, Trakya Üniversitesi, 2006.

[6] Elminaam, D., Kader, H.ve Hadhoud, M., **"Evaluating The Performance of Symmetric Encryption Algorithms"**, International Journal of Network Security, 10(3), pp. 216-222, 2010.

[7] Kumar, N., Thakur, J. ve Kalia, A., **"Performance Analysis Of Symmetric Key Cryptography Algorithms: Des, Aes And Blowfish"**, An International Journal of Engineering Sciences, pp. 28-37, 2011.

[8] Ciğer, İ., **"Data Şifreleme Algoritmaları ve Performans Analizi"**, Yüksek Lisans Tezi, İstanbul Üniversitesi, 2012.

[9] Zadeh, L., **"Fuzzy Sets"**, Information and Control, no. 8, pp. 338-353, 1965.

[10] Baykal, N. ve Beyan, T., **"Bulanık Mantık Uzman Sistemler ve Denetleyiciler"**, Bıçaklar Kitabevi, 2004.

[11] Altaş, İ., **"Bulanık Mantık : Bulanıklılık Kavramı"**, Enerji, Elektrik, Elektromekanik-3e, Sayı 62, S:80-85, Bileşim Yayıncılık 1999.

[12] Yılmaz, A., **"Sinirsel Bulanık Mantık Modeliyle Kanser Risk Analizi"**, Doktora Tezi, Sakarya Üniv., Fen Bilimleri Enstitüsü, 2015.

[13] Yılmaz, S., **"Bulanık Mantık ve Mühendislik Uygulamaları Ders Notları"**, Kocaeli Üniversitesi, 2006.

[14] Zimmermann, J.H., **"Fuzzy Sets Decision Making and Expert Systems"**, Boston: Kluwer Academic Publishers, 1987.

[15] Ballı, S., **"Melez Zeki Karar Destek Sistemlerinin Tasarımı ve Gerçekleştirimi"**, Doktora Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, 2010.

[16] Göksu, A., **"Bulanık Analitik Hiyerarşik Proses ve Üniversite Tercih Sıralamasında Uygulanması"**, Doktora Tezi, Süleyman Demirel Üniv., Sosyal Bilimler Enstitüsü, 2008.

[17] Chen, S. ve Hwang, C., **"Fuzzy Multiple Attribute Decision Making"**, Springer-Verlag, 1992.

[18] Hwang, C. L. ve Yoon, P., **"Multiple Attribute Decision Making In: Lecture Notes in Economics and Mathematical Systems"**, Springer-Verlag, 228p., 1981.

[19] Demireli, E**., "Topsis Çok Kriterli Karar Verme Sistemi: Türkiye'deki Kamu Bankaları Üzerine Bir Uygulama"**, Girişimcilik ve Kalkınma Dergisi, (5:1), 2010.

[20] Yurdakul, M. ve İç, Y.T., **"Türk Otomotiv Firmalarının Performans Ölçümü ve Analizine Yönelik TOPSIS Yöntemini Kullanan Bir Örnek Çalışma"**, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, cilt 18, no. 1, pp. 1-18, 2003.

[21] Dağdeviren, M. ve Eraslan, E., **"Promethee Sıralama Yöntemi İle Tedarikçi Seçimi"**, Gazi Üniversitesi Müh. Mim. Fakültesi Dergisi, 2008.

[22] Genç, T., **"Promethee Yöntemi Ve Gaia Düzlemi"**, İİBF Dergisi, C. XV, S. I, 2013.

[23] Ballı, S., Karasulu, B. ve Korukoğlu, S., **"En Uygun Otomobil Seçimi Problemi İçin Bir Bulanık Promethee Yöntemi Uygulaması",** D.E.Ü.İ.İ.B.F. Dergisi, 2007.

[24] Sakarya, Ş. ve Aytekin, S., **"İMKB'de İşlem Gören Mevduat Bankalarının Performansları ile Hisse Senedi Getirileri Arasındaki İlişkinin Ölçülmesi: PROMETHEE Çok Kriterli Karar Verme Yöntemiyle Bir Uygulama",** Uluslararası Alanya İşletme Fakültesi Dergisi, cilt 5, no. 2, 2013.

[25] Araz, C., Özfırat, P. ve Özkarahan, I., **"An integrated multicriteria decision-making methodology for outsourcing management",** Computers & Operations Research, doi:10.1016/j.cor.2006.01.014., 2006.