

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE GÖMÜLÜ SİSTEM
UYGULAMASI**

YÜKSEK LİSANS TEZİ

Oğuz AYDIN

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

EKİM 2018

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE GÖMÜLÜ SİSTEM
UYGULAMASI**

YÜKSEK LİSANS TEZİ

**Oğuz AYDIN
(504131217)**

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Mürvet KIRCI

EKİM 2018

İTÜ, Fen Bilimleri Enstitüsü'nün 504131217 numaralı Yüksek Lisans Öğrencisi Oğuz AYDIN, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE GÖMÜLÜ SİSTEM UYGULAMASI” başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Doç. Dr. Mürvet KIRCI**
İstanbul Teknik Üniversitesi

Jüri Üyeleri : **Prof. Dr. Hakan Ali ÇIRPAN**
İstanbul Teknik Üniversitesi

Asst. Prof. Dr. Nihan KAHRAMAN
Yıldız Teknik Üniversitesi

Teslim Tarihi : **19 Ekim 2018**
Savunma Tarihi : **3 Ekim 2018**



ÖNSÖZ

Tezimi hazırlarken değerli fikirleri ve yorumlarıyla beni yönlendiren tez danışmanım Doç. Dr. Mürvet Kırcı'ya, çalışmalarındaki ilgi ve yardımlarından dolayı Yeşil Otomasyon kurucusu Yük. Müh. Fevzi Erdal Karaağaç'a ve iş arkadaşlarıma, maddi-manevi beni sürekli destekleyen aileme ve dostlarıma teşekkür ediyorum.

Eylül 2018

Oğuz Aydın
(Elektronik Mühendisi)



İÇİNDEKİLER

Sayfa

ÖNSÖZ	v
KISALTMALAR	ix
ÇİZELGE LİSTESİ	xi
ŞEKİL LİSTESİ	xiii
ÖZET	xv
SUMMARY	xix
1. GİRİŞ VE ÇALIŞMANIN AMACI	1
1.1 Sayısal Damgalamanın Kullanım Alanları	2
2. GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE YÖNTEMLERİ	5
2.1 Damgalama Yöntemlerinin Sınıflandırılması	7
2.1.1 Sayısal veri tipine göre sınıflandırılma	7
2.1.2 Filigran tipine göre sınıflandırılma	7
2.1.3 İnsan perspektifine göre sınıflandırılma	8
2.1.4 Damgalamanın sağlamlığına göre sınıflandırılma	8
2.1.5 Damganın algılanışına göre sınıflandırılma	9
2.1.6 Dönüşüm bölgesine göre sınıflandırılması	9
2.2 Damgalama yöntem ve kodlama teknikleri	10
2.2.1 Görüntü damgalama sırasında kullanılabilecek dönüşüm yöntemleri	10
2.2.1.1 Ayırık Kosinüs Dönüşümü	10
2.2.1.2 Hızlı Fourier Dönüşümü	11
2.2.1.3 Ayırık Dalgacık Dönüşümü	12
2.2.1.4 Çevrecik Dönüşümü	13
2.2.2 Sayısal damgalama için kullanılan yöntemler	14
2.2.2.1 Uzamsal alanda LSB damgalama yöntemi	14
2.2.2.2 Uzamsal alanda CDMA ile damgalama yöntemi	15
2.2.2.3 DCT temelli alçak frekans bölgesinde yapılan damgalama yöntemi	16
2.2.2.4 DCT ve SVD temelli damgalama yöntemi	17
2.2.2.5 DCT temelli orta frekans bölgesinde yapılan damgalama yöntemi	18
2.2.2.6 Çevrecik dönüşümü ile sayısal damgalama yöntemi	20
2.2.2.7 DWT temelli sayısal damgalama yöntemi	21
2.2.2.8 DWT ve SVD temelli sayısal damgalama yöntemi	22
2.3 Sayısal Damgalama için Saldırı Yöntemleri ve Ölçüm Teknikleri	24
2.4 Sayısal Damgalama Uygulamaları ve Ölçümleri	26

2.4.1 LSB temelli sayısal damgalama uygulaması ve ölçümleri.....	26
2.4.2 DWT-SVD temelli sayısal damgalama uygulaması ve ölçümleri	28
2.4.3 DCT orta frekans temelli sayısal damgalama uygulaması ve ölçümleri...	30
2.4.4 DCT-SVD temelli sayısal damgalama uygulaması ve ölçümleri.....	32
2.4.5 DWT temelli sayısal damgalama uygulaması ve ölçümleri.....	34
2.5 Sayısal Damgalama Uygulama Sonuçları	36
3. SAYISAL DAMGALAMA GÖMÜLÜ SİSTEM UYGULAMASI	37
3.1 Sayısal Damgalama Gömülü Sistem Elemanları.....	37
3.1.1 Gömülü Linux ortamı.....	38
3.1.2 Biyometrik sensor modülü	39
3.1.3 Görüntü sensörü	40
3.2 Biyometrik Sayısal Damgalama Gömülü Sistem Uygulaması.....	41
3.2.1 Biyometrik sayısal filigranın konak görüntüsüne gömülmesi	42
3.2.2 Damgalanmış görüntüden sayısal filigranın çıkarılması ve doğrulama	46
3.3 Biyometrik Sayısal Damgalama Çıktıları ve Sonuçları.....	47
4. SONUÇ VE ÖNERİLER	51
KAYNAKLAR.....	53
ÖZGEÇMİŞ	55



KISALTMALAR

DCT	: Discrete Cosine Transform
DWT	: Discrete Wavelet Transform
FFT	: Fast Fourier Transform
CDMA	: Code Division Multiple Access
PN	: Pseudo-Noise
DFT	: Discrete Fourier Transform
LP	: Laplacian Pyramid
DFB	: Directional Filter Bank
PDFB	: Pyramidal Directional Filter Bank
JPEG	: Joint Photographic Experts Group
MP3	: Moving Picture Experts Group Layer-3 Audio
LSB	: Least Significant Bit
MSB	: Most Significant Bit
SVD	: Singular-Value Decomposition
PSNR	: Peak Signal to Noise Ratio
MSE	: Mean Squared Error
SNR	: Signal to Noise Ratio
NC	: Normalized Correlation Coefficient
IP	: Internet Protocol
USB	: Universal Serial Bus
MJPEG	: Motion Joint Photographic Experts Group
H.264	: Advancing Video Coding
AES	: Advanced Encryption Standard
RSA	: Rives Shamir Adleman
DES	: Data Encryption Standard
CRC	: Cyclic Redundancy Check



ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1 : LSB sayısal damgalama ölçüm sonuçları	26
Çizelge 2.2 : DWT-SVD sayısal damgalama ölçüm sonuçları	28
Çizelge 2.3 : DCT orta frekans sayısal damgalama ölçüm sonuçları	30
Çizelge 2.4 : DCT-SVD sayısal damgalama ölçüm sonuçları.....	32
Çizelge 2.5 : DWT sayısal damgalama ölçüm sonuçları.....	34
Çizelge 3.1 : GT-511C3 parmak izi sensorunun teknik özellikleri	40
Çizelge 3.2 : DS-2CD2110F-IS kamera teknik özellikleri.....	41
Çizelge 3.3: Beaglebone ve bilgisayar arasındaki performans karşılaştırması.....	49



ŞEKİL LİSTESİ

	<u>Sayfa</u>
Şekil 2.1 : Sayısal filigran gömme şeması.....	6
Şekil 2.2 : Sayısal filigran çıkarma şeması.....	6
Şekil 2.3 : Sayısal damgalamanın sınıflandırılması.....	7
Şekil 2.4 : İnsan perspektifine göre sınıflandırma	8
Şekil 2.5 : DCT frekans bölgeleri	11
Şekil 2.6 : Görüntü üzerinde FFT dönüşümü	12
Şekil 2.7 : Sırasıyla 1., 2. ve 3. dereceden DWT dönüşümleri.....	13
Şekil 2.8 : Görüntünün 2. dereceden DWT dönüşümü.....	13
Şekil 2.9 : LSB yönteminin temsili	15
Şekil 2.10 : Frekans bölgesinde biçim değiştirilmesi	17
Şekil 2.11 : JPEG katsayı matrisi	19
Şekil 2.12 : Konak görüntünün ve sayısal filigranın seviye-1 Haar dalgacık dönüşümleri.	21
Şekil 2.13 : LSB sayısal damgalama	26
Şekil 2.14 : LSB sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonrasında çıkarılan sayısal filigranlar	27
Şekil 2.15 : DWT-SVD temelli sayısal damgalama	28
Şekil 2.16 : DWT-SVD sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonrasında çıkarılan sayısal filigranlar	29
Şekil 2.17 : DCT orta frekans sayısal damgalama.....	30
Şekil 2.18 : DCT orta frekans sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar	31
Şekil 2.19 : DCT-SVD Sayısal Damgalama.....	32
Şekil 2.20 : DCT-SVD sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar	33
Şekil 2.21 : DWT Sayısal Damgalama	34
Şekil 2.22 : DWT sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar	35
Şekil 3.1 : Biyometrik sayısal damgalama sistemi	37
Şekil 3.2 : Beaglebone	38
Şekil 3.3 : GT-511C3.....	39
Şekil 3.4 : Hikvision/Haikon DS-2CD2110F-IS kamera	40

Şekil 3.5 : Biyometrik sayısal filigranın gömme şeması	42
Şekil 3.6 : GT-511C3 komut paket yapısı	42
Şekil 3.7 : GT-511C3 cevap paketi yapısı	43
Şekil 3.8 : GT-511C3 veri paketi yapısı	43
Şekil 3.9 : Parmak izi kaydı akış şeması	44
Şekil 3.10 : Biyometrik sayısal filigranın damgalanmış görüntüden çıkarılmasına dair işlem şeması	46
Şekil 3.11 : Gömülü sistemde kamera tarafından yakalanan görüntü	48
Şekil 3.12 : Gömülü sistem ile damgalanmış görüntü	48



GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE GÖMÜLÜ SİSTEM UYGULAMASI

ÖZET

Bilgisayar ve internet çağını yaşadığımız günümüzde ses, görüntü gibi sayısal medyaların kullanımı hızlı bir şekilde yükselişe geçmiştir. İnternet ortamında, özellikle sosyal ağ platformlarında sayısal medyaların telif hakkı sahiplerinin izni olmaksızın değiştirilerek veya doğrudan kullanılması bir sorun teşkil etmektedir. Bu çalışma da sayısal medyaların üreticisinin izni olmaksızın kullanılması, telif haklarının ihlal edilmesi, kopyalanmanın engellenmesi ve içeriğin korunması gibi problemlerin çözümü için önerilen sayısal damgalama ve yöntemleri üzerinde durulmuştur.

Sayısal damgalama, ses, görüntü video gibi sayısal medyalar üzerinde aidiyeti belli etmek amacıyla kullanılan bir yöntemdir. Çalışmada ilk olarak sayısal damgalamaya olan ihtiyaç, tarihte ortaya çıkışı ve kullanım alanlarıyla ilgili bilgilere yer verilmiştir. Sayısal damgalamalar, özel filigranların sayısal medya üzerine gömülmesini ve gerektiğinde çıkarılıp orijinallik karşılaştırması yapılabilmesini sağlayan yöntemlerdir. Bu yöntemlerin daha iyi anlaşılabilmesi için çalışmada, sayısal damgalamaların hangi konuları hedeflediği ve çeşitli parametrelere göre nasıl sınıflandırıldığı incelenmiştir. Sayısal damgalama insan perspektifine göre görünür ve görünür olmayan şeklinde sınıflandırılmaktadır, bu çalışmada özellikle görünür olmayan ve görüntü üzerine uygulanabilinen yöntemler üzerinde durulmuştur. Bu yüzden ilgilenilen sayısal damgalama yöntemleri kümesi, steganografi yani bilgi gizleme biliminin bir alt kümesidir.

Ses, görüntü, video ve metin üzerinde yapılabilen sayısal damgalama yöntemleri mevcut olmasına rağmen çalışmaların büyük çoğunluğu görüntü üzerinde yapılmaktadır. Bu çalışmada da görüntü üzerine uygulanabilinen sayısal damgalama yöntemleri üzerinde durulmuştur, fakat görüntü üzerine uygulanabilen sayısal damgalama yöntemleri MJPEG, H.264 gibi video standartlarına uygulanabilmektedir. H.264 üzerinde sayısal filigran I-çerçeve üzerine gömülebilir.

Görüntü üzerinde sayısal damgalama yöntemleri geliştirilebilmesi için uzamsal düzlemde çalışmalar yapılmıştır ancak çeşitli özelliklerinden dolayı frekans bölgesi dönüşüm kullanan sayısal damgalama yöntemlerinin popüleritesi daha fazladır. Bu yüzden çalışmada, görüntü üzerinde uygulanabilecek frekans bölgesi dönüşümleri hakkında bilgiler verilmiştir ve bu dönüşümlerin iyi ve eksik yönleri tartışılmıştır. Özellikle JPEG görüntü sıkıştırma algoritmasında kullanılan frekans dönüşümleri; ayırık kosinüs dönüşümü (DCT) ve ayırık dalgacık dönüşümü (DWT) sayısal damgalama yöntemlerinde kullanılan en popüler dönüşümlerdir.

Çalışmada görüntü üzerinde yapılabilen sayısal damgalama yöntemleri hakkında bilgi edinilmiştir. Bunun için uzamsal düzlem ve frekans bölgelerinde sayısal damgalama

yapan 8 ayrı teknik incelenmiştir. Bu bölüm içerisinde sayısal damgalama yöntemlerin sayısal filigranı konak görüntüye gömme teknikleri ve damgalanmış görüntüden çıkarma işlemlerine yer verilmiştir. Yapılan araştırmalar da göz önünde bulundurularak yöntemlerin avantajlı ve dezavantajlı yönlerinden bahsedilmiştir. İncelenen yöntemlerden LSB üzerinde yapılan, ayrık dalgacık dönüşümü temelli, ayrık dalgacık dönüşümü ve tekil değer ayrışımı temelli, ayrık kosinüs dönüşümü alçak frekans bölgesi içerisinde yapılan ve ayrık kosinüs dönüşümü orta frekans bölgesinde yapılan 5 sayısal damgalama yöntemi uygulamaya dökülmüştür.

Sayısal damgalama ile ilgili üzerinde durulan diğer bir konuda, sayısal damgalama uygulanmış görüntü üzerine yapılabilecek saldırılara karşı başarı ölçümüdür. Bu amaç ile kullanılabilecek filtreler, geometrik ve sıkıştırma yöntemleri hakkında bilgiler verilmiştir. Uygulaması yapılan sayısal damgalama yöntemlerinde elde edilen damgalanmış görüntüler tuz ve karabiber gürültüsü, bulanıklaştırma, kontrast değişimi, yeniden boyutlandırma, parlaklık değişimi, medyan filtre, görüntünün döndürülmesi ve Gaussian gürültü ile saldırılara uğratılarak dayanıklılıkları test edilmiştir. Bu testlerde, saldırıya uğramış görüntüleri ve damgalanmış görüntüleri orijinal konak görüntüsü ile karşılaştırmak için tepe sinyal-gürültü oranı (PSNR) değerleri hesaplanmıştır. Benzer şekilde her yöntem için damgalanmış görüntüden çıkarılan sayısal filigran ile orijinal sayısal filigranın benzerliğini test etmek için normalleştirilmiş korelasyon katsayıları(NC) bulunmuştur. Bu ölçümlerden hareket ile hangi sayısal damgalama yönteminin, hangi saldırı yöntemine karşı dayanıklı veya dayanıksız olduğuna dair fikir edinilmiştir.

Bu çalışmada, görüntü üzerinde yapılabilen sayısal damgalama yöntemleri araştırılarak gömülü sistemlerde de uygulanabilecek düşük işlem gücüne, karmaşık olmayan, dirençli ve kapasite bakımından sistemi rahatsız etmeyecek sayısal damgalama yöntemlerinin üretilmesi amaçlanmıştır. Test ve ölçümlerden elde edilen tepe sinyal-gürültü oranı ve normalleştirilmiş katsayılar da baz alınarak uygulanan yöntemler arasında en iyi sonuç veren yöntem olarak sayısal damgalama yöntemi ayrık dalgacık dönüşümü ve tekil değerler ayrışımı ile sayısal damgalama bulunmuştur. Ancak, gömülü sistemlere uygulanabilirliği, sayısal filigranı damgalanmış görüntü içerisinde çıkarırken orijinal görüntüye ihtiyaç duymaması, sayısal filigran olarak görüntü yerine bit dizisi de kullanabilmesinden dolayı gömülü sistemde gerçeklemek için damgalama yöntemi olarak ayrık kosinüs dönüşümü ile orta frekans bölgesinde yapılan sayısal damgalama yöntemi seçilmiştir.

Tasarlanan gömülü sistemde üreticinin aidiyetini şüphesiz sağlayacak sayısal filigran oluşturmayı, görüntü yakalamayı ve sayısal damgalamayı tek bir yapıda birleştirecek şekilde tasarlanmıştır. Bu hedef doğrultusunda damgalamada kullanılacak sayısal filigran biyometrik damga olarak parmak izi seçilmiştir. Sayısal damgalama için seçilen yöntem çıkarma işlemi sırasında orijinal görüntüye ihtiyaç duyulmadığı ve sayısal filigran olarak biyometrik veri kullanıldığı için gömülü sistemde uygulanan sayısal damgalama yöntemi biyometrik kör sayısal damgalama yöntemi olarak isimlendirilebilir. Gömülü sistemde biyometrik sayısal filigranı oluşturmak için GT-511C3 parmak izi tanıma modülü kullanılmıştır. Oluşturulan gömülü sistemin merkezinde Texas Instruments AM3352 işlemcisinin bulunduğu Beaglebone geliştirme platformu bulunmaktadır. Bu cihaz USB, Ethernet ve SD kart ara yüzlerinden dolayı tercih edilmiştir. Sistemde biyometrik verinin sensor modülünden alınması USB üzerinden gerçekleştirilmektedir. Meydana getirilen yapıda bir diğer önemli eleman ise görüntü yakalamayı sağlayan IP kameradır. Damgalanmak istenen görüntüler merkezi birim Beaglebone tarafından ethernet üzerinden Haikon/Hikvision

DS-2CD2110F-IS IP kameradan alınmaktadır. Beaglebone üzerinde bulunan SD kart ile damgalanmış görüntüler ve IP kameradan yakalanan görüntülerin kayıt edilmesi amaçlanmıştır. Ayrıca tasarlanan gömülü sistem ile IP kameradan görüntü almadan SD kart üzerine daha önceden kayıt edilmiş görüntülerde biyometrik filigran ile damgalanabilmektedir. Parmak izi tanıma sensörü ve IP kamera içeren gömülü sistem üzerinde biyometrik kör sayısal damgalama yöntemi başarıyla gerçekleştirilmiştir. Aynı sistem Beaglebone yerine Intel Core i7-3630QM işlemcisine sahip bir bilgisayar ile de gerçekleştirilmiştir ve iki sistemin performansları karşılaştırılmıştır. Çalışmanın son bölümünde oluşturulan gömülü sisteme üzerinde yapılabilecek yazılımsal ve donanımsal geliştirmelerden de bahsedilmiştir.





DIGITAL WATERMARKIN ON IMAGES AND EMBEDDED SYSTEM APPLICATION

SUMMARY

Nowadays, when we live in the age of computer and internet, the use and sharing of digital media such as audio, image and video are rapidly increasing. Unauthorized modification or direct use of digital media on the Internet, especially on social networking platforms, creates a major problem. In this study, digital watermarking and its methods are suggested for solving problems such as the use of digital media without the creator's permission, violation of copyrights, prevention of copying and preservation of contents.

Digital watermarking is a method that can be used on audio, images, texts and videos to provide copyright information about content creator. To establish a common ground for this method, firstly, the information about a brief history, necessity and usage areas of digital watermarking is given place in this study.

Digital watermarking techniques are methods that allows custom watermarks to be embedded on digital media and to be extracted when it is necessary to compare originality of digital media. In order provide better understanding about these watermarking methods, which subjects are targeted by digital watermarking techniques and how they are classified according to various parameters are explained. Digital watermarking can be classified as visible and invisible according to human perspectives, the methods which are invisible to human eye and can be applied to the images are emphasized. Therefore, the set of digital watermarking methods which are interested in this research are a subset of the science of hiding information which is called steganography.

Although there are digital watermarking methods that can be applied on audio, video, image and text, most of the works related with watermarking are implemented on images. In this work, digital watermarking methods which can be applied on image are emphasized, but most of the watermarking methods used on images also can be applied to video standards such as MJPEG, H.264. For MJPEG streams or videos, watermark can be embedded on every frame or some of the frame selected by content owner, but digital watermark should embed in I-frames for H.264 based videos or streams.

In the literature, there are watermarked methods that developed in spatial domain can be applied on images, but because of various features, digital watermarking methods that use frequency domain in watermarking process are more popular then spatial domain ones. Therefore, in this study, information about the frequency domain transformations that can be applied on the image has been given and the advantages and the disadvantages of these transformations are discussed.

Frequency domain transformations used in JPEG image compression algorithm and H.264 video compression algorithm like discrete cosine transform (DCT) and discrete wavelet transform (DWT) are the most preferred transformations used in digital watermarking methods. Also, other transformations that can be used for digital watermarking like fast Fourier transform, counterlet transform are included in this project.

In this study, information about the digital watermarking methods that can be made on the image has been obtained. For this purpose, 8 separate techniques for digital watermarking in spatial and frequency domain have been studied. In this section, processes that embedding digital watermark to host image and extracting watermark from watermarked image of digital watermarking methods are included, and based on literature search about watermarking, advantages and disadvantages of digital watermarking methods are mentioned. From the analyzed methods, 5 digital watermarking methods; discrete wavelet transform-based watermarking, least significant bit-based watermarking, discrete wavelet transform and singular value decomposition-based watermarking, watermarking technique that uses discrete cosine transform in low frequency region and watermarking technique that uses discrete cosine transform in medium frequency region are implemented for images to determine suitable method for embedded systems.

Another subject of digital watermarking process is immunity of watermarking method against various attacks to destroy watermark embedded in images. For this purpose, information about filters, geometric modifications and compression algorithms that can be used as an attack technique are given in section 2. Images that are watermarked with implemented digital watermarking methods are tested for immunity with following attacks; salt and pepper noise, blurring, contrast change, resizing, brightness change, median filter, image rotation and Gaussian noise. In these tests, peak signal-noise ratio is calculated on attacked images and watermarked images compared with original images so that similarity between these images can be measured. On the other hand, like peak signal-noise ratio, normalized correlation coefficients are calculated to compare original watermark and extracted watermark from watermarked or attacked image. From these measurements, it has been gained the idea of which digital watermarking method is resistant or vulnerable to which attack.

In this study, it is aimed to find digital watermarking technique which can be implemented in embedded systems by investigating the digital watermarking methods that can be applied on the image, which are uncomplicated, resistant to various attacks and will not disturb the system in terms of capacity. Among implemented digital watermarking methods, discrete wavelet transform and singular value decomposition based watermarking technique is found as a best method according to the peak signal-to-noise ratio and the normalized coefficients obtained from the tests and measurements. However, since original host image is not required while extracting the digital watermark from the watermarked image and any images or bit series can be used as a watermark, discrete cosine transform based medium frequency region watermarking technique is chosen to be implemented on embedded system as a digital watermarking method.

In the designed embedded system, digital watermark that guarantees the belonging of the content creator, image capturing, and digital watermarking are combined in a single structure. For this purpose, fingerprint which biometric data is selected as a digital

watermark to be used in watermarking system. Since the selected method for digital watermarking does not require the original image during the extraction process and biometric data is used as the digital watermark, the digital watermarking method implemented in the embedded system can be named as the biometric blind digital watermarking method. Because biometric watermark is used as a watermark, this can cause security vulnerabilities. Thus, to avoid security obligation and protect content creator's biometric data, Fisher-Yates shuffling algorithm is applied to biometric data with key before watermarking process begins.

The GT-511C3 fingerprint recognition module is used to create a biometric digital watermark on the embedded system. On the other hand, Beaglebone development platform with Texas Instruments AM3352 processor stand at the center of the created embedded system. This device is preferred because of its USB, ethernet and SD card interfaces capabilities. Biometric data is moved to Beaglebone over USB interface from fingerprint recognition module. Data exchange between GT-511C3 fingerprint recognition and Beaglebone embedded system module is established over USB with C/C++ programming. To capture, enroll, verify fingerprints and to get 498 Byte fingerprint template, GT-511C3 uses vendor specific protocol which contains command and data packet structures. The protocol that is explained on GT-511C3's datasheet is implemented on Beaglebone side to use these features on sensor module. With this implementation, fingerprint templates which are taken from fingerprint sensor module can be stored on Beaglebone for biometric digital watermarking process.

Another important element in the structure is IP or USB camera as an image capturing device. Both USB and IP cameras can be used in the designed embedded system. However, since USB port of Beaglebone is reserved for finger print recognition module, Haikon/Hikvision DS-2CD2110F-IS IP camera which communicates over ethernet with Beaglebone is preferred as an image capturing device. Images that will be watermarked are captured from MJPEG stream of IP camera using OpenCV and FFMPEG libraries.

In the embedded system, main digital watermarking process which combines fingerprint template from GT-511C3 fingerprint sensor module and captured image from DS-2CD2110F-IS IP camera is implemented on Beaglebone system module using standard C/C++ and OpenCV libraries. SD Card that is located on Beaglebone are planned to store received images from IP camera and images that are watermarked with biometric data. Also, with using biometric watermark which is taken from GT-511C3 fingerprint recognition module, the designed embedded system can perform digital watermarking on previously recorded images on SD card without taking any images from IP camera.

The biometric blind digital watermarking method has been successfully performed on the embedded system that has the fingerprint recognition sensor and the IP camera. Similar biometric watermarking system was implemented on a computer with Intel Core i7-3630QM processor and 8 GB memory instead of Beaglebone, and the performance of the two systems was compared. In the last section of the study, software and hardware enhancements that can be made on designed biometric digital watermarking embedded system like encryption algorithms that can be implemented by using crypto accelerator on AM3352, recovery algorithms, integrity control methods are discussed.



1. GİRİŞ VE ÇALIŞMANIN AMACI

Günümüzde sayısal medyanın yükselişe geçmesinden dolayı günlük yaşantının her bölümünde ses, video, görüntü gibi sayısal içeriklerin kullanımı artmaktadır. Özellikle bilgisayar ve ağ teknolojileri üzerinde yapılan sayısal veri paylaşımları bu veriler üzerindeki telif hakkı ve aidiyet korunması sorununu ortaya çıkarmaktadır, çünkü sayısal içeriklerin kopyalanması ve değiştirilebilmesi oldukça kolaydır. Sayısal içeriklerin üreticisinin veya yaratıcısının izni olmaksızın kullanılması, içeriğinin değiştirilmesi ve ticari amaçlı yarar sağlanmasının önüne geçilebilmesi zor bir problemdir.

Sayısal damgalama yöntemleri, sayısal içerik üzerindeki telif hakkı problemleri çözmek için gün geçtikçe daha çok rağbet gören yaklaşımları temsil etmektedir. Bu amaca yönelik olarak, son yıllarda literatürde fark edilmezlik, ekleme kapasitesi ve sağlamlık kısıtlamalarını birleştiren birçok teknik önerilmiştir. Pratikte, bir sinyalin, algılanması çok zor olan, ama aynı zamanda çıkarılması da çok zor bir şekilde, görüntü verisine doğru bir şekilde gizlenmesi gerekmektedir [3]. Tüm bu ihtiyaçlar göz önüne alındığında, sayısal damgalamaya olan gereksinim ve bununla ilgili yöntemlerin geliştirilmesi hiçbir zaman olmadığı kadar önem kazanmıştır.

Sayısal damgalama ile ilgili çalışmaların 1954 yılında Emil Hembrooke'un Muzac Corporation adına aldığı "Identification of sound and like signals" başlıklı patent ile başladığı düşünülmektedir [1]. Bu patentte sayısal damgalama "Bu buluş, bir müzikal sunumun kökeninin pozitif olarak tanımlanması mümkün kılınır ve bu şekilde korsanlığı önlemek için etkili bir araç teşkil eder, yani kâğıda basılan bir filigrana benzetilebilir." şeklinde belirtilmektedir [2].

Sayısal damgalama ile ilgili çalışmalar, özellikle ses, görüntü ve videonun dünya genelinde yayılması ile beraber 2000 yılından sonra hızla artmaya başlamıştır. Ancak sayısal damgalama terimi ilk olarak 1992 yılında Andrew Z. Tirkel ve Charles F. Osbourne tarafından ortaya atılmıştır. 1993 yılında, 512*512 boyutundaki 8-bit siyah-beyaz bir görüntü üzerine insan perspektifi açısından görülemeyen sayısal damgalama

yöntemi Andrew Z. Tirkel, Charles F. Osbourne, R.M. van Schyndel, W.J. Ho, N.R.A. Mee ve Gerard Rankin tarafından bilim dünyasına tanıtılmıştır [4].

1.1 Sayısal Damgalamanın Kullanım Alanları

Sayısal medya içeriklerinin tüm dünya çapında kolaylıkla paylaşılabilir olması, sayısal damgalama yöntemlerinin hızlı gelişmesine neden olmuştur. Bunun sonucunda bu yöntemler birçok uygulamada kullanılmaya başlanmıştır.

Sayısal damgalamanın kullanıldığı en önemli uygulamalar telif hakkı koruması uygulamalarıdır. Sayısal damgalama yöntemleri, telif hakkıyla korunan malzemelerin internet gibi güvenilirliği az olan ağ üzerinden yeniden dağıtımından korumak için kullanılabilir [7]. Verilerin internet üzerinden doğrudan veya değiştirilerek paylaşılması sırasında, korunaklı dağıtım yollarına ihtiyaç vardır. Sayısal damgalamanın en belirgin uygulamaları yasal veya korsan yayınlarda görülen izinsiz kullanımları ve hak ihlallerini engellemek için başlamıştır. Sayısal damgalama yöntemleri, yayından önce her videoya veya ses klibine benzersiz bir filigran koyularak kullanıla bilinir. Otomatik izleme istasyonları daha sonra yayınları alabilir ve bu filigranları arayabilir, her klibin ne zaman ve nerede görüntüleneceğini belirlenebilir. Bu şekildeki ticari sistemler uzun yıllardır kullanılmaktadır [6].

Sayısal damgalamanın kullanıldığı bir diğer alan sahiplik onayı uygulamalarıdır. Standart metinsel telif hakkı bildirimleri kolayca çıkarılabildikleri için ilgili sınırlamalar vardır. Fiziksel belgede basılı olan telif hakkı bildirimi, dijital içerikle birlikte kopyalanamaz [8]. Bir hak sahibi, sahipliğini kanıtlamak için sayısal damgalama yöntemi ile yerleştirdiği filigranı sayısal içerikten alabilir.

Benzersiz işaretleme, sayısal damgalama yöntemlerinin kullanıldığı diğer bir uygulamadır. Burada sayısal damga veya filigran bir seri numara gibi davranmaktadır. Bu uygulamada, ürün sahibi her müşteri kimliğine göre farklı filigranlar yerleştirmelidir. Bu, filigran olarak kullanılan verilerin, müşterinin bilgilerine göre seçileceği anlamına gelir. Bu yöntem, sahibin yasadışı kopya kaynağını ve herhangi bir şekilde lisans sözleşmesini bozan müşteriyi kolayca bulmasını sağlar [9].

Medikal uygulamalarda oluşturulan görüntüleri hastanın bilgilerini içerecek şekilde sayısal damgalama ile işaretlemekte mümkündür. Bu uygulama tıbbi kayıtları aramada

belirsizlikleri önlemede yardımcı olur [11]. Yukarıda anlatılan uygulamalar dışında sayısal damgalama yöntemlerinin kullanıldığı alanlar şu şekilde sıralanabilir: sayısal hak yönetimi, kurcalamaya karşı koruma, giriş kontrolü, görüntü ve içerik kimliği doğrulama, ek açıklama ve gizlilik kontrolü, medya adli bilimi, iletişim geliştirme, ses ve video içeriği için içerik koruması, içerik filtreleme, medya içerikleri üzerinde geliştirilmiş denetim [10].

Bu çalışmada dışarıdan gelen saldırılara, sıkıştırma algoritmalarına karşı dayanıklı, işlem gücü düşük dolayısıyla gömülü sistemlere uygun ve görüntü veya video üzerine uygulanabilen bir sayısal damgalama yönteminin kazanımı hedeflenmektedir.





2. GÖRÜNTÜ ÜZERİNDE SAYISAL DAMGALAMA VE YÖNTEMLERİ

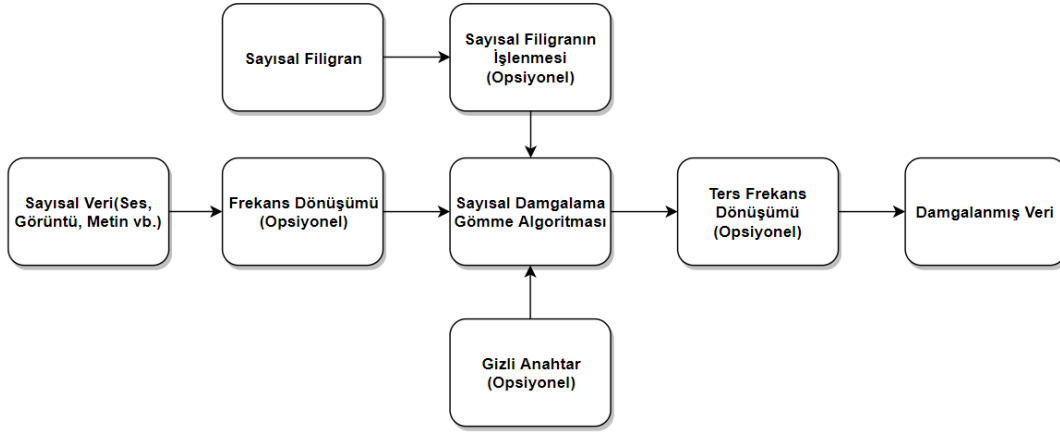
Sayısal damgalama; ses, görüntü, video ya da herhangi bir sayısal medya üzerinde telif haklarının önlenmesi veya bilgi gizlenmesi amacı ile kullanılan bir yöntemdir. Damgalama sırasında kullanılan yöntemler steganografik yöntemlerdir, bu yöntemler iyi bir damgalama için gürültüye, işaret saldırılarına ve sıkıştırma algoritmalarına karşı dayanıklılığı yüksek olmalıdır. Sayısal bir medya içerisinde gizlenmiş bir damga, eğer tahribata uğrayabiliyorsa ve bu tahribattan sonra bir geri dönüşüm ile tekrar elde edilemiyorsa damgalama işleminin başarısız olduğu sonucuna varılır.

Sayısal damgalama yöntemlerinin hedefleri aşağıdaki gibi sıralanabilir [7].

- **Sahiplik iddiası;** içerik (ses, görüntü, video vb.) üzerinde telif hakkı talep edilmesini sağlama.
- **Benzersiz işaretleme;** bu teknik, kamuya açık çoklu ortam içeriğinin yetkisiz çoğaltılmasını ve dağıtılmasını önlemek için kullanılır ve uygulanır.
- **Doğrulama ve bütünlük doğrulama;** doğrulayıcı, içeriğe, içerikle ilişkili benzersiz bir anahtara sahip olan ve filigranı çıkararak bu içeriğin bütünlüğünü doğrulayabilen içeriğe ayrılmaz bir şekilde bağlıdır.
- **İçeriğin etiketlenmesi;** zaman ve yer bilgisiyle grafik bir görüntü gibi içerik hakkında daha fazla bilgi veren verilerin damgalanması işlemidir.
- **Kullanım kontrolü;** bazı sistemlerde, içeriğin yasa dışı kopyasını önlemek veya kopyalanma sayısını sınırlamak için bir kopya ve kullanım kontrol mekanizmasıdır.

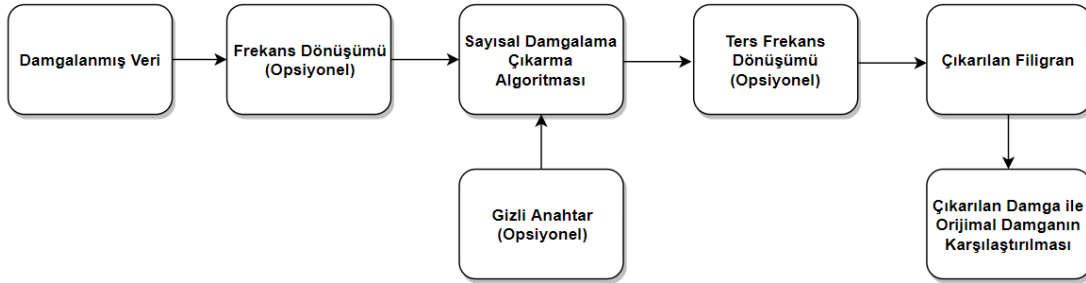
Sayısal damgalama yöntemleri, yukarıda bahsedilen hedeflerden biri veya birkaçını sağlayabilir.

Sayısal damgalamada, damgalamanın yapılacağı veri ya da medyaya konak veya ev sahibi ismi verilir, damga olarak kullanılacak veriye ise sayısal filigran olarak adlandırılır. Sayısal filigran, konak veriye yerleştirilmesi işlemine gömme, konak veriden tekrar elde edilmesine çıkarılma işlemi denir.



Şekil 2.1 : Sayısal filigran gömme şeması

Şekil 2.1’de sayısal damgalama yöntemlerinin genel işlem sırası gösterilmektedir. Sayısal damgalama şemasının merkezinde gömme algoritması yer alır, bazı damgalama yöntemlerinde sayısal filigranın boyutunun küçültülmesi veya şifrelenmesi için ön işlem uygulanabilmektedir. Ayrıca damgalama işleminin saldırılara karşı daha dirençli olması için frekans bölgesine dönüşüm yapılabilmektedir. Güvenliğin artırılması için gizli anahtar da sisteme eklemek mümkündür.

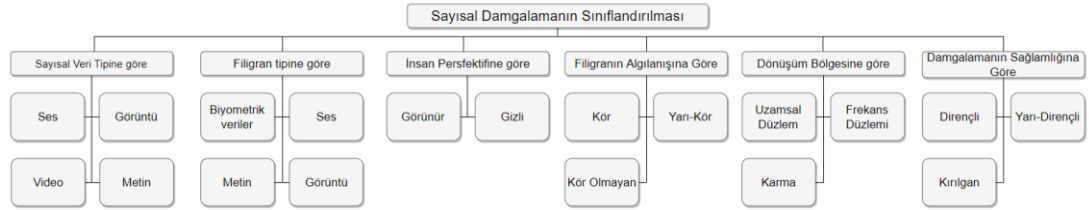


Şekil 2.2 : Sayısal filigran çıkarma şeması

Sayısal damgalama yöntemleriyle damgalanmış bir görüntüden damganın geri elde edilmesi en kritik adımdır. Eğer gömme işlemi frekans bölgesinde yapıldıysa damgalanmış veriye tekrar frekans dönüşümü uygulanarak frekans bölgesine geçilir. Sayısal damgalama çıkarma algoritması ve ihtiyaç var is gizli anahtar ile beraber uygulanır. Çıkarma algoritmaları genel gömme algoritmalarının tersi şeklindedir. Bu işlemlerin sonucunda çıkarılan filigran, orijinal filigran ile karşılaştırılarak başarı gözlemlenir. Sayısal filigran çıkarma işlemine ilişkin blok diyagram Şekil 2.2’deki gibidir.

2.1 Damgalama Yöntemlerinin Sınıflandırılması

Sayısal damgalama yöntemlerinin daha iyi anlaşılabilmesi ve çalışma sırasında gerekli tanımlama yapılabilmesi için sayısal damgalamanın sınıflandırılması oldukça önemlidir. Sayısal damgalamaya ilişkin sınıflandırma şeması şekil 2.3'deki gibidir.



Şekil 2.3 : Sayısal damgalamanın sınıflandırılması

2.1.1 Sayısal veri tipine göre sınıflandırılma

Sayısal damgalama işlemleri birçok sayısal veri üzerine uygulanabilmektedir. Bunlardan en önemlileri ses, video, metin ve görüntüdür.

Bu çalışmada görüntü üzerinde yapılan damgalama yöntemleri üzerinde durulacaktır, bu yüzden ses, video, metin vb. verilerde yapılabilen damgalama işlemlerine yer verilmeyecektir. Ancak görüntü üzerinde yapılabilen damgalama yöntemleri video dosyasındaki her bir kareye ya da seçilen karelere uygulanabilir.

2.1.2 Filigran tipine göre sınıflandırma

Damgalama sırasında sayısal veri üzerine gömülecek filigranın çeşidi bu sınıflandırmayı belirleyen etkidir. Teknik olarak ses, görüntü, metin vb. herhangi bir veri filigran olarak kullanılabilir.

Filigranın seçilmesinde önemli unsur aidiyetin belirli olmasıdır. Sayısal damgalamadan telif hakkı iddia edilebilmesi için damganın özel bilgiler içermesi gerekmektedir. Eğer kişiye özel bir damgalama yapılacaksa parmak izi, göz irisi vb. biyometrik veriler filigran için oldukça iyi malzemelerdir. Fakat biyometrik verilerin damga olarak kullanılması ifşa olma riski olduğundan güvenlik açığına yol açabilmektedir. Bu yüzden damga olarak kullanılacak olan biyometrik verinin damgalanmadan önce şifrelenmesi veya kodlanması gerekmektedir [5].

2.1.3 İnsan perspektifine göre sınıflandırılma

Bu sınıflandırma ile damgalama yöntemlerini insan algısı ile doğrudan algılanabilen veya algılanamayan olarak ikiye ayırmak mümkündür. Doğrudan algılanamayan damgalama yöntemlerinde, orijinal görüntünün insan algısı açısından bozulmaya uğramaması gerekmektedir.



Şekil 2.4 : a) Görünmez filigran ile damgalanmış görüntü b) Görünür filigran (İTÜ logosu) ile damgalanmış görüntü

Şekil 2.4’de de görülebileceği gibi görüntü üzerinde yapılan damgalama işleminde (b)’de yer alan resimde filigran görünür şekildedir, fakat (a)’daki resimde filigran doğrudan resmin içerisine gömülmüştür dolayısıyla resim üzerinde dekodlama yapılmadan filigrana ulaşmak mümkün değildir.

2.1.4 Damgalamanın sağlamlığına göre sınıflandırılma

Damgalama yönteminin dışarıdan gelen saldırılara karşı olan direncine göre sınıflandırmadır. Kırılgan damgala yöntemleri oldukça hassastır, dışarıdan yapılan saldırılara karşı bağışıklıkları çok azdır. Görüntü üzerinde uygulanan bu tür yöntemler bulanıklaştırma, sıkıştırma gibi saldırılarla kolayca içerisindeki filigranı kaybedebilir. Yarı-kırılgan ve yarı-dirençli yöntemlerde, filigranlı sinyaldeki değişiklikler önceden tanımlanmış bir kullanıcı eşiğini aşarsa bu filigranlar kırılır. Eşik sıfıra ayarlanırsa, o zaman kırılgan bir filigran olarak çalışır. Bu yöntem, veri bütünlüğünü ve veri kimlik doğrulamasını sağlamak için kullanılabilir [11].

Dirençli sayısal damgalama yöntemleri ise dışardan gelen saldırılara karşı oldukça dayanıklıdır ve sayısal damgalanma yapılmış veri içerisindeki filigran silinmeye veya

bozulmaya çalışıldığında damgalanmış veri de bozulmaya uğrar. Böylece filigransız kullanımın önüne geçilmiş olur. Bu yöntemler özellikle sıkıştırma algoritmalarına dirençli olabilmesi için frekans bölgesinde yapılmaktadır.

2.1.5 Damgalama algılanışına göre sınıflandırılma

Damgalama işleminin en önemli basamaklarından biri de damgalanmış sayısal veriden filigranın geri çıkarılmasıdır. Bu sınıflandırma damgalanmış veriden filigranın çıkarılması sırasında ihtiyaç duyulan bilgiye göre yapılır.

Kör damgalamada, damgalama yöntemi dışında hiçbir bilgi olmaksızın filigran doğrudan damgalanmış veri içerisinde çıkarılır [5].

Yarı-kör damgalama yöntemlerinde, sayısal filigran içeren veriden orijinal filigranı çıkarmak için bazı özel bilgiler gerekmektedir [12]. Bu bilgiler sayısal filigranı bütünüleyici şekildedir.

Kör olmayan damgalama tekniklerinde ise, sayısal filigranlı medya içeriğinden (ses, görüntü, video vb.) gömülü bilgileri algılamak için orijinal medya içeriğine ihtiyaç vardır. Kör damgalama yöntemlerine kıyasla sinyale yapılan saldırılara karşı daha dayanıklıdır.

Genel olarak kör damgalama yöntemleri ile gömülebilecek veri kapasitesi diğer yöntemlere göre daha azdır, fakat filigranın algılanması sırasında ilave yük getirmemesi büyük bir avantajdır.

2.1.6 Dönüşüm bölgesine göre sınıflandırılması

Damgalama işlemi; uzamsal alan doğrudan sayısal verinin üzerine veya çeşitli dönüşümler kullanılarak frekans bölgesinde yapılabilir. Bu dönüşümlerden en önemlileri DCT (Ayrık Kosinüs Dönüşümü), DFT (Ayrık Fourier Dönüşümü), DWT (Ayrık Dalgacık Dönüşümü) gibi işlemlerin frekans bölgesinde yapıldığı dönüşümlerdir. Görüntü için uzamsal alanda yapılan sayısal damgalama işleminde doğrudan pikseller üzerinde işlem yapılabilir, fakat doğrudan piksel üzerinde işlem yapıldığı için bu yöntemler kırılmalıdır ve görüntü üzerinde bozulmalara neden olabilir.

2.2 Damgalama yöntem ve kodlama teknikleri

Sayısal damgalama yöntemleri hakkında bilgiler verilmeden önce bu yöntemlerde kullanılan dönüşümlerin bilinmesi gerekmektedir. Uzamsal alanda damgalama işlemi yapılabilmesine rağmen frekans bölgesinde yapılan damgalama işlemleri dışardan gelen saldırılara ve özellikle sıkıştırma algoritmalarına bağışlıkları daha fazladır.

2.2.1 Görüntü damgalama sırasında kullanılabilecek dönüşüm yöntemleri

2.2.1.1 Ayırık Kosinüs Dönüşümü

Ayrık kosinüs dönüşümü, bir işaret veya görüntüyü frekans bileşenlerini ayırarak üzerinde işlem yapılabilme olanağı veren matematiksel bir yöntemdir. Bu dönüşüm günümüzde kullanılan MP3, H.264, JPEG gibi birçok sıkıştırma algoritmasının temel unsurudur. Ayırık kosinüs dönüşümü kullanılarak, bir görüntü veya işaret değişken büyüklükler ve frekansların kosinüs ve sinüs toplamı şeklinde ifade edilmesi sağlanır. Görüntü üzerinde sayısal damgalama yönteminde kullanılabilecek 2-D ayırık kosinüs dönüşümünün ve 2-D ters ayırık kosinüs dönüşümünün denklemleri sırasıyla denklem 2.1 ve denklem 2.2'e verilmiştir.

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \leq p \leq M-1 \\ 0 \leq q \leq N-1 \end{matrix} \quad (2.1)$$

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \leq m \leq M-1 \\ 0 \leq n \leq N-1 \end{matrix} \quad (2.2)$$

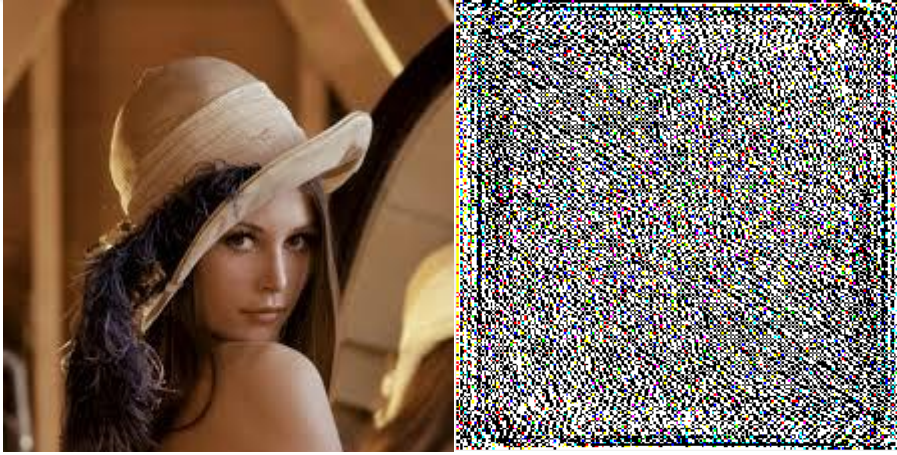
Burada α_p ve α_q denklem 2.3'deki gibi tanımlanmıştır.

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M-1 \end{cases} \quad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N-1 \end{cases} \quad (2.3)$$

$$Y_{p+1,q+1} = \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} \omega_m^{jp} \omega_n^{kq} X_{j+1,k+1} \quad \begin{matrix} \omega_m = e^{-2\pi i/m} \\ \omega_n = e^{-2\pi i/n} \end{matrix} \quad (2.4)$$

$$X_{p,q} = \frac{1}{m} \sum_{j=1}^m \frac{1}{n} \sum_{k=1}^n \omega_m^{(j-1)(p-1)} \omega_n^{(k-1)(q-1)} Y_{j,k} \quad (2.5)$$

Burada ω_m and ω_n , eşitliğin karmaşık kökleridir. FFT ve DFT dönüşümleri, DCT'ye göre daha kompleks ve daha fazla işlem basamağı içermesine rağmen sayısal damgalama yöntemlerinde tercih edilebilmektedir. Bunun nedeni Fourier dönüşümlerinin, damgalanmış görüntü üzerine yapılan saldırılara karşı daha dirençlidir. Görüntü üzerinde yapılan FFT dönüşüm Şekil 2.6'de verilmiştir.



Şekil 2.6 : Görüntü üzerinde FFT dönüşümü

2.2.1.3 Ayırık Dalgacık Dönüşümü

Sayısal damgalama yöntemlerinde en çok kullanılan güçlü dönüşüm yöntemlerinden biri ayırık dalgacık dönüşümü, DWT'dir. Güncel uygulamalardan JPEG2000 sıkıştırması bu dönüşümü kullanmaktadır. DWT, sayısal filigranların gömülebildiği alt bantlara ayrıştırabildiğinden, sayısal damgalama alanında büyük bir popülerite bulur. DWT ayrıca bir görüntüyü hiyerarşik olarak ayrıştırmak için matematiksel bir araçtır. Orijinal görüntüyü daha düşük yakınlaştırma görüntüsü (LL), yatay (HL), dikey (LH) ve diyagonal (HH) olarak isimlendirilen dört alt banda ayırır [14].

LL	HL	LL ₂	HL ₂	HL ₁	LL ₃	HL ₃	HL ₂	HL ₁
		LH ₂	HH ₂		LH ₃	HH ₃		
LH	HH	LH ₁		HH ₁	LH ₁		HH ₂	

Şekil 2.7 : Sırasıyla 1., 2. ve 3. dereceden DWT dönüşümleri

Ayrık dalgacık dönüşümü ile bantlar oluşturulur, istenildiği takdirde seviye arttırılarak daha fazla bant elde edilebilir. Bant seviyesindeki artış sayısal damgalamanın daha spesifik noktalara yapılmasına yardımcı olabilir. 1.seviye, 2.seviye ve 3.seviye dalgacık ayrışmaları şekil 2.7’de yer almaktadır. Ayrık dalgacık dönüşümü kullanılarak siyah-beyaz görüntüden elde edilen çıktı şekil 2.8’da verilmiştir.



Şekil 2.8 : Görüntünün 2. dereceden DWT dönüşümü

2.2.1.4 Çevrecik Dönüşümü

Çevrecik (Konturlet) dönüşümü, M.N Do ve M. Vitterli'nin ortaya koyduğu, konturları ve dokuları içeren görüntüleri etkili bir şekilde temsil edebilen geometrik bir görüntü tabanlı dönüşümdür. DWT, filigran teknikleri arasında popüler, güçlü ve tanınmış olmasına rağmen, düz konturlar ve görüntünün yönelimli kenarları gibi yönlü bilgileri

yakalama konusunda kendi sınırlamalarına sahiptir [16]. Bu problem, çevrecik dönüşümüyle çözülebilmektedir.

Çevrecik dönüşümde, ilk olarak laplasyan piramidi (LP) nokta süreksizliklerini yakalamak için kullanılır. Daha sonra nokta süreksizliklerini lineer yapılara bağlamak için bir yönlü filtre bankası (DFB) izler. Gerekli yönlendirme sayısı kullanıcı tarafından belirlenebilir. Çevreler daha fazla kenar sağladığından, veri gizleme uygulamaları için daha uygundur. Orijinal görüntüyü bozmadan algılamaksızın yüksek frekans bölgelerinde daha fazla veri gizlenebilir. Bu, çevre bölümleri gibi temel elemanları kullanarak bir görüntü genişlemesi ile sonuçlanır ve böylece piramidal yönlü filtre bankası (PDFB) tarafından uygulanan çevrecik dönüşümü olarak adlandırılır [15].

Çevrecik yöntemi ile yüksek frekansların olduğu kenar ve çevreler ayırık kosinüs dönüşümüne göre daha kesin bir şekilde bulunur. Sayısal damgalama işlemi yüksek frekanslara yapılabilmesine imkân sağlamaktadır.

İnsan gözü, görüntülerdeki yüksek frekans bileşenlerden çok düşük frekanstaki bileşenlere daha duyarlıdır. Bu yüzden kayıplı sıkıştırma algoritmalarında öncelikle yüksek frekansta veri atılmaya başlanmaktadır. Bu gerçek göz önüne alındığında DCT, FFT ve DWT dönüşümlerinde düşük frekans bölgesine yapılan sayısal damgalamalar, çevrecik dönüşümüyle yüksek frekans bölgelerine yapılan sayısal damgalamalara göre sıkıştırma algoritmalarına karşı daha dirençli olacaktır.

2.2.2 Sayısal damgalama için kullanılan yöntemler

1993 yılında sayısal damgalama terimi kullanılarak ilk yöntemler ortaya çıkmaya başlamıştır. Sayısal damgalama ile ilgili yüzlerce çalışma yapılmıştır. Bu yöntemlerden önemli olanları ve orijinal konak görüntü üzerinde değişikliğe yol açmayan görünmez sayısal damgalama teknikleri aşağıdaki başlıklarda incelenmiştir.

2.2.2.1 Uzamsal alanda LSB damgalama yöntemi

Görüntü üzerinde uzamsal alanda yapılan damgalama yöntemleri doğrudan imge üzerindeki pikseller üzerine yapılır. Genel olarak siyah-beyaz görüntüler için bir piksel 8-bit, renkli görüntüler ise bir piksel için RGB 3x8-bitlik alanlar kullanılmaktadır. Bu piksellerde yer alan 8-bitlik yapıların LSB (en az anlamlı bit)'lerinde yapılan manipülasyonlar ile damgalama işlemi sağlanabilir.



Şekil 2.9 : LSB yönteminin temsili[17]

En basit LSB damgalama yöntemine ilişkin şema şekil 2.9'de verilmiştir. Bu yöntemde gizli anahtar temel alınarak piksellerin LSB'lerinde manipülasyon yapılmaktadır.

LSB damgalama yöntemin bir piksel gizli anahtar ile karşılaştırılarak bu piksele gömme işlemi yapıp yapılmayacağına karar verilir ve her piksele filigranın bir biti gömülebilir. Filigranın damgalanmış görüntüden çıkarılması da benzer şekilde gizli anahtar kullanılarak tersten uygulanır. Bu yöntemde LSB'den başlayarak MSB'e kadar damgalama işlemi bir veya daha fazla bit için yapılabilir. Fakat MSB'ye yaklaştıkça görüntüde bozulma olmaya başlayacaktır. LSB'ye yapılan damgalama yöntemleri basittir ve uygulaması kolaydır. Fakat oldukça kırılgan bir damgalama yöntemidir. Dışarıdan gelecek saldırılara ve sıkıştırma algoritmalarına karşı dayanıksızdır.

2.2.2.2 Uzamsal alanda CDMA ile damgalama yöntemi

Uzamsal alanda yapılabilen birçok damgalama yöntemi vardır, bunlardan dikkat çeken bir diğer uygulamada CDMA (Kod Bölmeli Çoklu Erişim) ile yapılan damgalama yöntemidir. Bu yöntemde LSB yer değiştirme yöntemi gibi uzamsal uzayda gerçekleştirilir ve haberleşme alanında kullanılan CDMA tekniği kullanılır. Bu teknikte öncelikle bit dizisi PN(Pseudo-Noise) serisine çevrilir [18]. Daha sonra denklem 2.6'da verilen formülasyon ile konak görüntüye gömülür.

$$I_w(x, y) = I(x, y) + \alpha * PN \quad (2.6)$$

Denklem 2.6'da yer alan $I(x, y)$, x ve y konumundaki pikseli, $I_w(x, y)$ ise damgalanmış pikseli temsil etmektedir. α katsayısı ise sayısal damgalama algoritmasının gücünü

temsil eder. Bu katsayı arttıkça yöntemin dayanıklılığı artar, fakat görüntüde bozulmalara yol açacaktır.

Bu yöntemde gömülen filigranın çıkarılması için orijinal görüntüye ihtiyaç vardır dolayısıyla kör olmayan damgala yöntemidir. Orijinal görüntü ve denklem 2.6'da yer alan formulasyon kullanılarak gömülmüş filigran damgalanmış görüntüden çıkarılabilir. CDMA ile yapılan damgalama işleminin özellikleri LSB ile yapılan damgalama sistemine oldukça benzemektedir, bu yüzden direnci benzer karakteristiği gösterecektir.

2.2.2.3 DCT temelli alçak frekans bölgesinde yapılan damgalama yöntemi

DCT dönüşümünde üç temel frekans bölgesi vardır, bu bölgelerden alçak frekans bölgesi insan perspektifine en çok hitap eden kısımdır. Bu yüzden bu bölgenin kayıplı sıkıştırma algoritmalarında atılması çok zordur. Bu bölgede yapılan sayısal damgalamanın dışarıdan gelecek saldırılara karşı gösterdiği direncin yüksek olması beklenmektedir.

Bu yöntem için konak görüntü önce 8x8'lik bloklara ayrılır ve her bloğun ayrık kosinüs dönüşümü alınır. Her bloğun alçak frekans bölgesindeki, DC katsayısına(c_{00}) ve ilk 3 AC katsayılarına(c_{01}, c_{10}, c_{11}), sayısal filigran verisi 2x2'lik matrislere ayrılarak denklem 2.7'deki gibi formülasyon ile gömme işlemi gerçekleştirilir [19].

$$c'_{ij}(k) = \begin{cases} c_{ij}(k)(1 + \alpha_{ij}) & \text{eğer } w_{ij}(k) = 1, \\ c_{ij}(k)(1 - \alpha_{ij}) & \text{eğer } w_{ij}(k) = 0. \end{cases} \quad (2.7)$$

Burada ω_{ij} sayısal filigran verisinin 2x2'lik matrislerinin elemanları ve α_{ij} , AC ve DC katsayılarına göre değişen katsayılar. Bu sayısal damgalama yönteminde, DC katsayılar için bu değer 0.02, AC katsayılar için 0.1 kullanılarak iyi sonuçlar elde edilmiştir [19] Gömme işlemi bittikten sonra ters DCT ile damgalanmış görüntü elde edilir.

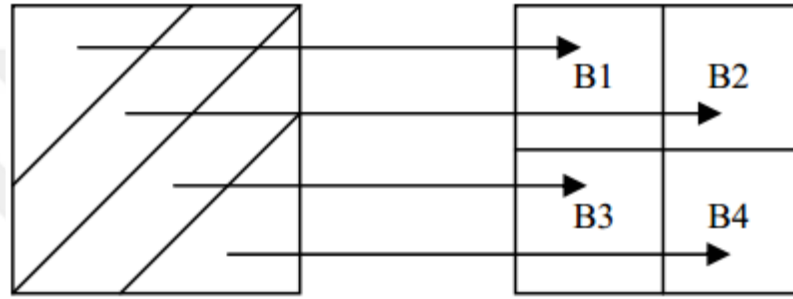
Bu yöntem, kör-olmayan sayısal damgalama olarak sınıflandırılabilir çünkü sayısal Orijinal görüntü ve damgalanmış görüntünün ayrık kosinüs dönüşümü alınarak yukarda belirtilen damgalama işlemi tersten uygulanır filigranın çıkarılması sırasında orijinal konak görüntüye ve orijinal filigrana ihtiyaç vardır.

Alçak frekans bölgesinde yapılan bu damgalama yöntemi birçok saldırı yöntemine karşı dayanıklı olmasına rağmen sayısal filigranın konak görüntü içerisinde çıkarılması esnasında hem orijinal konak görüntüsüne hem de orijinal filigrana ihtiyaç

duyar. Bu durum ilave orijinal görüntünün saklanması problemi ortaya çıkarmaktadır.

2.2.2.4 DCT ve SVD temelli damgalama yöntemi

Sayısal filigranın konak görüntüye gömülmesi için sayısal kosinüs dönüşümü ve Tekil Değer Ayırışımından (SVD) yararlanılmaktadır. Gömme işleminde, diğer DCT kullanılan sayısal damgalama yöntemlerinde olduğu gibi öncelikle konak görüntü uzamsal alandan frekans bölgesine dönüştürülür. Daha sonra elde edilen frekans uzayındaki görüntü aşağıdaki gibi zikzak mantığı ile şekil 2.8'deki gibi 4 parça birleştirilir.



Şekil 2.10 : Frekans bölgesinde biçim değiştirilmesi

Bu biçimlendirme yapıldıktan sonra denklem 2.8 dikkate alınarak her 4 bölge için SVD eşitliği yazılır ve tekil değerler (Σ_X^k) bulunur.

$$X^k = U_X^k \Sigma_X^k V_X^{kT}, k = 1, 2, 3, 4 \quad (2.8)$$

Benzer şekilde sayısal filigrana da SVD denklem 2.9'daki gibi uygulanır ve Σ_w tekil değerleri elde edilir.

$$W = U_w \Sigma_w V_w^T \quad (2.9)$$

Konak görüntüden ve sayısal filigrandan, SVD kullanılarak çıkarılan tekil değerler aşağıdaki denklem 2.10 ile toplanarak damgalanmış görüntü için yeni tekil değerler oluşturulmaktadır.

$$\Sigma_X^{*k} = (\Sigma_X^k + \Sigma_w) \cdot \alpha, k = 1, 2, 3, 4 \quad (2.10)$$

Bu toplama işlemi damgadan elde edilen Σ_w değerleri bitene kadar devam etmektedir (Σ_w bittikten sonra kalan Σ_X^k değerleri değiştirilmeden devam etmekte) ve yöntemde formülasyondaki α değişkeni 0,25 olarak alınmıştır [20]. Bu işlemden sonra oluşan yeni Σ_X^{*k} tekil değerler aşağıdaki gibi kullanılarak denklem 2.11 kullanılarak damgalanmış veri oluşturulur.

$$X^{*k} = U_X^k \sum X^k V_X^{kT}, k = 1,2,3,4 \quad (2.11)$$

X^{*k} matrisinde zikzak ile dörde bölmekten kaynaklanan yer değişikliği eski haline döndürülür ve ters kosinüs dönüşümü yapılarak damgalanmış görüntü elde edilir.

Damganın görüntüden çıkarılma işlemi için damgalanmış görüntü ile birlikte orijinal konak görüntüsüne ve sayısal filigrana ihtiyaç vardır. Orijinal konak görüntüsü, damganın çıkarılması için kullanılır, sayısal filigran ise damga ile karşılaştırma yapılabilmesi için kullanılır. Damganın görüntüden çıkarılması için gömme işlemi tersten uygulanır. Önce damgalanmış görüntünün ayrık kosinüs dönüşümü alınır ve SVD uygulanarak tekil değerleri elde edilir. Daha sonra orijinal görüntünün ayrık kosinüs dönüşümü alınır ve SVD uygulanarak tekil değerleri elde edilip, damgalanmış görüntününükilerden çıkarılır (Denklem 2.12).

$$\Sigma_A = (\sum X^{*k} - \sum X^k) / \alpha, k = 1,2,3,4 \quad (2.12)$$

Böylece damganın tekil noktaları elde edilir. Bu tekil noktalar, telif hakkı iddia eden kişinin parmak izinden elde edilen Σ_A matrisinin tekil değerleri ile aynı ise damgalanmış görüntüden çıkan filigranın başarılı olduğu söylenebilir. Damgalama yöntemi, DCT ve SVD kullanılarak yapıldığından işaret ataklarına karşı dayanıklı fakat gömme ve çıkarılma işlemleri için çok sayıda işlem gerektiğinden karmaşıklığı yüksektir [20].

2.2.2.5 DCT temelli orta frekans bölgesinde yapılan damgalama yöntemi

Bir görüntünün içerisine damgalama yapılabilmesi için iki önemli parametre vardır, damgalama sonucunda orijinal görüntünün bozulmaması ve işaret saldırılarına veya sıkıştırma algoritmalarına karşı damganın bağımsızlığı. Bu koşulları sağlayan en uygun bölge F_M , orta frekans, bölgesidir. Çünkü bu bölge F_L 'nin aksine görüntünün üzerinde majör bir etkisi yoktur ve F_H bölgesi gibi sıkıştırma ve işaret saldırılarına karşı duyarlı değildir [5]. Böylece F_M bölgesi seçilerek, damgalama yapılırken hem orijinal görüntüye zarar verilmemiş olur hem de gömülen filigran tahribata karşı dayanıklı olur.

Bu yöntemde damgalama için orta frekans bölgesi seçilmiş ve damgalamanın sağlamlığı açısından JPEG sıkıştırmasında en çok kullanılan katsayı tablosundan yararlanılmıştır. Bu Şekil 2.11'daki JPEG katsayı matrisi incelendiğinde orta frekans bölgesinde bulunan (4,1) ile (3,2) veya (5,2) ile (4,3) lokasyonlarında bulunan katsayılar birbiri ile aynı değerde olduğu görülür. Bu lokasyonlarda yer alan katsayılar

birbiri ile aynı olduğundan bunlar ile yapılan işlemler benzer etkiyi yaratmaktadır ve bu lokasyonların kendi aralarında yer değiştirilmesi aynı frekans bandı üzerinde yer aldıklarından dolayı orijinal görüntü üzerinde gözlenebilir bir değişikliğe neden olmamaktadır [5].

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Şekil 2.11 : JPEG katsayı matrisi

Filigranın gömülmesi veya kodlanması için öncelikle damgalama yapılması istenen konak görüntü 8x8'lik bloklara ayrılır, daha sonra bu blokların ayrık kosinüs dönüşümü alınarak frekans bileşenlerini içeren B bloğu elde edilir. Bu B bloğunun orta frekans bölgesinde yer alan B(4,1) ile B(3,2) veya B(5,2) ile B(4,3) pikselleri kullanılarak kodlama işlemi şu şekilde gerçekleştirilir: Damga biti 1 olduğu zaman eğer $B(u_1, v_1) > B(u_2, v_2)$ ise bu lokasyon üzerinde bir değişiklik yapılmaz, fakat bu koşul sağlanmıyorsa bu iki lokasyonun birbiri ile yeri değiştirilir ve 1 biti bloğa gömülmüş olur. Benzer şekilde, damga bitinin 0 olduğunda $B(u_1, v_1) < B(u_2, v_2)$ ise bu lokasyon üzerinde bir değişiklik yapılmaz, aksi durumda ise iki lokasyonun yeri değiştirilerek 0 biti yerleştirilmiş olur [5]. Sonrasında ters DCT kullanılarak damgalanmış görüntü elde edilir.

Damgalanmış görüntü içerisinde damganın bulunabilmesi için damgalanmış görüntü 8x8'lik bloklara ayrılır ve ayrık kosinüs dönüşümü yapılarak frekans uzayına geçilir. Daha önceden kodlama yapılan lokasyonlar birbiri ile karşılaştırılarak damga elde edilir. Eğer $B(u_1, v_1) > B(u_2, v_2)$ ise damga biti 1, $B(u_1, v_1) < B(u_2, v_2)$ ise damga biti 0 olarak alınarak gömülü filigran çıkarılmış olur.

Bu yöntem özellikle JPEG sıkıştırma algoritmasına bağımlılığı yüksek olacak şekilde tasarlanmıştır. Ancak gömme işlemi orta frekans bölgesinde yapıldığı için genel olarak direnci yüksektir.

2.2.2.6 Çevrecik dönüşümü ile sayısal damgalama yöntemi

Bu yöntem ile, sayısal filigran çevrecik dönüşümü kullanılarak konak görüntü içerisine gömülmesi hedeflenmiştir. Damganın gömme işlemi çevrecik dönüşümü kullanılarak elde edilen yüksek enerjiye sahip yüksek frekanslı yönlü alt bant içerisinde yapılmıştır. Damganın çıkarılması işleminde orijinal konak görüntüsüne ihtiyaç duyulmaz. Önerilen yöntemin birçok saldırıya (siyah ve gürültü gürültüsü, Gaussian gürültü vb.) karşı dayanıklı olduğu öne sürülmektedir, fakat sıkıştırmaya karşı dayanıklılığı hakkında bilgi verilmemektedir [16]. Gömme işlemi yüksek frekans bileşenlerinde yapıldığı için bu yöntemin sıkıştırmaya karşı dayanıksız olması beklenir.

$$\begin{aligned} D_s(i,j) &= D(i,j) \text{ eğer } (\text{sign}(D(i,j))=1) \& W_s==1) \\ &= D(i,j) \text{ eğer } (\text{sign}(D(i,j))=-1) \& W_s==0) \\ &= -D(i,j) \text{ eğer } (\text{sign}(D(i,j))=-1) \& W_s==1) \\ &= -D(i,j) \text{ eğer } (\text{sign}(D(i,j))=1) \& W_s==0) \end{aligned} \quad (2.12)$$

Burada $D(i,j)$, alt bantta yer alan (i,j) pozisyonundaki değer ve W_s binari damga kodudur. Bu işlemden sonra aşağıdaki (denklem 2.13) formülasyon ile çevrecik uzayındaki değerler modifiye edilir ve gömme işlemi tamamlanır.

$$D_w(i,j) = \alpha * D_s(i,j). \quad (2.13)$$

Bu denklemdeki α katsayısı değiştirilerek damganın gücü veya sağlamlığı ile damganın konak görüntü üzerindeki algılama bilirliliği belirlenebilir. Bu işlemler sonrasında çevrecik uzayında damgalama işlemi gerçekleşir ve son olarak ters çevrecik dönüşümü uygulanarak damgalanmış görüntü elde edilir.

$$\begin{aligned} W_s &= 1, \text{ if } \text{sign}(D(i,j))=1) \\ &= 0, \text{ if } \text{sign}(D(i,j))=-1) \end{aligned} \quad (2.14)$$

Filigranın çıkarılması aşamasında gömme işleminde uygulanan adımlar tersten uygulanır. Bunun için öncelikle damgalanmış görüntünün çevrecik dönüşümü alınır ve en yüksek enerjili alt bant üzerinde damga aranır. Bu alt bant üzerinden aşağıdaki algoritma ile şifrelenmiş damga çıkarılır.

2.2.2.7 DWT temelli sayısal damgalama yöntemi

Sayısal damgalama yapılırken kullanılan dönüşümlerden biri de ayrık dalgacık dönüşümüdür. DWT ile yapılan en temel sayısal damgalama yöntemi 1-seviyeli ve LL bandına yapılan damgalama yöntemidir. Bu yöntem LL bandına yapıldığı için saldırılara karşı dayanıklıdır, fakat sayısal filigranın damgalanmış görüntüden çıkarılması için orijinal görüntüye ve orijinal sayısal filigrana ihtiyaç duymaktadır.



Şekil 2.12 : Konak görüntünün ve sayısal filigranın seviye-1 Haar dalgacık dönüşümleri

Bu yöntemle ilişkin dönüşümler şekil 2.12'deki gibi yapılmaktadır. Şekilde de belirtildiği üzere sayısal filigranın gömme işlemi için öncelikle sayısal filigranın ve konak görüntünün seviye-1 Haar dalgacık dönüşümü alınır. Sonrasında aşağıdaki denklem kullanılarak gömme işlemi gerçekleştirilir.

$$LL_{WI} = LL_I + \alpha \cdot LL_W \quad (2.15)$$

Denklem 2.15’de LL_I konak görüntünün seviye 1 LL bandı, LL_W sayısal filigranın seviye 1 LL bandı, LL_{WI} damgalanmış görüntünün LL bandıdır. α katsayısı ise damgalama yönteminin gücünü sağlamaktadır. Bu katsayı yükseldikçe konak görüntüde bozulmalara yol açmaktadır, azaldığında ise damgalanmış görüntüden sayısal filigranın çıkarılması zorlaşmaktadır. Bu kriter göz önüne alınarak alpha değeri 0,02 olarak belirlenmiştir. Denklem 2.15 gerçekleştirildikten sonra LL_I bandı, LL_{WI} ile değiştirilip ters Haar dalgacık dönüşümü alınır ve damgalanmış görüntü elde edilir.

Sayısal filigranın, konak görüntüden çıkarılması için damgalanmış görüntünün, orijinal sayısal filigranın ve orijinal konak görüntün Haar dalgacık dönüşümü alınır ve aşağıdaki denklem ile sayısal filigran konak görüntüden çıkarılır.

$$LL_{EW} = (LL_{WI} - LL_I) / \alpha \quad (2.16)$$

Denklem 2.16’da LL_{EW} , damgalanmış görüntüden çıkarılan sayısal filigranın LL bandı, orijinal sayısal filigranın LH, HL ve HH bantlarıyla birleştirilir ve oluşan yapının ters dalgacık dönüşümü alınarak sayısal filigran çıkarılmış olur.

2.2.2.8 DWT ve SVD temelli sayısal damgalama yöntemi

Sayısal damgalamada çok kullanılan diğer bir yöntem, ayrık dalgacık dönüşümü ve tekil değer ayrışımı temelli sayısal damgalama yöntemidir. Bu yöntem sayısal filigranın çıkarılması sırasında orijinal konak görüntüsüne ve orijinal filigrana ihtiyaç duyduğundan kör olmayan sayısal damgalama olarak sınıflandırılır.

Sayısal damgalamanın gömme basamağını gerçekleştirmek için öncelikle konak görüntüsünün ayrık dalgacık dönüşümü alınır ve LL_1 , HL_1 , LH_1 ve HH_1 level-1 bantları elde edilir. Daha sonra LL_1 bandının ayrık dalgacık dönüşümü alınarak LL_2 , HL_2 , LH_2 ve HH_2 oluşturulur.

$$LL_2 = U_Y S_Y V_Y^*, I_W = U_W S_W V_W^* \quad (2.17)$$

DWT-SVD yönteminde DCT-SVD’ye benzer bir yol izlenmektedir. LL_2 ’nin ve sayısal filigranın tekil değer ayrışımı uygulanarak tekil değerleri içeren köşegen

matrisler S_Y ve S_W elde edilir (Denklem 2.17). Daha sonra aşağıdaki Denklem 2.18 kullanılarak yeni köşegen matris elde edilir.

$$S_{YW} = S_Y + \alpha S_W \quad (2.18)$$

Bu köşegen matris kullanılarak damgalanmış LL_{2W} matrisi denklem 2.19'deki gibi oluşturulur. Bu denklemde alpha diğer sayısal damgalama yöntemlerinde olduğu gibidir, bu yöntemde alpha, damgalamanın saldırılara karşı gücünü ve konak görüntüsü deformasyonunu dengelemesi 0,75 olarak seçilmiştir.

$$LL_{2W} = U_Y S_{YW} V_Y \quad (2.19)$$

Oluşturulan LL_{2W} ile konak görüntünün LL_2 bandı yer değiştirilerek, damgalanmış yapının ters dalgacık dönüşümü alınır ve LL_{1W} elde edilir. Benzer şekilde tekrar ters dalgacık dönüşümü alınarak damgalanmış görüntü elde edilir.

Sayısal filigranın çıkarılma işlemi için, gömme işleminde olduğu gibi iki adet ayrık dalgacık dönüşümü alınarak başlar, fakat bu işlem hem damgalanmış görüntüye hem de orijinal konak görüntüsüne uygulanır. İki görüntünün de Denklem 2.20'deki gibi köşegen matrisleri bulunur.

$$LL_{2W} = U_Y S_{YW} V_Y^*, LL_{2O} = U_Y S_{YO} V_Y^* \quad (2.20)$$

Elde edilen köşegen matrisler ile Denklem 2.21 kullanılarak sayısal filigranın köşegen matrisi damgalanmış görüntüden çıkarılır.

$$S_{EW} = (S_{YO} - S_{YW}) / \alpha \quad (2.21)$$

Damgalanmış görüntüden çıkarılan köşegen matris S_{EW} Denklem 2.17'da elde edilen S_W ile yer değiştirilerek sayısal filigran aşağıdaki denklem ile tekrar elde edilir.

$$I_{EW} = U_W S_{EW} V_W^* \quad (2.22)$$

I_{EW} ve I_W karşılaştırılarak sayısal filigranın doğruluğu gözlenir.

2.3 Sayısal Damgalama için Saldırı Yöntemleri ve Ölçüm Teknikleri

Görüntü üzerine yapılan damgalama yöntemleri dışarıdan gelecek saldırılara karşı dirençli olması çok önemlidir. Dışarıdan gelen herhangi bir saldırı ile damgalanmış görüntü bozulmadan içerisindeki filigran bozulabiliyor olması bir problem ortaya çıkarır. Bu yüzden sayısal damgalama yöntemleri geliştirilirken saldırılara karşı önceden test edilmesi gerekmektedir. Damgalanmış bir görüntüye saldırı yapılırken dikkat edilmesi gereken nokta görüntü üzerinde insan algı perspektifine göre bozulma olmaması ya da çok az bozulma olması gerekmektedir. Eğer kullanılan saldırı yöntemi konak görüntü içerisinde yer alan sayısal damgaya sadece konak görüntüyü bozarak zarar verilebiliyor ise kullanılan sayısal damgalama yönteminin saldırı yöntemine karşı dirençli olduğu sonucuna varılır.

Sayısal damgalama yöntemlerine karşı uygulanan saldırı yöntemlerinden biri gürültü algoritmalarının konak görüntüye uygulanması şeklinde olur. Tuz ve karabiber (siyah-beyaz) gürültü, Gaussian gürültü ve Poisson gürültüsü gibi gürültüler bu tarz saldırı yöntemlerine örnek olarak verilebilir.

Görüntü üzerinde yapılan geometrik değişimler de saldırı yöntemleri arasındadır. Konak görüntünün boyutu değiştirilerek, bir kısmı kesilerek ve rotasyon işlemleri yapılarak sayısal filigrana zarar vermeye çalışıp, sayısal damgalama yönteminin direnci ölçülebilir. Bir diğer saldırı yöntemi de görüntü işlemede kullanılan filtrelerdir. Gaussian, medyan, yüksek ve alçak geçiren veya özel tasarlanmış filtreler konak görüntüdeki filigranın bütünlüğünü bozmak için uygulanabilir. Bunun dışında görüntü üzerinde yapılan parlaklık, kontrast ve bulanıklık manipülasyonları da saldırı yöntemleri arasında yer almaktadır.

Dirençli sayısal damgalama yöntemlerinin kayıplı sıkıştırma algoritmalarına karşı dayanıklı olması beklenmektedir. Bu yüzden damgalama yönteminin gücünü test etmek için JPEG, JPEG2000, JPEG XR, CPC gibi sıkıştırma yöntemleri konak görüntüye uygulanabilir.

Görüntü üzerinde yapılan sayısal damgalamada, damgalanmış bir görüntü ile orijinal görüntü arasındaki görsel benzerliği ölçmek için tepe sinyal gürültü oranı(PSNR) hesaplanır [21].

PSNR'ın hesaplanmasına ilişkin eşitlik Denklem 2.23'de verilmiştir.

$$\begin{aligned}
 PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\
 &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\
 &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE)
 \end{aligned} \tag{2.23}$$

Bu eşitlikte MSE ortalama karasel hatadır ve aşağıdaki Denklem 2.24 ile tanımlanır.

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \tag{2.24}$$

Burada I damgalanmamış orijinal konak görüntüsünü, K ise içerisine sayısal filigran gömülmüş damgalanmış görüntüyü temsil etmektedir.

Damgalanmış görüntü ile orijinal görüntünün benzerliğinin ölçülmesi gibi gömülen sayısal filigran ve çıkarılan sayısal filigran arasında da benzerlik ölçümü yapılabilir [21]. Bunun için normalleştirilmiş korelasyon katsayısı, NC, kullanır.

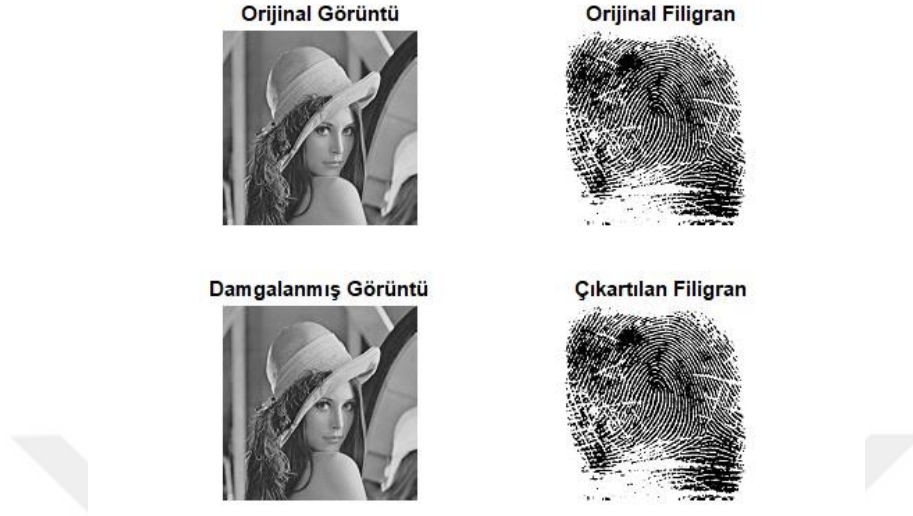
$$NC = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2 \right) \left(\sum_m \sum_n (B_{mn} - \bar{B})^2 \right)}} \tag{2.25}$$

Bu eşitlikte A, konak görüntüye gömülecek sayısal filigranı temsil etmektedir, B ise damgalanmış görüntüden çıkarılan sayısal filigrandır. $\bar{A}$ ve $\bar{B}$ ise sırasıyla A ve B'nin aritmetik ortalamalarıdır.

Bir sonraki bölümde, bölüm 2.2.2'de anlatılan sayısal damgalama yöntemlerinden 5 tanesine tuz ve karabiber gürültüsü, bulanıklaştırma, kontrast değişimi, görüntünün yeniden boyutlandırılması, parlaklık değişimi, medya filtre, görüntünün döndürülmesi, Gaussian gürültü uygulanacaktır ve PSNR ile NC değerleri incelenecektir.

2.4 Sayısal Damgalama Uygulamaları ve Ölçümleri

2.4.1 LSB temelli sayısal damgalama uygulaması ve ölçümleri



Şekil 2.13 : LSB sayısal damgalama

LSB sayısal damgalama yöntemi ile yapılan damgalama Şekil 2.13'deki gibidir. Hiçbir saldırı olmadığı zaman konak görüntüye gömülen sayısal filigran doğrudan çıkarılabilmektedir. Bu yöntem ile yapılan damgalamaya karşı yapılan saldırılar sonucunda alınan ölçümler Çizelge 2.1'de verilmiştir.

Çizelge 2.1 : LSB sayısal damgalama ölçüm sonuçları

Saldırı Yöntemleri	MSE	PSNR(dB)	NC	SNR
Saldırı Olmadan	0.50	51.15	1.000	45.49
Tuz ve Karabiber Gürültüsü	37.51	32.39	0.998	26.73
Bulanıklaştırma	113.28	27.59	0.003	21.93
Kontrast Değişimi	143.20	26.57	0.004	20.91
Görüntünün Boyutlandırılması	0.73	49.48	0.329	43.82
Parlaklık Değişimi	98.65	28.19	0.999	22.53
Medyan Filtre	25.20	44.01	0.923	38.35
Görüntünün Döndürülmesi	509.57	21.060	0.604	15.40
Gaussian Gürültü	642.31	20.050	0.001	14.39

LSB yönteminin bulanıklaştırma, kontrast değişimi, görüntünün yeniden boyutlandırılması, görüntünün döndürülmesi ve Gaussian gürültüsüne karşı bağışıklığı olmadığı görülmektedir. Saldırıya uğramış görüntüler ve bu görüntülerden çıkarılan sayısal filigranlar Şekil 2.14'de verilmiştir.

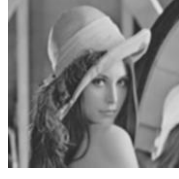
Tuz & Karabiber Gürültüsü



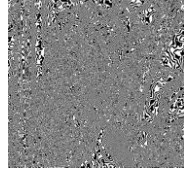
Çıkarılan Sayısal Filigran



Bulanıklaştırma



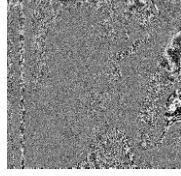
Çıkarılan Sayısal Filigran



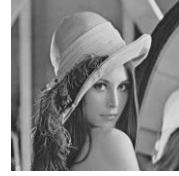
Kontrast Değişimi



Çıkarılan Sayısal Filigran



Görüntünün Boyutlandırılması



Çıkarılan Sayısal Filigran



Parlaklık Değişimi



Çıkarılan Sayısal Filigran



Medyan Filtre



Çıkarılan Sayısal Filigran



Görüntünün Döndürülmesi



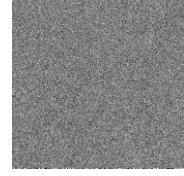
Çıkarılan Sayısal Filigran



Gaussian Gürültü

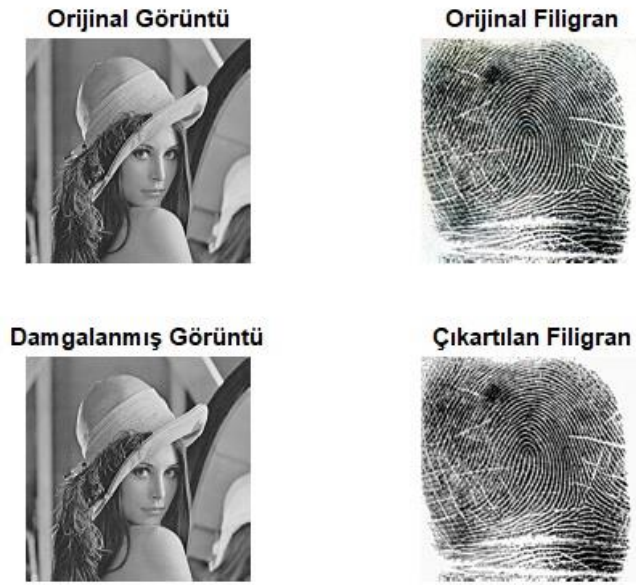


Çıkarılan Sayısal Filigran



Şekil 2.14 : LSB sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonrasında çıkarılan sayısal filigranlar

2.4.2 DWT-SVD temelli sayısal damgalama uygulaması ve ölçümleri



Şekil 2.15 : DWT-SVD temelli sayısal damgalama

DWT-SVD temelli sayısal damgalama yöntemine ilişkin damgalanmış görüntü ve damgalanmış görüntüden çıkarılan sayısal filigran Şekil 2.15'deki gibidir. Bu yönteme karşı yapılan saldırılardan elde edilen sonuçlar ise Çizelge 2.2'de verilmiştir.

Çizelge 2.2 : DWT-SVD sayısal damgalama ölçüm sonuçları

Saldırı Yöntemleri	MSE	PSNR(dB)	NC	SNR
Saldırı Olmadan	888.08	18.65	0.999	12.970
Tuz ve Karabiber Gürültüsü	922.78	18.48	0.999	12.802
Bulanıklaştırma	888.09	18.65	0.832	12.971
Kontrast Değişimi	1506.70	16.35	0.963	10.670
Görüntünün Boyutlandırılması	887.36	18.65	0.999	12.972
Parlaklık Değişimi	439.77	21.70	0.984	16.020
Medyan Filtre	886.39	18.65	0.999	12.981
Görüntünün Döndürülmesi	1509.93	16.34	0.992	10.661
Gaussian Gürültü	1451.15	16.50	0.975	10.842

Bu sayısal damgalama yöntemi birçok saldırıya karşı yüksek bağışıklık göstermiştir. Fakat sayısal filigranın çıkarılması esnasında hem orijinal görüntüye hem de orijinal sayısal filigrana ihtiyaç duyması bu yöntemin dezavantajıdır. Bu yönteme uygulanan saldırılar ve bu saldırı sonrasında çıkarılan sayısal filigranlar Şekil 2.16'da verilmiştir.

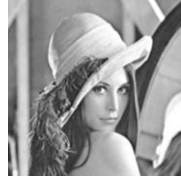
Tuz & Karabiber Gürültüsü



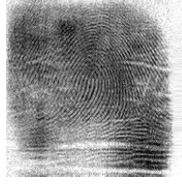
Çıkarılan Sayısal Filigran



Bulanıklaştırma



Çıkarılan Sayısal Filigran



Kontrast Değişimi



Çıkarılan Sayısal Filigran



Görüntünün Boyutlandırılması



Çıkarılan Sayısal Filigran



Parlaklık Değişimi



Çıkarılan Sayısal Filigran



Medyan Filtre



Çıkarılan Sayısal Filigran



Görüntünün Döndürülmesi



Çıkarılan Sayısal Filigran



Gaussian Gürültü

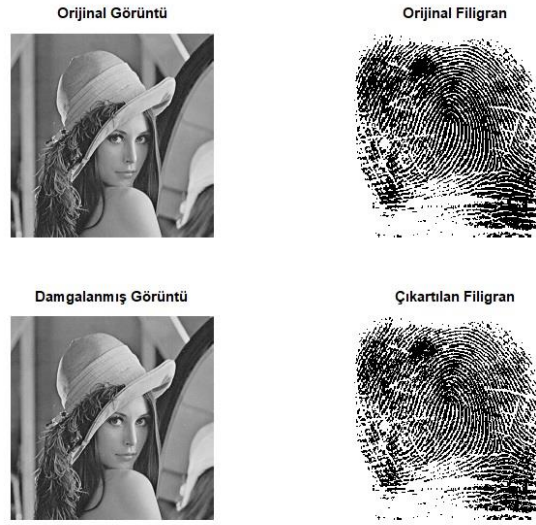


Çıkarılan Sayısal Filigran



Şekil 2.16 : DWT-SVD sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonrasında çıkarılan sayısal filigranlar

2.4.3 DCT orta frekans temelli sayısal damgalama uygulaması ve ölçümleri



Şekil 2.17 : DCT orta frekans sayısal damgalama

DCT orta frekans üzerinde yapılan sayısal damgalamaya ilişkin damgalanmış görüntü ve çıkarılan sayısal filigran Şekil 2.17'deki gibidir. Bu yöntem ile yapılan damgalamaya karşı yapılan saldırılar sonucunda alınan ölçümler Çizelge 2.3'de verilmiştir.

Çizelge 2.3 : DCT orta frekans sayısal damgalama ölçüm sonuçları

Saldırı Yöntemleri	MSE	PSNR(dB)	NC	SNR
Saldırı Olmadan	167.56	25.89	0.948	20.21
Tuz ve Karabiber Gürültüsü	203.31	25.050	0.898	19.37
Bulanıklaştırma	59.71	30.37	0.049	24.69
Kontrast Değişimi	385.57	22.27	0.868	16.59
Görüntünün Boyutlandırılması	133.39	26.88	0.674	21.20
Parlaklık Değişimi	266.79	23.87	0.948	18.19
Medyan Filtre	61.28	30.26	0.761	24.58
Görüntünün Döndürülmesi	672.91	19.85	0.005	14.17
Gaussian Gürültü	798.87	19.110	0.533	13.43

Sonuçlar incelendiğinde DCT orta frekans bölgesinde yapılan damgalama yöntemi bulanıklaştırma, Gaussian gürültüye ve geometrik saldırılara karşı dayanıksız olduğu görülmektedir. Damgalanmış görüntüye yapılan saldırılar sonrasında çıkarılan sayısal filigranlar ve saldırılar Şekil 2.18'de verilmiştir.

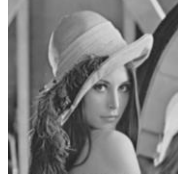
Tuz & Karabiber Gürültüsü



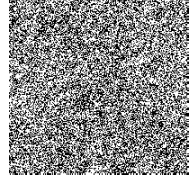
Çıkarılan Sayısal Filigran



Bulanıklaştırma



Çıkarılan Sayısal Filigran



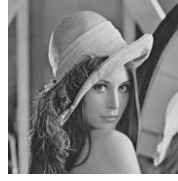
Kontrast Değişimi



Çıkarılan Sayısal Filigran



Görüntünün Boyutlandırılması



Çıkarılan Sayısal Filigran



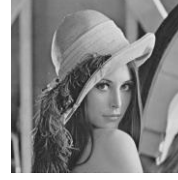
Parlaklık Değişimi



Çıkarılan Sayısal Filigran



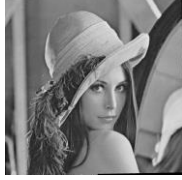
Medyan Filtre



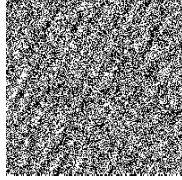
Çıkarılan Sayısal Filigran



Görüntünün Döndürülmesi



Çıkarılan Sayısal Filigran



Gaussian Gürültü



Çıkarılan Sayısal Filigran



Şekil 2.18 : DCT orta frekans sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar

2.4.4 DCT-SVD temelli sayısal damgalama uygulaması ve ölçümleri



Şekil 2.19 : DCT-SVD Sayısal Damgalama

DCT-SVD temelli sayısal damgalama yöntemine ilişkin damgalanmış görüntü ve damgalanmış görüntüden çıkartılan sayısal filigran ile orijinallerinin benzerliği Şekil 2.19’de gösterilmiştir.

Çizelge 2.4 : DCT-SVD sayısal damgalama ölçüm sonuçları

Saldırı Yöntemleri	MSE	PSNR(dB)	NC	SNR
Saldırı Olmadan	261.53	23.96	1.000	182.770
Tuz ve Karabiber Gürültüsü	298.14	23.38	0.861	17.70
Bulanıklaştırma	291.68	23.48	0.567	17.80
Kontrast Değişimi	652.12	19.99	0.905	14.31
Görüntünün Boyutlandırılması	261.94	23.95	1.000	18.27
Parlaklık Değişimi	65.56	29.96	0.898	24.29
Medyan Filtre	260.95	23.97	0.999	18.29
Görüntünün Döndürülmesi	848.54	18.84	0.982	13.17
Gaussian Gürültü	889.05	18.64	0.342	12.960

Bu yöntemle karşı yapılan saldırılardan elde edilen sonuçlar ise Çizelge 2.4’de verilmiştir. Bu çizelge incelendiğinde bulanıklaştırma ve Gaussian gürültüye karşı dayanıksız olduğu görülmektedir. Yapılan saldırılar ve sonrasında saldırıya uğramış görüntüden çıkarılmış sayısal filigran Şekil 2.20’de verilmiştir.

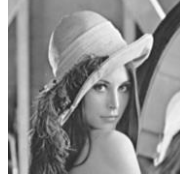
Tuz & Karabiber Gürültüsü



Çıkarılan Sayısal Filigran



Bulanıklaştırma



Çıkarılan Sayısal Filigran



Kontrast Değişimi



Çıkarılan Sayısal Filigran



Görüntünün Boyutlandırılması



Çıkarılan Sayısal Filigran



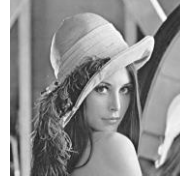
Parlaklık Değişimi



Çıkarılan Sayısal Filigran



Medyan Filtre



Çıkarılan Sayısal Filigran



Görüntünün Döndürülmesi



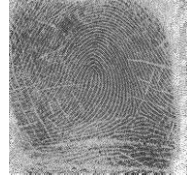
Çıkarılan Sayısal Filigran



Gaussian Gürültü



Çıkarılan Sayısal Filigran



Şekil 2.20 : DCT-SVD sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar

2.4.5 DWT temelli sayısal damgalama uygulaması ve ölçümleri



Şekil 2.21 : DWT Sayısal Damgalama

Şekil 2.21’de görüldüğü gibi DWT sayısal damgalama yönteminde hiçbir saldırı yapılmayan konak görüntüye gömülen sayısal filigran doğrudan çıkarılabilmektedir. Bu yöntem ile yapılan damgalamaya karşı yapılan saldırılar sonucunda alınan ölçümler Çizelge 2.5’de verilmiştir.

Çizelge 2.5 : DWT sayısal damgalama ölçüm sonuçları

Saldırı Yöntemleri	MSE	PSNR(dB)	NC	SNR
Saldırı Olmadan	10.850	37.78	0.983	32.10
Tuz ve Karabiber Gürültüsü	47.35	31.38	0.968	25.70
Bulanıklaştırma	68.74	29.76	0.356	24.080
Kontrast Değişimi	151.13	26.34	0.083	20.66
Görüntünün Boyutlandırılması	11.170	37.65	0.971	31.970
Parlaklık Değişimi	52.11	30.96	0.001	25.28
Medyan Filtre	11.550	37.51	0.932	31.83
Görüntünün Döndürülmesi	524.43	20.93	0.136	15.26
Gaussian Gürültü	655.11	19.97	0.099	14.29

DWT yönteminin bulanıklaştırma, kontrast değişimi, parlaklık, görüntünün döndürülmesi ve Gaussian gürültüsüne karşı bağışıklılığı olmadığı görünmektedir. Saldırıya uğramış görüntüler ve bu görüntülerden çıkarılan sayısal filigranlar Şekil 2.22’de verilmiştir.

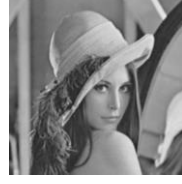
Tuz & Karabiber Gürültüsü



Çıkarılan Sayısal Filigran



Bulanıklaştırma



Çıkarılan Sayısal Filigran



Kontrast Değişimi



Çıkarılan Sayısal Filigran



Görüntünün Boyutlandırılması



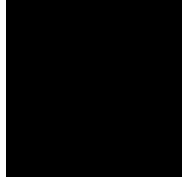
Çıkarılan Sayısal Filigran



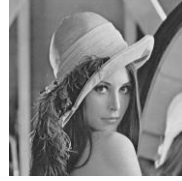
Parlaklık Değişimi



Çıkarılan Sayısal Filigran



Medyan Filtre



Çıkarılan Sayısal Filigran



Görüntünün Döndürülmesi



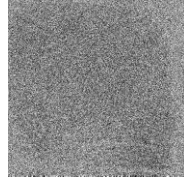
Çıkarılan Sayısal Filigran



Gaussian Gürültü



Çıkarılan Sayısal Filigran



Şekil 2.22 : DWT sayısal damgalama üzerine yapılan saldırılar ve bu saldırılar sonucunda çıkarılan sayısal filigranlar

2.5 Sayısal Damgalama Uygulama Sonuçları

Sayısal damgalama yöntemleri incelenirken gömülü sistemler için en uygun sayısal damgalama yönteminin bulunması hedeflenmektedir. Sayısal damgalama yöntemlerinde DWT-SVD temelli damgalama yöntemi en iyi sonucu vermektedir, fakat sayısal filigranın çıkarılması sırasında orijinal görüntüye ve orijinal sayısal filigrana ihtiyaç duyan kör olmayan sayısal damgalama yöntemidir. Bu yüzden orijinal görüntüyü ve orijinal sayısal filigranın saklanması gerekmektedir, bu durum gömülü sisteme ekstra yük getirmektedir.

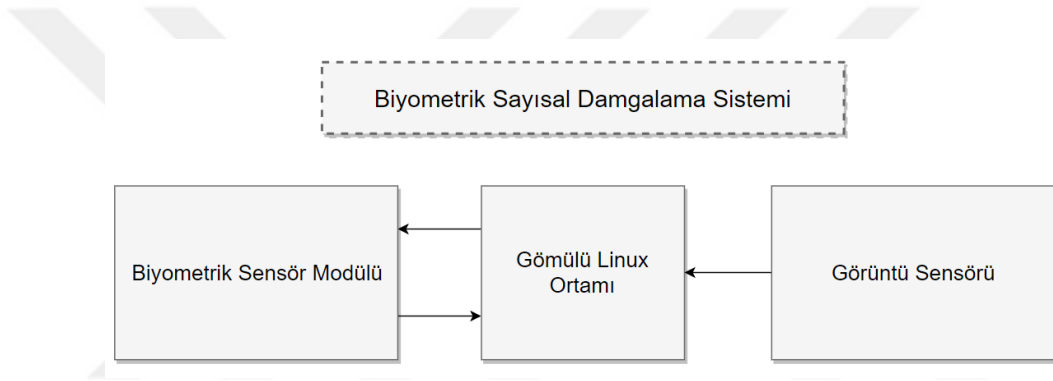
DWT temelli ve DCT-SVD temelli sayısal damgalama yöntemleri de benzer özelliklerden dolayı gömülü sistemler için uygun değildir.

LSB ve DCT orta frekans sayısal damgalama yöntemleri ise diğer yöntemlerin aksine kör sayısal damgalama sistemleridir ve orijinal konak görüntüsü ile orijinal sayısal filigran olmaması durumunda gömülmüş sayısal filigran damgalanmış görüntüden çıkarılabilmektedir. Ayrıca bu yöntemlerde sayısal filigranın görüntü olması zorunluluğu da yoktur, herhangi bir bit dizisi bu yöntemler ile konak görüntüsü içerisinde saklanabilir.

3. SAYISAL DAMGALAMA GÖMÜLÜ SİSTEM UYGULAMASI

Bu bölümde biyometrik ve kör sayısal damgalama yapabilen gömülü sistem tasarımına dair bilgiler verilecektir. Bunun için öncelikle gömülü sistemi oluşturan sistem elemanları açılacaktır ve sonrasında sayısal damgalama sisteminin çalışma basamakları gösterilecektir.

3.1 Sayısal Damgalama Gömülü Sistem Elemanları



Şekil 3.1 : Biyometrik sayısal damgalama sistemi

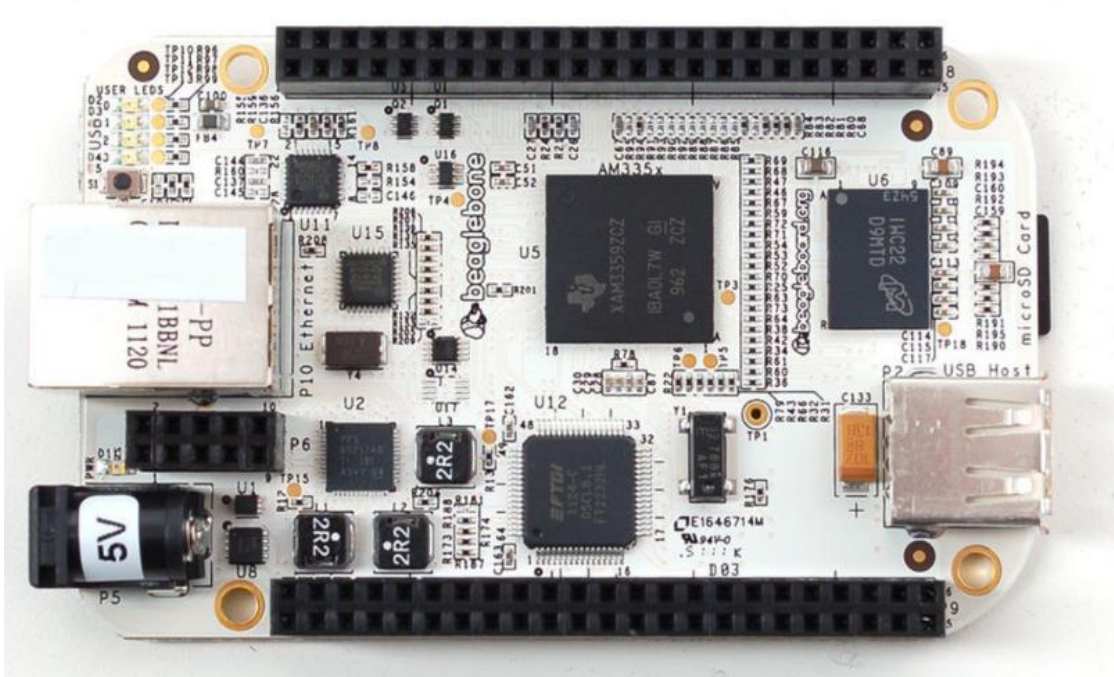
Biyometrik sayısal damgalama sistemine ilişkin blok diyagramı Şekil 3.1’de verilmiştir. Bu sistemde Biyometrik sensor modülü olarak ADH-Tech GT-511C3 optik parmak izi tanıma gömülü modülü kullanılmaktadır. Bu modül parmak izinin kaydı ve doğrulamasını yapılmasına yardımcı olmaktadır. Bu sistemin çekirdeğinde üzerinde gömülü Linux koşan Beaglebone bulunmaktadır. Beaglebone parmak izi sensörü ile görüntü sensoründen ihtiyacı olan bilgileri alarak biyometrik sayısal damgalama işlemini gerçekleştirmektedir. Bu sistem ile hazır görüntüler üzerinde sayısal damgalama yapılabilir, fakat sistemin kompakt olması için görüntü sensörü de eklenmiştir. Burada görüntü sensörü olarak USB veya IP kamera kullanılabilmektedir, ancak uygulamada Hikvision/Haikon DS-2CD2110F-IS model IP kamera kullanılmıştır.

3.1.1, 3.1.2 ve 3.1.3 bölümlerinde sistem modülleri daha ayrıntılı şekilde incelenecektir ve modüller arasında bilgi alışverişinin nasıl olduğu anlatılacaktır.

3.1.1 Gömülü Linux ortamı

Beaglebone, ARM tabanlı işlemciye sahip çeşitli Linux dağıtımlarını koşturabilen gömülü sistem oluşturmak için kullanılabilen mini bir bilgisayardır. Cihazın donanım özellikleri aşağıdaki gibidir.

- AM335X 720 MHz ARM Cortex-A8 işlemci
- 3D grafik hızlandırıcı
- Güç yönetimi için ARM-Cortex M3
- 2x PRU 32-bit RISC CPUs
- 256 MB DDR2 RAM
- Bağlantılar; 10/100 Mbps Ethernet, USB Host, USB Client, SD kart, 2x46 pin başlıklar[24]



Şekil 3.2 : Beaglebone [24]

Beaglebone'a ilişkin görsel Şekil 3.2'deki gibidir. Cihaz SD kart üzerine kayıtlı Linux 3.8.13 kernele sahip Angstrom dağıtımı ile çalışmaktadır. Kurulan Linux ortamı ile kullanıcı uzayında USB, UART ve Ethernet gibi birçok çevresellere erişmek de

mümkündür. Mini bir bilgisayar ortamı olduğu için standart masaüstü bilgisayarda çalıştırıla bilinen birçok kütüphane kullanılabilir, ancak bu kütüphanelerin kullanılabilmesi için çapraz derleme yapılması gerekmektedir.

Sayısal damgalama projesi için görüntü işleme algoritmalarına yardımcı olması için OpenCV kütüphanesi sisteme eklenmiştir. Bunun dışında standart C/C++ kütüphaneleri de cihaz içinde yer almaktadır.

Biyometrik sayısal damgalama sistemi için Beaglebone'un USB host portu parmak izi sensor modülüne ayrılmıştır. Ethernet portu ise IP kamera ile haberleşmek için kullanılmaktadır.

3.1.2 Biyometrik sensor modülü

Biyometrik sensor modülü olarak ADH-Tech GT-511C3 parmak izi tanıma modülü kullanılmaktadır. Modüle ait görsel Şekil 3.3'deki gibidir.



Şekil 3.3: GT-511C3 [22]

Modül yüksek doğruluk ve hızda parmak izi kaydı ve tanımlaması yapabilmektedir. Parmak izi görüntüsü, parmak izi şablonları doğrudan modülden alınabilir, ayrıca modülü kullanan cihazdan modüle parmak izi şablonu gönderilebilir.

Parmak izi sensor modülünün teknik özellikleri Çizelge 3.1’deki gibidir.

Çizelge 3.1 : GT-511C3 parmak izi sensorunun teknik özellikleri [22]

GT-511C3	Teknik özellikler
İşlemci	ARM Cortex M3 Core
Sensor	Optik sensor
Sensorun etkin alanı	14 x 12.5 mm
Görüntü boyutu	202 x 258 piksel
Çözünürlük	450 dpi
Şablon boyutu	496 Byte (şablon) + 2 Byte (sağlama)
Haberleşme ara yüzü	UART, USB
Yanlış kabul oranı (FAR)	%0.001
Yanlış ret oranı (FRR)	%0.1
Kayıt zamanı	< 3 saniye
Kayıt tanımlama zamanı	< 1 saniye
Parmak izi tanıma algoritması	SmackFinger 3.0

3.1.3 Görüntü sensoru

Tasarlanan biyometrik sayısal damgalama sisteminde görüntü sensoru olarak USB veya IP kamera kullanılabilir. Ancak uygulamada görüntü sensoru olarak Hikvision/Haikon DS-2CD2110F-IS kullanılmıştır. Kameraya ilişkin görsel Şekil 3.4’de verilmiştir.



Şekil 3.4 : Hikvision/Haikon DS-2CD2110F-IS kamera [23]

Bu cihazın özelliği çektiği görüntüye MJPEG/H264 akış olarak ağ üzerinden ulaşılabilir olmasıdır. Aynı zamanda ONVIF desteği sayesinde doğrudan görüntüde alınabilmektedir, fakat gömülü sistem uygulamasında OpenCV kütüphanesinin özelliklerinden yararlanılarak MJPEG akışından görüntü alınmıştır. Kameralara ait teknik özellikler Çizelge 3.2’deki gibidir.

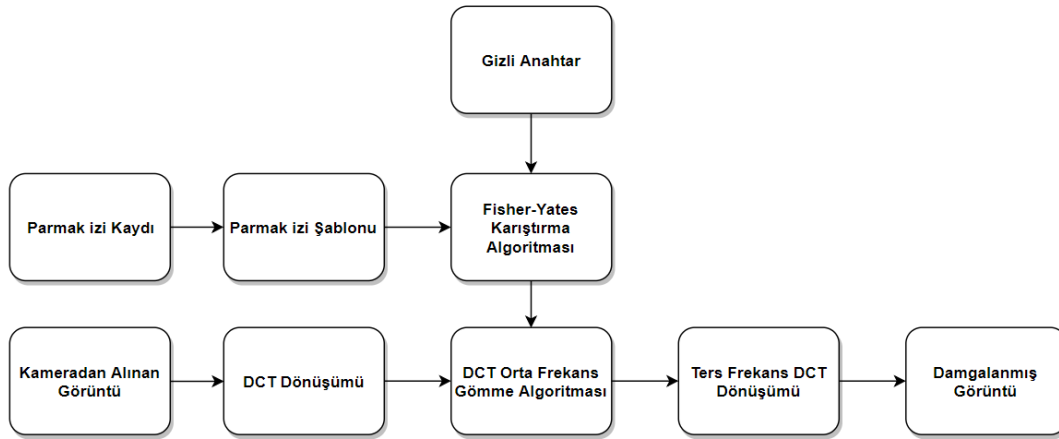
Çizelge 3.2 : DS-2CD2110F-IS kamera teknik özellikleri [23]

DS-2CD2110F-IS	Teknik özellikler
Görüntü Sensörü	1/3" Progressive Scan CMOS
Maksimum Çözünürlük	1280x960
Çerçeve Hızı	50 Hz: 25 fps (1280 × 960), 25 fps(1280 x 720) 60 Hz: 30 fps (1280 × 960), 30 fps (1280 x 720)
Objektif Hızı	1/3 s to 1/100,000 s
Lens	4mm@ F2.0 (2.8mm, 6mm optional)
Lens Kurulumu	M12
Geniş Dinamik Aralık	Digital WDR
Dijital Gürültü Azaltma	3D DNR
Video Sıkıştırma	H.264/MJPEG
H.264 Türü	Baseline Profile / Main Profile
Video Bit Hızı	32Kbps-8Mbps

3.2 Biyometrik Sayısal Damgalama Gömülü Sistem Uygulaması

Sayısal filigranın seçilmesinde önemli unsurlardan biri de aidiyetin bilgisinin belirgin olmasıdır. Sayısal damgalama sonrasında telif hakkı iddia edilebilmesi için damganın özel bilgiler içermesi gerekmektedir. Dolayısıyla eğer kişiye özel bir damgalama yapılması planlanıyorsa parmak izi, göz irisi, yüz hatları gibi biyometrik veriler sayısal filigran için oldukça iyi malzemelerdir. Bu temelden hareket ile parmak izini biyometrik veri olarak kullanan, DCT orta frekans bandında damgalama yapan ve kör sayısal damgalama yöntemini içeren gömülü sistem tasarımı yapılmıştır. Belirtilen gömülü sistem damgalama kısmı sayısal filigranın gömülmesi işlemi ve sayısal filigranın çıkarılması ile doğrulanması işlemi olarak iki başlıkta incelenecektir.

3.2.1 Biyometrik sayısal filigranın konak görüntüsüne gömülmesi



Şekil 3.5 : Biyometrik sayısal filigranın gömme şeması

Şekil 3.5’de tasarlanan biyometrik sayısal damgalama yöntemlerinin işlem sırası gösterilmektedir. Şemadan da görüleceği üzere gömme işlemi parmak izi kaydı ile başlamaktadır, kaydı alınan parmak izinin şablonu parmak izi sensoründen Beaglebone’a taşınmaktadır. Alınan şablon güvenli hale getirilmesi için Fisher-yates karıştırma algoritmasına verilen gizli anahtar ile karıştırılır. Daha sonra kameradan alınan konak görüntünün DCT dönüşümü alınır ve DCT orta frekans bölgesinde kayıt yapılır. Daha sonra ters DCT dönüşümü yapılarak damgalanmış görüntü elde edilir.

Biyometrik sayısal damgalamanın en önemli basamaklarından biri sayısal filigranı yani biyometrik veriyi elde etmektir. Oluşturulan sistem bu veriyi oluşturmak için GT-511C3 parmak izi modülünden yararlanılmıştır. Beaglebone ile GT-511C3 arasındaki haberleşme UART protokolü üzerinden kurulmuştur ve varsayılan 9600 Baud hızında veri aktarımı yürütülmüştür. Parmak izi sensorüyle haberleşme Şekil 3.6’da gösterilen 12 bytelık komut paketleri gönderilerek sağlanır.

Başlangıç Byte'ları		Cihaz ID		Giriş Parametre				Komut		2 Byte Sağlama
0x55	0xAA	0x00	0x01							Önceki 10 byte'ın toplamı

Şekil 3.6 : GT-511C3 komut paket yapısı [22]

Komut paketleri başlangıç byteleri 0x55 ve 0xAA ile başlar. Cihaz ID’si sabit olarak 0x0001’dir. Giriş parametreleri ve komut byteleri sensordan yapılması istenilen göreve göre değişiklik göstermektedir. Sağlama byteleri ise komut paketinin doğruluğunu kontrol etmek amacıyla kullanılır.

Parmak izi sensörü aldığı komut paketlerine cevap paketleri ile karşılık verir, bu pakete ilişkin yapıda komut paketine benzer şekilde 12 byte uzunluğundaki yapı Şekil 3.7’de verilmiştir.

Başlangıç Byte'ları		Cihaz ID		Çıkış Parametre				Cevap		2 Byte Sağlama
0x55	0xAA	0x00	0x01							Önceki 10 byte'ın toplamı

Şekil 3.7 : GT-511C3 cevap paketi yapısı [22]

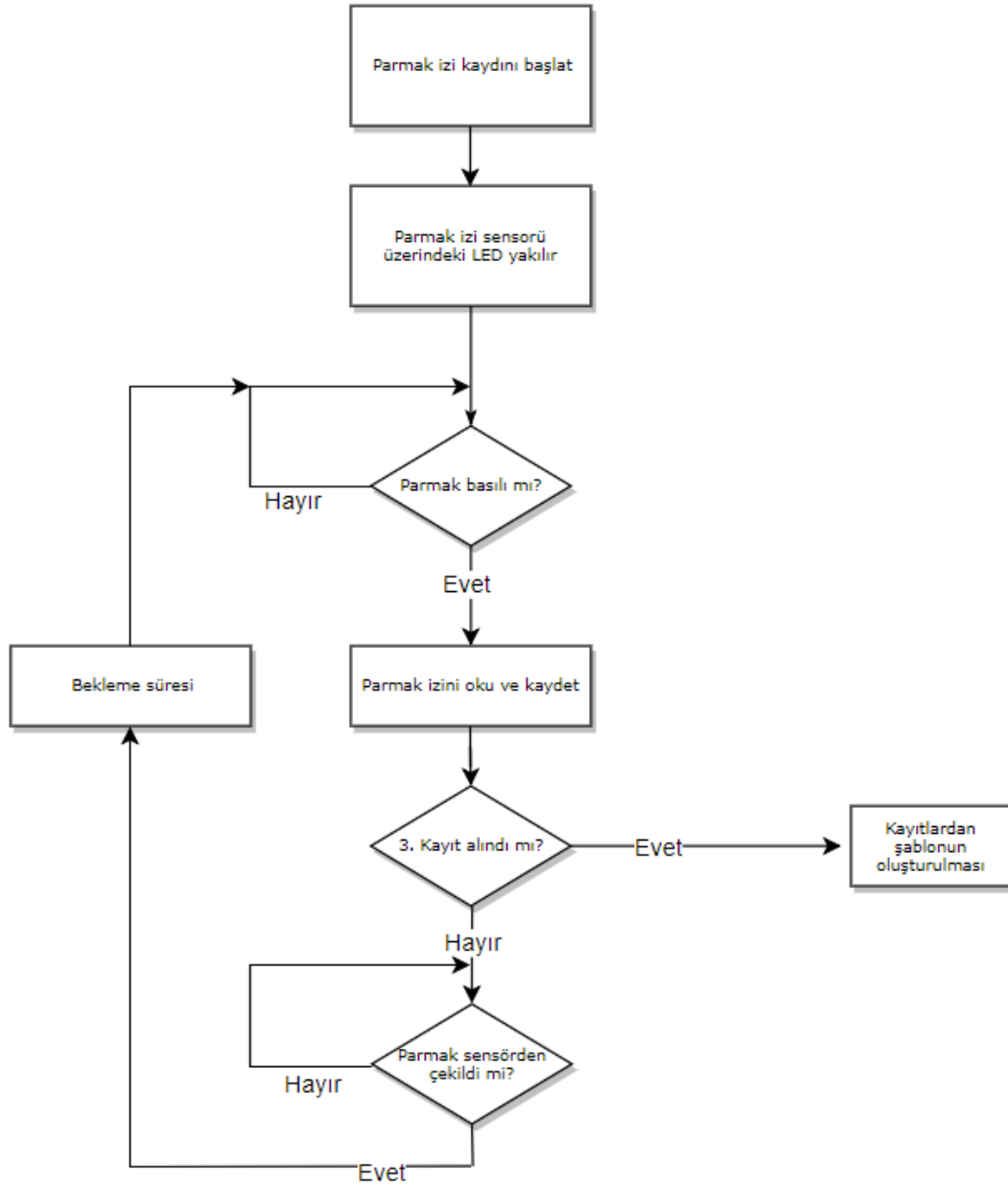
Bunun dışında parmak izi sensoründen parmak izi görüntüsünü almak, parmak izi şablonunu almak veya yüklemek için Şekil 3.8’deki gibi veri paketi kullanılmaktadır. Bu veri paketinin uzunluğu şablonlar için 498 Byte, parmak izi görüntüsü için ise 52116 Byte’tır.

Başlangıç Byte'ları		Cihaz ID		N-Byte Veri				2 Byte Sağlama
0x5A	0xA5	0x00	0x01					Önceki 4+N byte'ın toplamı

Şekil 3.8 : GT-511C3 veri paketi yapısı [22]

GT-511C3 modülünde kayıt parmak izi kaydı başlamadan önce sensör üzerindeki LED, sensörün parmak izini görebilmesi için yakılır. Bunun için *CmosLed*(0x0012) komutu Beaglebone’den UART üzerinden GT-511C3 modülüne gönderilir. Biyometrik verinin parmak izi sensöründen alınması *EnrollStart*(0x0022) komutunun Beaglebone’den UART üzerinden GT-511C3 modülüne gönderilmesiyle başlar. Bu aşamada *isPressFinger*(0x0026) komutu gönderilerek parmak izi alınacak parmağın sensör üzerinde olup olmadığı komuta karşılık gelen cevap paketi üzerinden kontrol edilir. Olumlu cevap gelmesi durumunda *captureFinger*(0x0060) komutu ile parmak izi yakalanır ve bunun ardından *enroll1*(0x0023) komutu gönderilerek sensör modülü üzerinde ilk kayıt alınır.

Bu aşamada parmağın parmak izi sensöründen ayrılması ve tekrar sensörün üzerine konulması gerekmektedir. *isPressFinger*(0x0026) komutu ile bu durum kontrol edilir. İlk kayıta benzer şekilde ikinci ve üçüncü kayıtlar sırasıyla *enroll2*(0x0024) ve *enroll3*(0x0025) komutlarıyla alınır. *enroll3*(0x0025) komutu ile beraber daha önce alınan kayıtlar birleştirilerek parmak izi şablonu GT-511C3 üzerinde kayıt edilir. Parmak izi kaydına ilişkin akış diyagramı Şekil 3.9’da verilmiştir.



Şekil 3.9 : Parmak izi kaydı akış şeması

Biyometrik verinin damgalamada kullanılabilmesi için GT-511C3 üzerinde kaydedilen parmak izi şablonunun Beaglebone'a taşınması gerekmektedir. Bunun için parmak izi sensörüne *GetTemplate(0x0070)* komutu gönderilir. Sensor modülü bu komuta cevap paketi ile cevap verir ve ardından 498 byte'lık parmak izi şablonunu içeren veri paketini Beaglebone'a gönderir.

498 Byte boyutundaki parmak izi şablonunun 496 byte'ı kaydedilen parmak ile ilgili bilgileri içermektedir. Bu bilgiler SmackFinger 3.0 algoritmasına göre oluşturulmuştur, bu algoritma açık kaynak değildir bu yüzden parmak izi şablonunun doğruluğu da GT-511C3 üzerinde yapılmak zorundadır. Geriye kalan 2 Byte ise,

verinin doğruluğunu kontrol etmek amacıyla 496 Byte biyometrik verinin toplanması ile elde edilir.

Elde edilen şablon doğrudan konak görüntüsüne gömülebilir yalnız daha güvenli olması için gizli bir anahtar kullanılarak yardımı ile parmak izi şablonu karıştırılacaktır. Bunun için Fisher-Yates karıştırma algoritması kullanılmıştır. Fisher-Yates karıştırma algoritması sonlu dizilerin rastgele bir şekilde yeniden oluşturulmasını sağlayan bir algoritmadır. Bu algoritmaya ilişkin sözde kod aşağıda verilmiştir.

n elemana sahip a dizisinin gizli anahtar ile karıştırılması;

anahtar ile sözde rastgele sayı üretici kökleme

a[n-1]'den a[1]'e kadar dizinin her elemanı için

$j \leftarrow \text{rasgele tamsayı } 0 \leq j \leq i$

a [j] ve a [i] dizideki yerlerinin değişimi

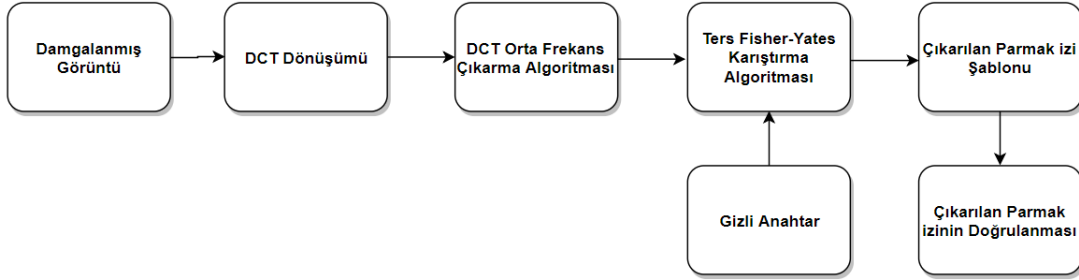
Karıştırma algoritması ile beraber sayısal filigran konak görüntüye gömmek için hazır duruma getirilmiştir. Gömülü sistemin diğer önemli aşaması ise IP kameradan görüntünün alınmasıdır. Bunun için Beaglebone ve IP kamera doğrudan tek bir Ethernet kablosuyla bağlanabilir ya da iki cihaz aynı ağ üzerine bağlanarak haberleşmesi sağlanabilir. Kullanılan IP kamera 640x480 boyutunda MJPEG akışı yapabilmektedir. Bu akışa kameranın IP numarası girilerek <http://<IP>/Streaming/channels/1/preview> URL'ini kullanılarak erişmek mümkündür.

Kameraya erişim doğrudan Beaglebone üzerinden OpenCV kütüphaneleri kullanılarak yapılabilmektedir. IP kameradan alınan 640x480 boyutundaki görüntü Beaglebone üzerindeki SD Karta kaydedilir.

Görüntü kaydı ve sayısal filigran oluşturulduktan sonra biyometrik sayısal damgalama için gerekli olan ihtiyaçlar edinilmiş olur. Bu aşamadan sonra Bölüm 2.2.2.5'de belirtildiği gibi DCT orta frekans gömme işlemi uygulanır. Uygulanan bu işlemde sonra ters DCT işlemi uygulanır ve damgalanmış görüntü Beaglebone üzerindeki SD karta kayıt edilir.

3.2.2 Damgalanmış görüntüden sayısal filigranın çıkarılması ve doğrulama

Damgalanan bir görüntüde aidiyet iddiasında bulunulabilmesi için sayısal filigranın damgalanmış görüntü içerisinden çıkarılması gerekmektedir. Biyometrik sayısal filigranın damgalanmış görüntüden çıkarılması için Şekil 3.10'da yer alan şema izlenmektedir. Çıkarılan sayısal filigranın doğruluğunun kontrol edilmesi gerekmektedir, bu yüzden çıkarılan veri GT-511C3 sensor modülü ile doğrulanır.



Şekil 3.10 : Biyometrik sayısal filigranın damgalanmış görüntüden çıkarılmasına dair işlem şeması

Biyometrik filigranın, damgalanmış görüntünün içerisinden çıkarılması DCT dönüşümü ile başlar. Daha sonra Bölüm 2.2.2.5’de bahsedildiği üzere DCT orta frekans bölgesindeki gömülü verileri uygulanan gömme algoritmasının tersi uygulanarak çıkarılır. Çıkarılan veri 498 byte karıştırılmış parmak izi şablonudur, bu yapı gizli anahtar kullanılarak ters Fisher-Yates karıştırma algoritması ile orijinal formuna getirilir. Ters Fisher-Yates algoritmasına ilişkin sözde kod aşağıdaki gibidir.

n elemana sahip a dizisinin gizli anahtar ile eski haline getirilmesi;

anahtar ile sözde rastgele sayı üretici kökleme

üreteç ile n boyutunda ve $0 \leq k \leq n$ olacak şekilde b dizisi üretimi

a[1]’den a[n-1]’e kadar dizinin her elemanı için

$j \leftarrow b[i]$

a [j] ve a [i] dizideki yerlerinin değişimi

Damgalanmış görüntüden çıkarılan veri saldırılardan dolayı yıpratılmış olabilir, bu yüzden 498 Bytelık dizinin ilk 496 byteı toplanır ve son 2 sağlama byteları ile karşılaştırılarak çıkarılan verinin sağlamlığı kontrol edilir.

Damgalanmış görüntüden çıkarılan biyometrik filigran sağlamlık testini geçer ise bir sonraki adım olan parmak izi şablonunun doğrulanmasına geçilir. Bunun için Beaglebone ile GT-511C3 parmak izi tanıma sensor modülü arasında komut ve veri paketlerinin gönderilmesi gerekmektedir.

Parmak izinin kayıt sürecinde olduğu gibi *CmosLed*(0x0012) komutu ile sensorun parmak izi doğrulması yapacak kişinin parmak izini daha iyi algılaması için sensor modülü üzerindeki LED yakılır. Daha sonra *SetTemplate*(0x0071) komutu sensor modülüne gönderilerek modülden onay içeren cevap paketi beklenir. Onay mesajının gelmesinin ardından damgalanmış görüntüden çıkarılan 498 byte boyutundaki parmak izi sayısal filigran şablonu veri paketi kullanılarak sensor modülüne gönderilir ve sensor modülü üzerinde kayıt edilir.

Bu noktadan itibaren damgalanmış görüntü üzerinde aidiyet iddia eden kişinin parmak izinin alınması gerekmektedir. Bunun için sensor modülüne 100 milisaniye aralıklarla *isPressFinger*(0x0026) komutu gönderilerek parmağın sensore bastırılması beklenir. Bu komut paketine olumlu cevap alınması durumunda *captureFinger*(0x0060) komutu ile parmak izi yakalanır. Yakalanan parmak izinin damgalanmış görüntüden çıkarılan şablon ile uyumluluğu kontrol etmek için *Verify*(0x0050) komutu parmak izi sensoruna gönderilerek modülün cevabı beklenir. Sensör modülünden Beaglebone'a gelen cevap olumlu ise doğrulama gerçekleştirilmiş olur ve damgalanmış görüntünün aidiyeti kanıtlanmış olur.

3.3 Biyometrik Sayısal Damgalama Çıktıları ve Sonuçları

GT-511C3 parmak izi tanıma sensoru, gömülü tasarım ortamı olarak Beaglebone ve görüntü sensoru olarak Haikon/Hikvision DS-2CD2110F-IS IP kamera kullanan gömülü biyometrik sayısal damgalama sistemi tasarlanmıştır. Gömülü sistemde sayısal damgalama yöntemi olarak DCT orta frekans damgalama yöntemi kullanılmıştır, dolayısıyla teknik kör sayısal damgalama yöntemidir. Bu yüzden damgalanın çıkarılması sırasında orijinal görüntüye ihtiyaç duymamaktadır. Bu durum gömülü sistem içi bir avantajdır. Gömülü sistem ile yakalanan görüntünün orijinali ve damgalanmış görüntü SD kart üzerinden alınmıştır ve sırasıyla Şekil 3.11 ve Şekil 3.12'de gösterilmiştir.



Şekil 3.11 : G m l  sistemde kamera tarafından yakalanan g r nt 



Şekil 3.12 : G m l  sistem ile damgalanmıř g r nt 

Şekil 3.11 ve Şekil.12 incelendiğinde iki görüntü arasında belirgin bir fark olmadığı görülmektedir ve ayrıca atağa uğramamış damgalanmış görüntüden sayısal parmak izi filigranı doğrudan çıkarılabilmektedir. Ayrıca damgalanmış görüntünün orijinal görüntüye göre tepe sinyal-gürültü oranı 36.45 dB olarak bulunmuştur.

Çizelge 3.3 : Beaglebone ve bilgisayar arasındaki performans karşılaştırması

İşlem	Beaglebone (Saniye)	Bilgisayar (Saniye)
Görüntü Yakalama	5.581	3.089
Gömme İşlemi	4.157	3.101
Çıkarma İşlemi	0.303	0.017
Doğrulama ve çıkarma işlemi	$\sim 1 + 0.303$	$\sim 1 + 0.017$
Parmak izi kaydı ve gömme işlemi	$\sim 3 + 4.157$	$\sim 3 + 4.101$

Gömülü sistemde yapılan damgalama işlemi benzer şekilde Intel Core i7 işlemcisine sahip bilgisayar üzerinde de yapılmıştır. Gömülü sistem ve bilgisayar arasındaki IP kameradan alınan 640x480 boyutundaki görüntü üzerine yapılan gömme işlemi, çıkarma işlemi gibi parametrelerin olduğu performans karşılaştırılması Çizelge 3.3’de verilmiştir.



4. SONUÇ VE ÖNERİLER

Çalışma içerisinde sayısal damgalama geniş bir şekilde incelenmesi hedeflenmiştir ve bu doğrultuda damgalama teknikleri sayısal veri tipine, sayısal filigran tipine, insan perspektifine, damgalamanın sağlamlığına ve dönüşüm bölgesine göre sınıflandırılmıştır. Sonrasında sayısal damgalama yöntemlerinde kullanılan dönüşümlere yer verilerek güncel sayısal damgalama yöntemlerinden bahsedilmiştir.

Gömülü sistemlere uygulanabilirliği göz önüne alınarak 5 sayısal damgalama yöntemi bilgisayar üzerinde gerçekleştirilmiştir ve bu yöntemlerin tepe sinyal-gürültü oranı ve normalize korelasyon katsayıları hesaplanmıştır. İncelenen yöntemler arasında en iyi sonuçları ayırık dalgacık dönüşümü ve tekil değer ayrışımı temelli sayısal damgalama yönteminden alındı, fakat gömülü sistemlere uygunluğu açısından ayırık kosinüs dönüşümünde orta frekans bölgesinde yapılan sayısal damgalama yöntemi tercih edilmiştir. Bu uygunluk, işlem gücü düşük olması, görüntü ve videoya uygulanabilir olması, çıkarma işlemi sırasında orijinal görüntüye ihtiyaç duyulmaması ve sayısal filigran olarak görüntü kullanma zorunluğu olmaması gibi özelliklerden kaynaklanmaktadır.

Çalışmada IP/USB kamera ve parmak izi kaydı içeren kompakt, biyometrik ve sayısal damgalama yöntemi kör olan bir gömülü sayısal damgalama sistemi tasarlanmıştır ve uygulaması gerçekleştirilmiştir. Sistem görüntü üzerinde sayısal damgalama yapabilecek şekilde uygulanmıştır, fakat görüntüye benzer şekilde video dosyalarına da uygulanabilir. Eğer video MJPEG ile oluşturulmuş ise MJPEG içerisindeki çerçevelerden bazılarını veya hepsine sayısal damgalama yapılabilir. H264 ile oluşturulmuş videolarda ise I-çerçevelerine damgalama yapılması gerekmektedir. H264'ün delta çerçevelerine yapılan damgalamanın çıkarılması oldukça zordur.

Uygulanan gömülü sistem geliştirmelere açıktır, istenildiği takdirde biyometrik veri olarak parmak izi yerine kesinliği daha yüksek biyometrik verilerde kullanılabilir. Gömülü sistemde sayısal damganın güvenliğini sağlamak için Fisher-Yates karıştırma algoritması kullanılmıştır. Güvenliği artırmak için AES, DES, RSA gibi kriptografik şifreleme algoritmaları kullanılabilir. Bu algoritmaların gömülü sistem üzerinde

yazılımsal olarak gerçekleşmesi performansı düşüreceğinden Beaglebone üzerinde yer alan AM3352 işlemcisinin üzerindeki donanımsal kripto hızlandırıcıları kullanılmalıdır.

Tasarlanan gömülü sistem damgalanmış görüntüleri SD kartına kaydetmektedir, fakat sistem üzerinde depolama alanı yeterince büyük olmadığından depolama sorunu ortaya çıkabilir. Bu sorunu çözmek için gömülü sistemin internet bağlantısı üzerinden bulut üzerindeki bir depoya kayıt yapılabilir.

Gömülü sistem üzerinde yapılan sayısal damgalamada görüntü üzerine yapılabilecek saldırılara karşı daha dayanıklı hale getirilebilir. Bunun için sayısal damga görüntü üzerine birkaç defa gömülebilir ve sayısal filigran üzerine eklenen kurtarma algoritmalarıyla sayısal filigranın zarar görmüş kısmı algoritmalar yardımıyla orijinal haline getirilebilir. Bunun dışında uygulanan yöntemde sayısal filigranın bütünlüğü 2 byte ile kontrol edilmektedir, bu yapıyı güçlendirmek için daha fazla byte ayrılabilir veya CRC(döngüsel artıklık denetimi) gibi veride yapılan değişimleri algılayabilen algoritmalar kullanılabilir.

Sistem oluşturulurken uygulanabilirliği ön planda olduğu için modüler şekilde tasarlanmıştır, bu yüzden özellikle Beaglebone üzerinde kullanılmayan donanımlar bulunmaktadır. Aynı sistemi daha düşük maliyetle ve tek bir kart üzerinde toplamak mümkündür. Bunun için AM3352 işlemcisinin merkezde olduğu parmak izi sensorunun ve kameranın bulunduğu bir sistem oluşturulabilir.

KAYNAKLAR

- [1] **Cox, I. J., Miller, M. L., & Way, I. (2002).** The first 50 years of electronic watermarking , 126–132.
- [2] **Frank, H. E. (1961).** Identification of sound and like signals. United States. Retrieved from <https://patents.google.com/patent/US3004104>
- [3] **Seddik, H., Sayadi, M., & Fnaiech, F. (2009).** A new blind image watermarking method based on shur transformation. Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE, 1967–1972. <http://doi.org/10.1109/IECON.2009.5414857>
- [4] **Tirkel, A. Z., Rankin, G. A., van Schyndel, R. M., Ho, W.J., Mee, N. R. A. & Osborne, C.F. (1993).** Electronic water mark.
- [5] **Dutta, M. K., Singh, A., Soni, K. M., Burget, R., & Riha, K. (2013).** Watermarking of digital media with encrypted biometric features for digital ownership. Contemporary Computing (IC3), 2013 Sixth International Conference of IEEE. <http://doi.org/10.1109/IC3.2013.6612172>
- [6] **Cox, I. J., Miller, M. L., Bloom, J. A., & Way, I. (2000).** Watermarking applications and their properties. The Int. Conf. on Information Technology'2000, Las Vegas, 1–5.
- [7] **Guru, J., & Damecha, H. (2014).** Digital Watermarking Classification: A Survey. International Journal of Computer Science Trends and Technology (IJCTST), 2(5), 8–13.
- [8] **Rashid, A. (2016).** Digital Watermarking Applications and Techniques: A Brief Review. International Journal of Computer Applications Technology and Research, 5(3), 147–150.
- [9] **Mousavi, S. M., & Naghsh, A. (2014).** Watermarking Techniques used in Medical Images: a Survey. Journal of Digital Imaging, 27(6), 714–729. <http://doi.org/10.1007/s10278-014-9700-5>
- [10] **Singh, P., & Chadha, R. S. (2013).** A Survey of Digital Watermarking Techniques, Applications and Attacks. International Journal of Engineering and Innovative Technology (IJEIT), 2(9), 165–175.
- [11] **Chawla, G., & Saini, R. (2012).** Classification of Watermarking Based upon Various Parameters. International Journal of Computer Applications & Information Technology, 1(2), 16–19.
- [12] **Shieh, J.M., Lou, D.C., Chang, M.C. (2006).** A semi-blind digital watermarking scheme based on singular value decomposition. Computer Standards & Interfaces, 28(4), 428–440.

- [13] **Asmara, R. A., & Agustina, R. (2017).** Comparison of Discrete Cosine Transforms (DCT), Discrete Fourier Transforms (DFT), and Discrete Wavelet Transforms (DWT) in Digital Image Watermarking. *International Journal of Advanced Computer Science and Applications*, 8(2), 245–249.
- [14] **Manikanda, S. (2014).** An Efficient Watermarking Algorithm Based on DWT and FFT Approach. *International Journal on Computer Science and Engineering*, 6(06), 211–216.
- [15] **Do, M. N., & Vetterli, M. (2005).** The Contourlet Transform : An Efficient Directional Multiresolution Image Representation. *IEEE Transactions on Image Processing*, 14(12), 2091–2106.
- [16] **Kishore Kumar, N. K., & Sheeba, V. S. (2012).** Blind biometric watermarking based on contourlet transform. 2012 3rd International Conference on Computing, Communication and Networking Technologies, ICCCNT 2012, (July). <http://doi.org/10.1109/ICCCNT.2012.6396042>
- [17] **Goyal, R., Kumar, N., & Ntroduction, I. (2014).** LSB Based Digital Watermarking Technique. *International Journal of Application or Innovation in Engineering & Management (IJAIEEM)*, 3(9), 15–18.
- [18] **Low, C. Y., Teoh, A. B. J., & Tee, C. (2007).** A preliminary study on biometric watermarking for offline handwritten signature. *Proceeding 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, ICT-MICC 2007*, (May), 691–696. <http://doi.org/10.1109/ICTMICC.2007.4448568>
- [19] **Mohanty, S. P., Adamo, O. B., & Kougianos, E. (2007).** VLSI architecture of an invisible watermarking unit for a biometric-based security system in a digital camera. *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 4, 7–8. <http://doi.org/10.1109/ICCE.2007.341340>
- [20] **Rao, N. N., Thrimurthy, P., & Babu, B. R. (2009).** An efficient copyright protection scheme for digital images using biometrics and watermarking. *Proceedings - 2009 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009*, 69–74. <http://doi.org/10.1109/ICCSIT.2009.5234757>
- [21] **Sreelekha, T., Dhamodhar, M., & Ramashri, T. (2013).** Watermarking algorithm using edge detection technique and DCT, DST, FFT. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2(12), 5982–5989.
- [22] **Url-1** < https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C3_datasheet_V2.1_20161025.pdf>, date retrieved 03.09.2018
- [23] **Url-2** < <https://www.hikvision.com/upload/20170115005456049.pdf> >, date retrieved 03.09.2018
- [24] **Url-3** < <http://beagleboard.org/bone-original> >, date retrieved 03.09.2018

ÖZGEÇMİŞ

Müh. Oğuz AYDIN, 1990 yılında Meram'da doğdu. 2007 yılında İstanbul Teknik Üniversitesi'nin Elektronik Mühendisliği Bölümü'nü kazandı. 2012 yılında bölümünü Onur Listesi derecesiyle bitirip, 2013 yılında Sayısal Sistemler Tasarım Evi'nde Gömülü Sistemler Yazılım ve Donanım Tasarım Mühendisi olarak çalışmaya başladı. Şu anda Yeşil Otomasyon 'da AR-GE Müdürü olarak iş hayatına devam etmektedir.

Ad-Soyad	: Oğuz Aydın
Doğum Tarihi ve Yeri	: 1990, Meram
E-posta	: aydnouz@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** : 2012, İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Fakültesi, Elektronik Mühendisliği Bölümü